

# Short Point Lists for CNFs and Stronger Constant-Depth Circuit Hardness

Xin Li\*

Yan Zhong\*

October 18, 2026

## Abstract

Proving lower bounds of an explicit function for the class of constant depth circuits with unbounded fan-in AND and OR gates is a central question in circuit complexity. The celebrated result of Håstad (1989) gives  $2^{\Omega(n^{1/(d-1)})}$  lower bounds for the parity and majority functions, which have been asymptotically the best known bounds for decades.

Recently, OpenAI (2026) improved these bounds and gave an explicit function in  $\mathsf{P}$  that requires  $2^{\omega(\sqrt{n})}$  size OR-AND-OR circuits. Soon after, Chukhin (2026) improved OpenAI's result and obtained a lower bound of  $2^{\Omega_d((n \log n / \log \log n)^{1/(d-1)})}$  against depth- $d$  circuits for every fixed  $d \geq 3$ . In this paper, we further improve Chukhin's result and prove a worst-case size lower bound of  $2^{\Omega_d((n \log n)^{1/(d-1)})}$  for three explicit functions: inverse trace over binary fields, the Goldreich–Tal trilinear function, and the polynomial evaluator of OpenAI with its original parameters. For inverse trace, we also prove a correlation bound under the uniform distribution: every depth-at-most- $d$  circuit of size at most  $S$ , where  $n \leq S \leq 2^{c_d n^{1/(d-1)}}$ , has correlation at most  $2^{-\eta_d n \log \log S / (\log S)^{d-1}}$  with the inverse trace function. Here  $c_d, \eta_d > 0$  are constants that depend only on the depth  $d$ . This improves on the classical parity correlation bound given by Håstad (2014).

Our worst case lower bounds are obtained by combining the techniques in previous works with a novel short-description decomposition of bounded-width CNFs, and the correlation bound additionally uses common partial decision trees. We also construct exact nonuniform AND/OR circuits for inverse trace of size  $2^{O(n^{2/3})}$  at depth eight and  $2^{O(\sqrt{n} \log n)}$  at depth nine. More generally, for every fixed integer  $h \geq 2$ , the construction gives depth- $(4h + 1)$  circuits of size  $2^{O_h(n^{1/h} \log n)}$ . The upper bounds follow by implementing a finite-field evaluation and interpolation construction using circuits that enumerate intermediate states.

---

\*Department of Computer Science, Johns Hopkins University. Emails: [lixints@cs.jhu.edu](mailto:lixints@cs.jhu.edu), [yzhong36@jhu.edu](mailto:yzhong36@jhu.edu).

# Contents

|          |                                                                       |           |
|----------|-----------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Introduction</b>                                                   | <b>1</b>  |
| 1.1      | Results . . . . .                                                     | 1         |
| 1.2      | Proof Overview . . . . .                                              | 3         |
| <b>2</b> | <b>An exact decomposition by lists of satisfying assignments</b>      | <b>6</b>  |
| <b>3</b> | <b>Restriction transfer without a clause-count loss</b>               | <b>7</b>  |
| <b>4</b> | <b>Inverse trace against every restricted CNF</b>                     | <b>8</b>  |
| <b>5</b> | <b>Controlling the whole circuit</b>                                  | <b>10</b> |
| 5.1      | Guarded CNFs and common trees . . . . .                               | 10        |
| 5.2      | Circuits with bounded bottom fan-in . . . . .                         | 11        |
| 5.3      | Removing the restriction on bottom fan-in . . . . .                   | 12        |
| <b>6</b> | <b>Worst-case hardness through monochromatic covers</b>               | <b>13</b> |
| <b>7</b> | <b>Explicit upper bounds for inverse trace</b>                        | <b>14</b> |
| 7.1      | Enumerating intermediate states . . . . .                             | 14        |
| 7.2      | Representing inverse trace by evaluations . . . . .                   | 15        |
| 7.3      | Three stages at adjustable depths . . . . .                           | 15        |
| <b>8</b> | <b>Consequences and limits of the representation</b>                  | <b>17</b> |
|          | <b>References</b>                                                     | <b>18</b> |
| <b>A</b> | <b>Deterministic switching parameters</b>                             | <b>20</b> |
| A.1      | The switching lemma . . . . .                                         | 20        |
| A.2      | Common partial decision trees . . . . .                               | 20        |
| <b>B</b> | <b>Uniform parameter checks for average-case hardness</b>             | <b>21</b> |
| <b>C</b> | <b>Uniform fields, general circuits, and padding</b>                  | <b>22</b> |
| C.1      | A deterministic field tower . . . . .                                 | 22        |
| C.2      | Layering a circuit without increasing its depth . . . . .             | 23        |
| C.3      | A single family at all lengths . . . . .                              | 23        |
| <b>D</b> | <b>The two parameterized worst-case targets</b>                       | <b>23</b> |
| D.1      | The trilinear function . . . . .                                      | 23        |
| D.2      | The original polynomial evaluator . . . . .                           | 25        |
| <b>E</b> | <b>Further consequences of the decomposition</b>                      | <b>26</b> |
| E.1      | Bounded-width CNFs and monochromatic sets for inverse trace . . . . . | 26        |
| E.2      | The intrinsic list-length requirement . . . . .                       | 26        |
| <b>F</b> | <b>Comparison with the Fourier-tail bound</b>                         | <b>27</b> |

# 1 Introduction

Circuit complexity is one of the most fundamental and well studied areas in theoretical computer science. Once viewed as a promising approach towards proving  $\text{NP} \neq \text{P}$ , the ultimate goal is to find some function in the class  $\text{NP}$  which requires super-polynomial circuit size. Unfortunately, the results remain far from satisfactory. For general fan-in-two Boolean circuits over the full binary basis, Li and Yang [LY22] proved an explicit size lower bound of  $3.1n - o(n)$ , and a recent preprint of Mishra and Santhanam [MS26] reports an improvement to  $3.5n - o(n)$ , despite the fact that a random Boolean function requires exponential circuit size with high probability. On the other hand, we do have exponential lower bounds for restricted circuit classes, and one of the most extensively studied cases is the class of  $\text{AC}^0$ , which captures constant depth circuits with AND and OR gates of unbounded fan-in.

Here, the celebrated result of Håstad [Hås89] (see also [Ajt83, FSS84, Yao85, Raz87, Smol87]) shows that the parity and majority functions both require  $2^{\Omega(n^{1/(d-1)})}$  size depth- $d$   $\text{AC}^0$  circuits. Subsequent work has refined these bounds and developed alternative proofs [HJP95, GRSS23, Kor26, KR26]. For parity, this is well known to be optimal, i.e., there exists a size  $2^{O(n^{1/(d-1)})}$  depth- $d$   $\text{AC}^0$  circuit that computes parity. For majority, this was not known until the recent result of Lecomte and Ramakrishnan [LR26], which constructed depth- $d$   $\text{AC}^0$  circuits of size  $2^{O(n^{1/(d-1)})}$  for every symmetric function. Hence, the bound is also optimal for majority, and in particular, no symmetric function can break this bound.

Breaking this barrier, and proving stronger lower bounds for  $\text{AC}^0$  circuits has since been one of the central open problems in circuit complexity. This question is important both in its own right and because of its connections to general circuit lower bounds. For example, Valiant [Val77, Val83] showed that any function computed by a linear size Boolean circuit of fan-in two and logarithmic depth can also be computed by a depth-three  $\text{AC}^0$  circuit of size  $2^{O(n/\log \log n)}$ , so an explicit function with a depth-three  $\text{AC}^0$  lower bound of  $2^{\omega(n/\log \log n)}$  would also give the first superlinear size lower bound for logarithmic depth general Boolean circuits. We refer the reader to [Vio09, GKW21] for further discussions of the connections between  $\text{AC}^0$  lower bounds and general circuit lower bounds.

Four decades after Håstad’s result, a recent paper by OpenAI [OAI26] breaks the depth three barrier, and gives an explicit function that requires OR–AND–OR circuits of size  $2^{\omega(\sqrt{n})}$ . As observed by Chukhin [Chu26], their proof implicitly gives the quantitative bound of  $2^{\Omega(\sqrt{n} \log \log n / \log \log \log n)}$ . Subsequently, Chukhin [Chu26] improved the result and obtained a lower bound of

$$2^{\Omega_d((n \log n / \log \log n)^{1/(d-1)})} \tag{1.1}$$

at every fixed depth  $d \geq 3$  for a particularly simple trilinear function.

In this paper, we further improve Chukhin’s result and obtain stronger lower bounds.

## 1.1 Results

Without loss of generality, we consider unbounded-fan-in AND/OR circuits with negations only at the inputs. This at most doubles the size of the  $\text{AC}^0$  circuit. Size counts all AND and OR gates, including bottom-layer gates; input negations are free. Depth is the largest number of gates on an input-to-output path. Arbitrary fan-out is allowed, so subcircuits may be shared. We obtain both worst case and average case hardness results. For average case hardness, we define the correlation of two Boolean functions  $F, C$  on  $n$  bits to be

$$\text{Corr}(F, C) = \left| \mathbf{E}_x (-1)^{F(x)+C(x)} \right|.$$

Thus the absolute deviation of the agreement probability from  $1/2$  is  $\text{Corr}(F, C)/2$ . All logarithms are base two unless written  $\ln$ .

**Worst-case hardness.** For a fixed binary basis of  $E = \mathbb{F}_{2^N}$ , let

$$I_N(x) = \text{Tr}_{E/\mathbb{F}_2}(\text{inv}_0(x)), \quad \text{inv}_0(x) = \begin{cases} x^{-1}, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

Thus  $I_N$  is the trace component of the inverse map, with inversion extended by  $\text{inv}_0(0) = 0$ . At  $N = 2^j$  we use an explicit quadratic tower; at other lengths we pad from the largest such  $N$ . Denote the resulting family by  $F_n$ . This family is fixed independently of the circuit depth and size.

**Theorem 1.1** (Worst-case lower bounds). *For every fixed  $d \geq 3$ , each of the following polynomial-time Boolean families requires depth-at-most- $d$  circuits of size*

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

where  $n$  counts all input bits:

1. the padded inverse-trace family  $F_n$ ;
2. the Goldreich–Tal trilinear function [GT18]

$$T_a(x, y, z) = \sum_{0 \leq i, j < a} z_{i+j} x_i y_j \pmod{2}, \quad n = 4a - 1;$$

3. the polynomial evaluator of OpenAI [OAI26], defined explicitly in [Appendix D.2](#), with its original hash dimension and polynomial degree.

The coefficient input  $z$  in the trilinear function is part of the input. Likewise the evaluator’s hash, modulus, and polynomial coefficients are counted. Hard parameter settings can be selected nonconstructively in a lower-bound proof without changing the uniform algorithm computing the full function. At depth three the lower bound is  $2^{\Omega(\sqrt{n \log n})}$ .

**Average-case hardness.** The inverse-trace family has an additional property that permits control of arbitrary circuit correlation, uniformly from polynomial size to a subexponential size range.

**Theorem 1.2** (Correlation under the uniform distribution). *For every fixed  $d \geq 3$  there are constants  $c_d, \eta_d > 0$  such that, for every sufficiently large  $n$ , every depth-at-most- $d$  circuit  $C$  of size at most  $S$  satisfies*

$$n \leq S \leq 2^{c_d n^{1/(d-1)}} \implies \text{Corr}(F_n, C) \leq 2^{-\eta_d n \log \log S / (\log S)^{d-1}}. \quad (1.2)$$

This improves the classical correlation benchmark of parity in [Hås14] by a factor of  $\log \log S$  in the exponent. For  $S = n^B$ , with  $B \geq 1$  fixed, the exponent in Eqn. (1.2) is  $\Omega_{d,B}(n \log \log n / (\log n)^{d-1})$ . For  $S = 2^{n^\alpha}$  and fixed  $0 < \alpha < 1/(d-1)$ , it is  $\Omega_{d,\alpha}(n^{1-\alpha(d-1)} \log n)$ . For example, depth-three circuits of size  $2^{n^{2/5}}$  have correlation at most  $2^{-\Omega(n^{1/5} \log n)}$ .

Tal’s Fourier-tail theorem [Tal17], together with the uniform bound on the Fourier coefficients of inverse trace, also gives the comparison bound  $2^{-\Omega_d(n/(\log S)^{d-1})}$  for inverse trace. Our bound gains a factor  $\log \log S$  in this exponent; the comparison is proved in [Appendix F](#). This comparison concerns the bound obtained from Tal’s theorem; we do not claim to subsume all previous correlation bounds. Also, the size range in [Theorem 1.2](#) is smaller than the worst-case threshold in [Theorem 1.1](#). The latter does not follow by substituting its threshold into Eqn. (1.2).

**Explicit upper bounds for inverse trace.** The same inverse-trace family also admits subexponential-size circuits at sufficiently large fixed depths. Write  $\text{size}_d(G)$  for the minimum number of AND/OR gates in a depth-at-most- $d$  circuit computing  $G$ , with free input negations and arbitrary sharing. For a triple  $\mathbf{h} = (h_1, h_2, h_3)$  of positive integers, put

$$\Phi_{\mathbf{h}}(N) = N^{1/h_1}(\log N)^{1-1/h_1} + N^{1/h_2} \log N + N^{2/h_3}.$$

Let  $U_d(N)$  be the minimum of  $N$  and these quantities over all such triples with  $h_1 + h_2 + h_3 + 1 \leq d$ ; if  $d = 2, 3$ , set  $U_d(N) = N$ .

**Theorem 1.3** (Nonuniform upper bounds). *For every fixed integer  $d \geq 2$ , inverse trace  $I_N$  in any fixed binary basis has circuits satisfying*

$$\text{size}_d(I_N) \leq 2^{O_d(U_d(N))}. \quad (1.3)$$

In particular,

$$\text{size}_8(I_N) \leq 2^{O(N^{2/3})}, \quad \text{size}_9(I_N) \leq 2^{O(\sqrt{N} \log N)}. \quad (1.4)$$

More generally, for every fixed integer  $h \geq 1$ ,

$$\text{size}_{4h+1}(I_N) \leq 2^{O_h(\min\{N, N^{1/h} \log N\})}. \quad (1.5)$$

The same estimates hold when wires are counted, and their constants are independent of the chosen basis. They also hold for the padded family  $F_n$  with  $n$  in place of  $N$ .

Together with [Theorem 1.1](#), this places the exact circuit complexity of one fixed explicit family between

$$2^{\Omega_d((n \log n)^{1/(d-1)})} \leq \text{size}_d(F_n) \leq 2^{O_d(U_d(n))}, \quad d \geq 3. \quad (1.6)$$

The upper bound is subexponential at every fixed depth  $d \geq 8$ . There remains a gap with the lower bound; at depths three and four, this construction gives only the full-DNF exponential estimate. We do not claim that the upper bounds are optimal or that depth eight is the first depth admitting subexponential circuits.

The proof uses the evaluation and interpolation approach to finite-field arithmetic of Healy and Viola [\[HV05\]](#). We implement three stages directly at constant depth: linear evaluation followed by logarithm tables, multiplication of the evaluated factors, and a final parity. Each stage can be viewed as a computation with few state bits, and enumerating intermediate states gives an adjustable depth–size tradeoff. Choosing the gate orientations at the two stage boundaries saves two layers. [Section 7](#) gives the construction and its depth accounting. All final gates are ordinary AND/OR gates, with negations only at the inputs.

## 1.2 Proof Overview

We prove our lower bounds by establishing the following main technical theorem.

**The structural theorem.** Given a nonempty list  $A$  of points of  $\{0, 1\}^m$ , we define its width- $b$  CNF closure to be

$$\text{cl}_b(A) = \{x : x|_U \in \{a|_U : a \in A\} \text{ for every } U \subseteq [m], |U| \leq b\}. \quad (1.7)$$

In other words, a string  $x$  belongs to  $\text{cl}_b(A)$  exactly when *every* local pattern of size at most  $b$  exhibited by  $x$  is exhibited by at least one member of  $A$ .

We first note that  $\text{cl}_b(A)$  is the set of satisfying assignments of a width  $b$  CNF. Indeed, for a subset  $I \subseteq [m]$  define the projection  $\pi_I : \pi_I(x) = x|_I$  and  $\pi_I(A) = \{a|_I : a \in A\}$ . Then for any  $z \in \{0, 1\}^I$  such that  $z \notin \pi_I(A)$ , any  $x \in \text{cl}_b(A)$  must satisfy that  $\pi_I(x) \neq z$ . Hence, let

$$C_{I,z}(x) = \bigvee_{i \in I} (x_i \neq z_i), \quad (1.8)$$

then

$$\mathbf{1}_{\text{cl}_b(A)}(x) = \bigwedge_{\substack{I \subseteq [m], |I| \leq b \\ z \in \{0,1\}^I \setminus \pi_I(A)}} C_{I,z}(x). \quad (1.9)$$

It is also not hard to see that  $\text{cl}_b(A)$  is the *smallest satisfying assignment set* of any width- $b$  CNF that contains every string in  $A$ . In this sense, we can use a list  $A$  to describe a CNF, without listing its clauses. This is particularly useful because the CNF can have a large number of clauses.

**Theorem 1.4** (Point-list decomposition, informal form). *For every fixed  $\varepsilon > 0$ , every width- $b$  CNF on  $m \geq 1$  variables is an exact disjoint union of at most  $2^{\varepsilon m}$  sets  $\text{cl}_b(A_i)$ , where*

$$|A_i| \leq 2^{O_\varepsilon(b)} \log(m+1).$$

*No bound on the number of clauses in a piece, or on the time to find the decomposition, is asserted.*

On a high level, our proof of lower bounds follows the same framework as in [Chu26] and [OAI26], by first reducing the problem to bounding correlations with width- $b$  CNFs for an appropriate choice of  $b$ . The key step in the analysis is to make sure that restrictions of the hard function have small correlation with *all* width- $b$  CNFs. However, the number of such CNFs is very large, hence [Chu26] uses the CNF sparsification results developed by Impagliazzo, Paturi, and Zane [IPZ01], and refined by Calabro, Impagliazzo, and Paturi [CIP06] to reduce the case to CNFs with few clauses. The number of such CNFs is much smaller than general width- $b$  CNFs, and therefore a union bound suffices. However, this approach still results in  $b^{O_\varepsilon(b)}m$  clauses, which only permits  $b = \Theta(\log n / \log \log n)$  as in [Chu26].

Here, we instead use our point-list decomposition, so that the problem is reduced to bounding the correlation with all width- $b$  CNFs that are described by a short list. The counting of such lists pays a better price in the union bound, replacing the  $b^{O_\varepsilon(b)}$  dependence from clause sparsification by  $2^{O_\varepsilon(b)}$ , thus allowing  $b = \Theta(\log n)$  even when the pieces have many clauses. Consequently, our theorem does not resolve the algorithmic CNF sparsification problem asking for pieces with only  $2^{O(b)}m$  clauses.

**Why short point lists improve the exponent.** Let  $\kappa_b(g) = \max_H |\mathbf{E}[gH]|$ , where  $H$  ranges over all width- $b$  CNFs and  $g$  is a sign function. The maximum includes the constant-one CNF. Here  $H$  is a  $\{0, 1\}$ -valued indicator:  $\kappa_b$  measures correlation with CNF indicators, whereas Corr uses the  $\{-1, 1\}$  encodings of both Boolean functions. A decomposition into  $2^{\varepsilon m}$  pieces gives

$$\kappa_b(g) \leq 2^{\varepsilon m} \max_{|A| \leq L} |\mathbf{E}[g \mathbf{1}_{\text{cl}_b(A)}]|.$$

There are fewer than  $2^{mL+1}$  lists of length at most  $L$  when  $m \geq 1$ . The simultaneous moment argument therefore pays  $O(mL)$  description bits. With our theorem,  $L = 2^{O_\varepsilon(b)} \log(m+1)$ ; hence widths  $b$  proportional to  $\log n$  remain affordable.

Here is the parameter calculation behind the worst-case result. Write  $\ell = \log S$ . Standard depth reduction leaves a depth-three circuit with bottom fan-in  $k = \Theta_d(\ell)$  and survival probability

$q = \Theta_d(\ell^{-(d-3)})$ . A second restriction of survival  $p = b/(64k)$  transfers width  $k$  to width  $b$  in expected signed coefficient mass. The expected number of free variables after both restrictions is

$$m = \Theta_d\left(\frac{nb}{\ell^{d-2}}\right). \quad (1.10)$$

Moment bounds and point-list counting give expected maximum bounded-width CNF correlation  $2^{-\Omega(m)}$ . An exact circuit covers a constant fraction of the cube by at most  $S^{O_d(1)}$  monochromatic CNFs, forcing  $m = O_d(\ell)$ . Taking  $b = \Theta_d(\log n)$  and solving this relation gives  $\ell = \Theta_d((n \log n)^{1/(d-1)})$ .

The trilinear function and the evaluator in [OAI26] provide moments through random parameter inputs. Inverse trace provides them through translations in a binary field, and Weil bounds for additive character sums. Its rational character sums remain controlled after conditioning on a coordinate subcube, paying explicitly for its codimension. This robustness is used in the average-case proof.

**From exact computation to small correlation.** For an exact circuit with OR output, the satisfying assignments of every CNF child lie in one level set of the target. Its density is therefore an absolute correlation. A circuit that makes errors has no such property: the accepting sets of its CNF children may overlap and contain inputs from both level sets of the target. Bounding each child alone does not bound the top OR's correlation.

We instead switch the entire restricted circuit down to depth two. For a circuit with bottom fan-in  $O(\ell)$ ,  $d - 2$  switching stages followed by CNF width reduction leave an expected number of free variables

$$m = \Theta_d\left(\frac{n \log \ell}{\ell^{d-1}}\right), \quad (1.11)$$

using  $b = \Theta(\log \ell)$ . The switching lemma gives failure probability only  $2^{-\Omega(\ell)}$ , which is insufficient when  $m \gg \ell$ . Common partial decision trees allow a much smaller failure probability  $2^{-\Omega_d(m)}$ .

The cost of a common partial decision tree is paid through an exact expansion. At a leaf, let  $P$  indicate its path and let  $H$  be a residual CNF. Then  $PH$  is still a CNF of the same width: the path contributes unit clauses, irrespective of the path length. A DNF leaf is written as  $P - PH$ . Thus a tree of depth  $R$  gives signed coefficient mass at most  $2^{R+1}$  in bounded-width CNFs. Choosing  $R$  as a sufficiently small depth-dependent fraction of  $m$  leaves an exponentially decaying correlation.

Finally, simply replacing bottom gates of large fan-in by their typical values introduces an error of order  $S2^{-k}$ , again too large when  $m \gg \ell$ . We remove it by a signed cofactor recursion. Each exceptional assignment fixes many coordinates and incurs its full probability. The bounded-width CNF estimate holds uniformly on large coordinate subcubes, so the recursion can continue until its residual probability is  $2^{-\Omega(n)}$ .

**Organization and dependencies.** Sections 2 to 4 prove the point-list theorem and the inverse-trace restriction estimate. Section 5 proves the correlation theorem, with detailed switching parameters and parameter checks in Appendices A to B. Section 6 gives the common worst-case reduction; Appendix D supplies the two other targets. Section 7 gives the complementary nonuniform upper bounds for inverse trace. Section 8 compares these bounds and discusses the limits of the lower-bound method. The external inputs are the switching lemma and multi-switching lemma of Håstad (the latter in Tal's formulation), rational additive-character bounds, and the trilinear restriction moments of Chukhin. Statements and locations are given where used. All other reductions are proved here.

## 2 An exact decomposition by lists of satisfying assignments

A clause is a disjunction of literals, and a CNF is a conjunction of clauses. Its width is the maximum number of variables in a clause. We remove tautological clauses and repeated literals. We identify a CNF with its Boolean indicator or its set of satisfying assignments, as appropriate. The constant-zero and constant-one functions are allowed, represented by an empty clause and an empty conjunction, respectively. The closure in Eqn. (1.7) forbids exactly the coordinate patterns of width at most  $b$  absent from  $A$ .

**Theorem 2.1** (Quantitative point-list partition). *Let  $m \geq 1$ ,  $b \geq 1$  be integers and  $C \geq 2$  a real number. Put*

$$\varepsilon_C = h_2(1/C) + 1/C, \quad L_C(m, b) = \left\lceil 2^{Cb} [b \ln(2m+1) + 1] \right\rceil,$$

*where  $h_2(u) = -u \log u - (1-u) \log(1-u)$ . Every width- $b$  CNF  $H$  has an exact disjoint decomposition*

$$\mathbf{1}_H = \sum_{i=1}^R \mathbf{1}_{\text{cl}_b(A_i)}, \quad R \leq 2^{\varepsilon_C m}, \quad 1 \leq |A_i| \leq L_C(m, b). \quad (2.1)$$

*Each  $A_i$  is a list of satisfying assignments of  $H$ . The empty set has the empty decomposition. For  $m = 0$  the assertion holds with one singleton list for the nonempty cube.*

*Proof.* Fix a deterministic order of partial assignments on at most  $b$  coordinates. At a nonempty current set  $S$ , query the first pattern  $\rho$  with

$$0 < \mathbf{Pr}_{X \sim U_S}[X \text{ extends } \rho] < 2^{-Cb},$$

if one exists. Split  $S$  into the true child  $S \cap [\rho]$  and the false child  $S \setminus [\rho]$ . Both children are nonempty and smaller than  $S$ . The true child adds unit clauses; the false child adds the clause forbidding  $\rho$ . Every state remains a width- $b$  CNF on the original  $m$  coordinates. The process terminates and its leaves partition  $H$ .

Every true branch decreases  $\log |S|$  by more than  $Cb$ . Hence a nonempty terminal path has at most  $m/(Cb)$  true branches. Let  $\sigma$  be the union of their partial assignments. It is consistent, every terminal satisfying assignment extends it, and  $|\text{dom } \sigma| \leq m/C$ . Here  $\text{dom } \sigma$  means the domain of the partial assignment  $\sigma$ .

Distinct leaves have distinct  $\sigma$ . At their first divergence, one takes the true branch of a pattern  $\rho$ . Its fingerprint  $\sigma$  extends  $\rho$ . If the other leaf had the same fingerprint, all its satisfying assignments would extend  $\rho$ , contrary to its false branch. Thus one partial assignment records enough information to distinguish the leaves; neither query order nor negative answers need be stored. The leaf count is at most

$$\sum_{j \leq \lfloor m/C \rfloor} 2^j \binom{m}{j} \leq 2^{m/C + mh_2(1/C)}.$$

We used the binomial entropy estimate  $\sum_{j \leq r} \binom{m}{j} \leq 2^{mh_2(r/m)}$  for integer  $0 \leq r \leq m/2$  and monotonicity of  $h_2$  on  $[0, 1/2]$ .

At a terminal set  $J$ , every occurring pattern on at most  $b$  coordinates has probability at least  $\theta = 2^{-Cb}$ . There are at most  $(2m+1)^b$  such patterns: encode the sorted literals and pad the remaining slots. With  $L = L_C(m, b)$  independent uniform samples from  $J$ , the probability of missing any occurring pattern is at most

$$(2m+1)^b e^{-L\theta} \leq e^{-1} < 1.$$

Therefore we can choose a covering list  $A$  with  $|A| \leq L$ . Every local pattern of a point of  $J$  is in  $A$ , so  $J \subseteq \text{cl}_b(A)$ . Conversely, a point outside  $J$  violates one of its width- $b$  clauses. That falsifying pattern occurs in no satisfying assignment of  $J$ , hence in no row of  $A$ , and the point is outside  $\text{cl}_b(A)$ . Thus  $J = \text{cl}_b(A)$  exactly.  $\square$

Since  $\varepsilon_C \rightarrow 0$ , the theorem implies [Theorem 1.4](#). We will use

$$\varepsilon_{512} < 1/32, \quad \varepsilon_{2048} < 1/128, \quad (2.2)$$

which follow from  $h_2(u) \leq u \log(e/u)$ . Lists of lengths one through  $L$  define fewer than  $2^{mL+1}$  tests for  $m \geq 1$ , regardless of their clause counts.

**A small example.** For  $b = 1$ , the closure retains exactly the coordinate values present in the rows. The list  $A = \{000, 110\}$  has closure  $\{000, 010, 100, 110\}$ : the first two bits are unrestricted and the last is zero. For  $b = 2$ , the same list has closure  $\{000, 110\}$ , since the first two bits must agree. The width parameter specifies which local patterns a list must preserve.

The decomposition also adapts to the number of satisfying assignments.

**Corollary 2.2** (Density refinement). *If  $H \neq \emptyset$  and  $h = \log |H|$ , the partition can be chosen with*

$$\log R \leq B_C(h) := mh_2\left(\frac{h}{Cm}\right) + \frac{h}{C}.$$

*If every allowed point-list test  $J$  satisfies  $|\mathbf{E}[gJ]| \leq \beta\sqrt{\mu_J}$ , where  $\mu_J = \mathbf{E}J$ , then*

$$|\mathbf{E}[gH]| \leq \beta 2^{B_C(h)/2} \sqrt{\mu_H}.$$

*Proof.* The logarithmic cardinality budget starts at  $h$ , so each fingerprint has at most  $h/C$  fixed coordinates. Count as above. Disjointness and Cauchy–Schwarz give  $\sum_i \sqrt{\mu_{J_i}} \leq \sqrt{R\mu_H}$ .  $\square$

### 3 Restriction transfer without a clause-count loss

For a real function  $G$  define

$$\text{Mass}_b(G) = \inf \left\{ \sum_i |c_i| : G = \sum_i c_i J_i, \quad J_i \text{ width-}b \text{ CNFs} \right\}.$$

Equivalently,  $\text{Mass}_b(G)$  is the minimum  $\ell_1$  norm of the coefficient vector over all exact expansions into width- $b$  CNFs. It is the quantity denoted  $\text{size}_b(G)$  by Chukhin [[Chu26](#), Section 2]. Then  $|\mathbf{E}[gG]| \leq \text{Mass}_b(G) \kappa_b(g)$ . Multiplication by a conjunction of unit clauses does not increase this mass. A  $p$ -random restriction independently keeps a variable free with probability  $p$  and otherwise fixes it to a fair bit. Composition of independent  $q$ - and  $p$ -restrictions has the  $qp$  product distribution.

**Lemma 3.1** (Expected CNF mass, Chukhin [[Chu26](#)]). *If  $H$  is a width- $k$  CNF,  $k \geq b \geq 1$ , and*

$$\vartheta = \sum_{j>b} \binom{k}{j} \left( \frac{2p}{1-p} \right)^j \leq 1,$$

*then  $\mathbf{E}_p \text{Mass}_b(H_p) \leq 1$ . In particular this holds for  $p = b/(64k)$ .*

*Proof.* We include the mass argument to make its independence of the clause count explicit. Order the clauses, and let  $H_i$  be the conjunction of the first  $i$ . For the next clause  $D$ , call it wide if no literal is fixed true and more than  $b$  variables remain free. Let  $v_D$  be the conjunction falsifying the remaining literals, and let  $\rho_D$  extend  $\rho$  by these assignments. On a wide restriction,

$$(H_i)_\rho = (H_{i-1})_\rho - v_D(H_{i-1})_{\rho_D}.$$

The last cofactor is extended to the original cube of free variables by ignoring its additional fixed coordinates. The mass is at most the sum of the two previous masses. If  $\rho$  falsifies  $D$ , the new mass is zero. In every other nonwide case, adding  $D_\rho$  to each summand does not increase mass.

Each preimage of a restriction  $\sigma$  falsifying  $D$  is obtained by freeing  $j > b$  of its at most  $k$  clause variables. Its product probability is  $(2p/(1-p))^j$  times that of  $\sigma$ . Summing the extra wide-case mass therefore costs at most  $\vartheta$  times the previous mass on restrictions falsifying  $D$ , precisely the mass removed in that case. Expected mass cannot increase as clauses are added. It starts at one for  $H_0 = 1$ .

For  $p = b/(64k)$ ,  $2p/(1-p) \leq 4p$ , and each summand with  $j > b$  is at most  $(eb/(16j))^j \leq 4^{-j}$ . Their sum is below one.  $\square$

**Lemma 3.2** (A simultaneous good event). *Let  $k \geq b \geq 1$  be integers and let  $\gamma, \Delta \geq 0$ . Let  $\phi$  have any distribution on outer restrictions, and conditional on  $\phi$  let  $\rho$  be a fresh  $p$ -restriction with  $p = b/(64k)$ . If  $|g| \leq 1$  and  $\kappa_b(g_{\phi\rho}) \leq \gamma$  outside a joint event of probability at most  $\Delta$ , then*

$$\mathbf{E}_\phi \kappa_k(g_\phi) \leq \gamma + \Delta.$$

*Proof.* Fix  $\phi$  and a width- $k$  CNF  $H$  before drawing  $\rho$ . Averaging a restriction and filling its free variables reproduces the uniform input distribution. Thus

$$\begin{aligned} |\mathbf{E}[g_\phi H]| &\leq \mathbf{E}_\rho |\mathbf{E}[g_{\phi\rho} H_\rho]| \\ &\leq \gamma \mathbf{E}_\rho \text{Mass}_b(H_\rho) + \mathbf{Pr}_\rho[\text{bad} \mid \phi] \\ &\leq \gamma + \mathbf{Pr}_\rho[\text{bad} \mid \phi]. \end{aligned}$$

On a bad restriction we use  $|\mathbf{E}[g_{\phi\rho} H_\rho]| \leq 1$ . The right side is independent of  $H$ , so we can maximize over  $H$  and then average  $\phi$ .  $\square$

The order matters: the resulting CNF may depend on all outer circuit restrictions. It is selected before the fresh inner restriction used in [Lemma 3.2](#). We never assume independence between the good event and coefficient mass.

## 4 Inverse trace against every restricted CNF

Let  $E = \mathbb{F}_{2^N}$  with a fixed binary basis,  $\psi(x) = (-1)^{\text{Tr}(x)}$ , and  $f(x) = \psi(c \text{inv}_0(x))$  for  $c \neq 0$ . Inverse trace corresponds to  $c = 1$ . A coordinate subcube  $V = x_0 + W$  fixes some basis coordinates; its codimension  $b_0$  is the number fixed. Expectations on subcubes are normalized.

**Lemma 4.1** (Additive-character sums for products of shifts). *For distinct  $u_1, \dots, u_h \in E$ ,  $h \geq 1$ , and every  $a \in E$ ,*

$$\left| \mathbf{E}_{x \in E} \psi(ax) \prod_{i=1}^h f(x + u_i) \right| \leq 8h 2^{-N/2}. \quad (4.1)$$

If  $u_i \in W$  and  $V = x_0 + W$  has codimension  $b_0$ , then

$$\left| \mathbf{E}_{x \in V} \prod_{i=1}^h f(x + u_i) \right| \leq 8h 2^{b_0 - N/2}. \quad (4.2)$$

*Proof.* Off its poles the summand in Eqn. (4.1) is  $\psi(r(x))$  for

$$r(X) = aX + \sum_{i=1}^h \frac{c}{X + u_i}.$$

Its finite poles are simple with nonzero residues. It cannot be  $R^2 - R$  over the algebraic closure, since every pole of such a nonconstant expression has even order. Apply the rational additive-character estimate, for example Fu–Wan [FW25, Theorem 4.6, version 3], with extension degree one, trivial multiplicative character on  $\prod_i (X + u_i)$ , and additive argument  $r$ . In their notation  $D_1 = D_3 = h$ ,  $D_4 = 0$ , and  $D_2 \leq 1$ , giving an unnormalized bound at most  $2h 2^{N/2}$  off the poles. Restoring the at most  $h$  values at the poles under our convention  $\text{inv}_0(0) = 0$  proves Eqn. (4.1) with slack.

Let  $W^\perp$  be the annihilator of  $W$  under the nondegenerate trace pairing. Orthogonality gives

$$\mathbf{1}_V(x) = 2^{-b_0} \sum_{a \in W^\perp} \psi(a(x - x_0)).$$

Normalized conditioning is therefore a sum of  $2^{b_0}$  twisted full-field expectations. Apply Eqn. (4.1) to each.  $\square$

**Lemma 4.2** (Even moments under random translation). *Let  $L_0 : \mathbb{F}_2^v \rightarrow W$  be injective and let  $J$  be a Boolean indicator of density  $\mu$ . For every integer  $t \geq 1$ ,*

$$\mathbf{E}_{A \sim U_V} |\mathbf{E}_z f(A + L_0 z) J(z)|^{2t} \leq (2t - 1)!! (\mu 2^{-v})^t + 16t 2^{b_0 - N/2} \mu^{2t}. \quad (4.3)$$

*Proof.* Expand over  $2t$  independent uniform points  $z$ . Tuples in which each point has even multiplicity are covered by the  $(2t - 1)!!$  pairings of positions. Each pairing has total  $J$ -weight  $(\mu 2^{-v})^t$ . Every other tuple leaves a nonempty set of at most  $2t$  distinct shifts of odd multiplicity. Apply Eqn. (4.2); all tuple weights are nonnegative and their total is  $\mu^{2t}$ .  $\square$

The paired term behaves like a moment bound for limited independence. The second term is the character-sum error term. Our list count must fit within the exponential bound supplied by the latter.

**Proposition 4.3** (Expected maximum CNF correlation on large subcubes). *Fix a coordinate subcube  $V$  of codimension  $b_0 \leq N/4$  and dimension  $v_0 = N - b_0$ . Let  $0 < q \leq 1$  be deterministic and let  $k \geq b \geq 2$  be integers. Set*

$$p = \frac{b}{64k}, \quad m = v_0 q p, \quad L = \left\lceil 2^{512b} [b \ln(4m + 1) + 1] \right\rceil. \quad (4.4)$$

If

$$m \geq 2b, \quad m \geq 16 \log(8L), \quad mL \leq N/64, \quad (4.5)$$

then for a  $q$ -random restriction  $\phi$  of  $V$ ,

$$\begin{aligned} \mathbf{E}_\phi \kappa_k(f_{V,\phi}) &\leq 2^{-3m/64} + \Delta, \\ \Delta &\leq 2 \cdot 2^{-m/8} + 2^{1-3mL/4} + 128L 2^{-3N/16}. \end{aligned} \quad (4.6)$$

The maximum over every width- $k$  CNF is taken before averaging  $\phi$ .

*Proof.* Draw a fresh inner  $p$ -restriction  $\rho$ . The number  $v$  of free variables under  $\sigma = \phi\rho$  has expectation  $m$ . Chernoff bounds give  $v \in [m/2, 2m]$  except with probability at most  $2e^{-m/8} \leq 2 \cdot 2^{-m/8}$ .

Fix a restriction whose number of free variables lies in this interval. First translate the target by a uniform element of  $W$ ; its offset becomes uniform in  $V$ . In [Lemma 4.2](#) take  $t = 4L$  and threshold  $\beta = 2^{-v/8}$ . Union over fewer than  $2^{vL+1}$  list tests and use  $(2t-1)!! \leq (2t)^t$ . Their simultaneous failure probability is at most

$$2^{1-2vL+4L \log(8L)} + 128L 2^{b_0-N/2+2vL} \leq 2^{1-3vL/2} + 128L 2^{b_0-N/2+2vL}, \quad (4.7)$$

because  $v \geq 8 \log(8L)$ . The list-length bound  $L$  dominates  $L_{512}(v, b)$ . On success, [Theorem 2.1](#) and Eqn. (2.2) imply

$$\kappa_b(f \text{ on this subcube}) \leq 2^{v/32} \beta = 2^{-3v/32} \leq 2^{-3m/64}.$$

The second term of Eqn. (4.7) is at most  $128L 2^{-3N/16}$ , since  $b_0 \leq N/4$  and  $2vL \leq 4mL \leq N/16$ . The first is at most  $2^{1-3mL/4}$ .

We now remove the translation average. Translation within  $W$  flips the unfixed binary coordinates of  $V$ . It preserves the product distribution of random restrictions and maps the class of all width- $b$  CNFs on the surviving bits to itself. Thus the bad-event probability just bounded is the same for each fixed translate of the target. Its average bound holds for the untranslated target as well. This does not say that every small subcube is good. It gives a joint good event for  $(\phi, \rho)$  under their unconditional product distribution. Apply [Lemma 3.2](#).  $\square$

The case  $V = E$  will suffice for worst-case hardness. The uniformity over initial subcubes of codimension up to  $N/4$  is needed to remove the restriction on bottom fan-in in the correlation argument.

## 5 Controlling the whole circuit

We first work at a tower length  $N$  with  $f = (-1)^{I_N}$ . Since inversion permutes  $E$  and trace is a nonzero linear functional,  $\mathbf{E}f = 0$ . Consequently, for Boolean  $C$ ,

$$\text{Corr}(I_N, C) = 2|\mathbf{E}[fC]|. \quad (5.1)$$

We prove bounds on the right, including bounds on subcubes where  $f$  need not be balanced.

### 5.1 Guarded CNFs and common trees

**Lemma 5.1** (Guarding leaves preserves width). *If a Boolean function  $G$  has a restriction tree of depth at most  $R$ , with each residual leaf a width- $k$  CNF or DNF, then*

$$\text{Mass}_k(G) \leq 2^{R+1}, \quad |\mathbf{E}[gG]| \leq 2^{R+1} \kappa_k(g).$$

*Proof.* Let  $P_\lambda$  be the conjunction of literals specifying the root-to-leaf path. We call the product  $P_\lambda H_\lambda$  a *guarded CNF*. A CNF leaf contributes  $P_\lambda H_\lambda$ . For a DNF leaf write its value as  $1 - H_\lambda$  with  $H_\lambda$  a CNF, and contribute  $P_\lambda - P_\lambda H_\lambda$ . Extend residual functions by ignoring path coordinates. All atoms are width- $k$  CNFs, since a path is a conjunction of units. Paths partition the cube and each of at most  $2^R$  leaves contributes at most two atoms.  $\square$

We use the following switching inputs. A width- $k$  CNF or DNF under a  $p$ -restriction has a decision tree of depth at most  $t$  except with probability  $(5pk)^t$  [Hås89]. It then has both width- $t$  forms with at most  $2^t$  terms or clauses. Håstad's multi-switching lemma [Hås14], in the formulation of Tal [Tal17, Definition 14 and Lemma 15], states that a family of  $M$  depth-two circuits of bottom fan-in at most  $k$  has, except with probability  $M(24pk)^D$ , a common  $\lceil \log(2M) \rceil$ -partial decision tree of depth at most  $D$ . At each leaf, each member has an ordinary decision tree of the stated residual depth. We use the constant 24 from the cited formulation.

Here and below, circuits are initially alternating and layered. Constants and unary gates are retained, and original layer labels are retained under cofactors. These conventions keep the circuit class closed under the operations in the proof. Appendix C normalizes general circuits at polynomial size cost.

**Proposition 5.2** (Two switching estimates). *Fix  $d \geq 3$ ,  $S \geq N$ ,  $\ell = \log S$ , and  $s = d - 2$ . For layered alternating circuits of depth at most  $d$ , size at most  $S$ , and bottom fan-in at most*

$$k_0 = \lceil 4 \log(2S) \rceil,$$

*there are deterministic parameters  $k = \Theta_d(\ell)$  and  $q = \Theta_d(\ell^{-s})$  with the following properties. For every initial subcube  $V$  and  $|g| \leq 1$ ,*

$$|\mathbf{E}_V[gC]| \leq s2^{-3\ell} + 2\mathbf{E}_\phi \kappa_k(g_{V,\phi}). \quad (5.2)$$

*Also, for any positive integer  $D_0$ , with  $R_s = (2^s - 1)D_0$  and  $A = 6^d$ ,*

$$|\mathbf{E}_V[gC]| \leq s2^{A\ell - 2D_0} + 2^{R_s + 1} \mathbf{E}_\phi \kappa_k(g_{V,\phi}). \quad (5.3)$$

*Here  $\phi$  has the  $q$ -random restriction distribution. It is drawn even after simplification failures; neither  $q$  nor  $k$  depends on a successful path.*

The full construction is in Appendix A. Its key feature is that  $s$  switching stages use fixed survival probabilities  $\Theta_d(1/\ell)$ . With common trees the depth bound at stage  $i$  pays for all previous leaves, yet the final tree depth stays at most  $(2^s - 1)D_0$ . Lemma 5.1 then gives Eqn. (5.3). At no point do we assert a product distribution of random restrictions after conditioning on a successful leaf.

## 5.2 Circuits with bounded bottom fan-in

Define

$$\mathcal{R} = \frac{N \log \ell}{\ell^{d-1}}.$$

Take  $b = \lfloor \log k / 2048 \rfloor$  and  $p = b / (64k)$ . On any initial subcube of codimension less than  $N/4$ , the expected number of free variables in Proposition 4.3 is

$$m = (\dim V)qp = \Theta_d(\mathcal{R}).$$

For a sufficiently small  $c_* > 0$ , uniformly in

$$\log N \leq \ell \leq c_* N^{1/(d-1)}, \quad (5.4)$$

the hypotheses in Eqn. (4.5) hold and

$$\mathbf{E}_\phi \kappa_k(f_{V,\phi}) \leq 5 \cdot 2^{-3m/64}. \quad (5.5)$$

Indeed the list-length bound is  $L = O_d(\ell^{1/4} \log \ell \log N)$ ,  $m$  is at least a sufficiently large multiple of  $\log \ell$ , and  $mL = o(N)$  even at  $\ell = \log N$ . [Appendix B](#) checks this uniformly, including both size endpoints.

When  $m$  is at most a sufficiently large depth-dependent multiple of  $\ell$ , use Eqn. (5.2). Both its terms are  $2^{-\Omega_d(m)}$ . For larger  $m$ , choose  $D_0 = \lfloor m/J \rfloor$  with  $J$  a sufficiently large depth constant. Then  $R_s \leq m/4096$  and the failure term in Eqn. (5.3) is also  $2^{-\Omega_d(m)}$ . Combining the cases proves:

**Proposition 5.3** (Correlation for circuits with bounded bottom fan-in). *There are constants  $c_*, \theta_d > 0$  such that, throughout the range in Eqn. (5.4), every circuit in [Proposition 5.2](#) satisfies*

$$|\mathbf{E}_V[fC]| \leq \Gamma := 2^{-\theta_d \mathcal{R}}$$

on every coordinate subcube  $V$  of codimension less than  $N/4$ .

### 5.3 Removing the restriction on bottom fan-in

The following lemma replaces an additive truncation error by recursion through cofactors. It is useful precisely because [Proposition 5.3](#) holds on every large initial subcube.

**Lemma 5.4** (Signed cofactor transfer). *Let  $|g| \leq 1$  on  $N$  coordinates. Suppose all layered circuits of depth at most  $d$ , size at most  $S$ , and bottom fan-in at most  $k$  satisfy  $|\mathbf{E}_V[gC]| \leq \Gamma$  on every coordinate subcube  $V$  of codimension less than an integer  $B \leq N$ . If*

$$a_0 = 2S2^{-k} < 1, \quad 2S2^{-k/2} \leq 1,$$

then the same circuits with unrestricted bottom fan-in satisfy

$$|\mathbf{E}[gC]| \leq \frac{\Gamma}{1 - a_0} + 2^{-B/2}.$$

*Proof.* Let  $B_b$  be the maximum of  $|\mathbf{E}_V[gC]|$  over all subcubes  $V$  with  $b$  fixed coordinates and all circuits  $C$  in the class with unrestricted bottom fan-in. On a subcube with  $b < B$ , list its bottom gates whose fan-ins  $w_i$  exceed  $k$ , removing repetitions and simplifying contradictory literals first. Replace each OR by one and each AND by zero, in sequence. The final circuit has bottom fan-in at most  $k$ . Gate  $i$  differs from its replacement only on the coordinate subcube on which all its literals are false (for an OR gate) or all are true (for an AND gate), of relative measure  $2^{-w_i}$ .

On that subcube the circuit difference is a difference of two Boolean cofactor circuits, each of depth at most  $d$  and size at most  $S$ . Sharing the replaced gate among several parents does not duplicate either cofactor circuit. Telescoping therefore gives

$$B_b \leq \Gamma + \sup_C 2 \sum_i 2^{-w_i} B_{b+w_i}. \quad (5.6)$$

There is no first-exception prefix condition in this identity.

Descending induction on  $b$  gives

$$B_b \leq \frac{\Gamma}{1 - a_0} + 2^{-(B-b)/2}.$$

For  $b \geq B$  the right side is at least one. For  $b < B$ , the constant contribution from Eqn. (5.6) is at most  $\Gamma + a_0\Gamma/(1 - a_0)$ . The remaining contribution is at most

$$2^{-(B-b)/2} 2 \sum_i 2^{-w_i/2} \leq 2^{-(B-b)/2}.$$

Each recursive call fixes fresh coordinates, so the induction is well founded. Set  $b = 0$ .  $\square$

Apply the lemma with  $k = k_0$  and  $B = \lfloor N/4 \rfloor$ . Then  $a_0 < 1/2$  and the second hypothesis holds. [Proposition 5.3](#) yields

$$|\mathbf{E}[fC]| \leq 2 \cdot 2^{-\theta_d \mathcal{R}} + 2^{-\lfloor N/4 \rfloor/2} \leq 2^{-\theta'_d \mathcal{R}}.$$

Here  $\mathcal{R} = o(N)$  uniformly over the range in Eqn. (5.4), and its minimum in that range tends to infinity. This proves the correlation estimate for layered circuits at tower lengths. Circuit normalization costs  $O_d(S_0^2)$  gates, which we absorb using budget  $S = S_0^3$ . Eqn. (5.1) and padding from  $N$  to  $n < 2N$  change only depth-dependent constants. The uniform field construction, normalization, and padding details are in [Appendix C](#); they complete [Theorem 1.2](#).

## 6 Worst-case hardness through monochromatic covers

For exact computation we can stop depth reduction one layer earlier. We use Håstad's depth reduction in the form stated by Chukhin [[Chu26](#), Lemma 2.3]: for fixed  $d \geq 3$  and  $S \geq M \geq 2$ , there are common parameters

$$k = \Theta_d(\log S), \quad q = \Theta_d((\log S)^{-(d-3)})$$

such that a  $q$ -restriction of a size- $S$ , depth-at-most- $d$  circuit with OR output is an OR of at most  $S^{A_d}$  width- $k$  CNFs with probability at least  $3/4$ . The same parameters work for all such circuits on  $M$  bits.

A CNF is *monochromatic* for a target if the target is constant on its set of satisfying assignments.

**Lemma 6.1** (Covering by monochromatic CNFs). *Let  $G$  be Boolean,  $g = (-1)^G$ , and suppose both level sets of  $G$  have density at least  $\delta$ . If a size- $S$ , depth-at-most- $d$  circuit computes  $G$ , then for the parameters above,*

$$\delta \leq \frac{1}{4} + S^{A_d} \mathbf{E}_\phi \kappa_k(g_\phi).$$

*Proof.* Complement all gates and literals if needed to give an OR output computing  $G$  or  $1 - G$ . On a successful depth reduction, the satisfying assignments of each top CNF lie in the corresponding level set of  $G$ . Its density equals its absolute correlation with  $g_\phi$ . Sum these densities over the at most  $S^{A_d}$  children. On failure use one, then average  $\phi$ . Restriction averaging preserves the unconditional output density.  $\square$

**Inverse trace.** At a tower length  $N$ , put  $\ell = c(N \log N)^{1/(d-1)}$ ,  $S = 2^\ell$ , and

$$b = \left\lfloor \frac{\log N}{8192(d-1)} \right\rfloor, \quad p = \frac{b}{64k}, \quad m = Nqp.$$

Then

$$m = \Theta_d(c^{-(d-2)}(N \log N)^{1/(d-1)}), \quad L \leq N^{1/[16(d-1)]} O_d((\log N)^2).$$

Thus  $mL = o(N)$ ,  $m \gg \log L$ , and  $m \gg b$ . [Proposition 4.3](#) with  $V = E$  gives

$$\mathbf{E}_\phi \kappa_k(f_\phi) \leq 5 \cdot 2^{-3m/64}$$

eventually. Since  $I_N$  is balanced, [Lemma 6.1](#) would imply

$$\frac{1}{2} \leq \frac{1}{4} + 5S^{A_d} 2^{-3m/64}.$$

But  $m/\ell = \Theta_d(c^{-(d-1)})$ , so a sufficiently small  $c$  makes the last term tend to zero. Padding proves the claim for  $F_n$ .

**The other two targets.** For the trilinear function, choose one coefficient slice using Chukhin’s restriction moments and union over our point-list tests. For the evaluator, fix an irreducible modulus for the analysis, use the original linear hash, and obtain  $t$ -wise independent signs by polynomial interpolation, where  $t$  is the number of polynomial coefficients. In both cases the slice is selected before the circuit is chosen, and its two level sets each have density at least  $1/3$ . The common point-list transfer gives  $\mathbf{E}_{\phi\kappa_k}(g_\phi) \leq 5 \cdot 2^{-\Omega(m)}$  at the scale in Eqn. (1.10). Lemma 6.1 finishes with  $\delta = 1/3$ . Appendix D gives the full moments, list counts, and input accounting. This completes Theorem 1.1.

## 7 Explicit upper bounds for inverse trace

We prove Theorem 1.3 by evaluating a product of Frobenius maps over an auxiliary field of polynomial size. Evaluation and interpolation over smaller fields are standard tools in constant-depth finite-field arithmetic [HV05]. The calculation below implements the arithmetic directly at the required Boolean depth, rather than first constructing a logarithmic-depth circuit and then compressing it. The qualitative existence of subexponential-size circuits at some fixed depth also follows from [HV05] for its explicit field representation; the depth allocations below are supplied here.

All circuits in this section are nonuniform. Field presentations, changes of basis, evaluation points, and lookup tables are fixed circuit data. The final circuits contain only unbounded-fan-in AND/OR gates and input negations. We count both gates and wires.

### 7.1 Enumerating intermediate states

**Lemma 7.1** (Computations with a bounded number of state bits). *Consider a deterministic computation that reads  $T$  consecutive input blocks of  $b$  bits each and maintains a  $w$ -bit state, where  $T, b, w \geq 1$ . Its initial state is fixed, each transition is an arbitrary fixed function of the state and the current block, and its output is an arbitrary fixed predicate of the final state. Put  $L = Tb$ . For every fixed integer  $k \geq 1$ , the output has a depth-at-most- $(k + 1)$  AND/OR circuit of size*

$$2^{O_k(L^{1/k}w^{1-1/k}+b+w+\log(T+2))}. \quad (7.1)$$

*Both an AND-top and an OR-top circuit are available, for the output and its complement. The same bound holds for the number of wires.*

*Proof.* For  $k = 1$ , use a full CNF or DNF on the  $L$  input bits. Suppose  $k \geq 2$  and  $1 \leq w < L$ . Set  $g = \lceil (L/w)^{1/k} \rceil$ , and first assume  $g \leq T$ .

Split the block sequence into at most  $g$  consecutive intervals of nearly equal length, and repeat this splitting for  $k - 1$  levels. To test a segment with a prescribed initial state and a prescribed final-state predicate, enumerate the states at its interval boundaries. For each boundary-state tuple, conjoin the corresponding interval tests; then take the OR over tuples. There are at most  $2^{gw}$  tuples at a node. At a leaf, the segment has at most  $\lceil T/g^{k-1} \rceil$  blocks, so its test has a full CNF on at most  $L/g^{k-1} + b$  input bits.

Each interval test is again a computation of the same kind. Complementing its final-state predicate complements the test, so De Morgan’s law gives an AND-top implementation whenever an OR-top implementation is available, and conversely. At each internal node, choose AND-top circuits for the interval tests and merge their top gates with the conjunction for a boundary-state tuple. Each recursion level therefore adds one layer. Starting from depth two at the leaves gives

total depth  $k + 1$ . Complementing the final predicate and applying De Morgan also gives both root types for both output polarities.

The number of levels is fixed. Counting copies, boundary tuples, and leaf truth tables bounds the logarithm of the size by

$$O_k \left( gw + \log(g + 1) + \frac{L}{g^{k-1}} + b + \log(T + 2) \right).$$

Here  $gw = O_k(L^{1/k}w^{1-1/k} + w)$  and  $L/g^{k-1} \leq L^{1/k}w^{1-1/k}$ . Leaf literal wires add only their input-length factor, and internal conjunctions add at most  $g$  wires per tuple, so the same estimate covers wires.

For completeness, if  $w \geq L$  or  $T = 1$ , the full truth table suffices. If  $g > T$ , then  $(L/w)^{1/k} > T$ , which gives  $Tw < b$  for  $k \geq 2$ . A single split into individual blocks has logarithmic size  $O(Tw + b + \log(T + 2))$  and depth three, within the claimed bounds. This covers the rounding cases.  $\square$

## 7.2 Representing inverse trace by evaluations

Let  $E = \mathbb{F}_{2^N}$ , with  $N \geq 2$ , in any fixed binary basis. Fix a polynomial presentation  $E \cong \mathbb{F}_2[Z]/(p)$ , where  $p$  is irreducible of degree  $N$ . For  $1 \leq j \leq N-1$ , let  $f_j(Z)$  be the degree-below- $N$  representative of  $x^{2^j}$ . Its coefficients are binary linear functions of the original input bits. Define

$$P_x(Z) = \prod_{j=1}^{N-1} f_j(Z).$$

This polynomial has degree at most  $D = (N-1)^2$ , and

$$P_x \bmod p = \text{inv}_0(x),$$

because  $\sum_{j=1}^{N-1} 2^j = 2^N - 2$ . The identity also holds at zero. Reduction modulo  $p$  followed by trace is a fixed binary linear functional of the coefficients of  $P_x$ ; denote it by  $\Lambda$ .

Put  $M = D + 1$  and choose an auxiliary field  $K = \mathbb{F}_{2^s}$  with  $s = \lceil \log M \rceil$ . Choose  $M$  distinct points  $\alpha_1, \dots, \alpha_M \in K$ . The auxiliary field need not embed in  $E$ . Interpolation determines  $P_x$  from the values

$$v_\ell(x) = P_x(\alpha_\ell) = \prod_{j=1}^{N-1} f_j(\alpha_\ell).$$

To extend  $\Lambda$  to the coefficients obtained by interpolation over  $K$ , choose a binary linear map  $\pi : K \rightarrow \mathbb{F}_2$  with  $\pi(1) = 1$  and apply it to each coefficient before applying  $\Lambda$ . This agrees with  $\Lambda$  on the actual polynomial, whose coefficients lie in  $\mathbb{F}_2$ . The resulting map from  $K^M$  to  $\mathbb{F}_2$  is binary linear, so there are fixed binary linear functionals  $\lambda_\ell : K \rightarrow \mathbb{F}_2$  such that

$$I_N(x) = \bigoplus_{\ell=1}^M \lambda_\ell(v_\ell(x)). \tag{7.2}$$

In particular, the final parity has  $M = O(N^2)$  scalar inputs.

## 7.3 Three stages at adjustable depths

Fix positive integers  $h_1, h_2, h_3$  and a generator  $\gamma$  of  $K^\times$ . For  $y \neq 0$ , represent  $\log_\gamma y$  by  $s$  bits; assign logarithm zero to  $y = 0$  and keep a separate zero flag. All logarithm and exponentiation tables are on  $O(\log N)$  bits, so their descriptions have polynomial size.

**Evaluation and logarithm tables.** For every  $j, \ell$ , the map  $x \mapsto f_j(\alpha_\ell)$  is a fixed binary linear map into  $K$ . A computation reading the  $N$  raw input bits can accumulate its value in an  $s$ -bit state. Any chosen bit of its logarithm, or its zero flag, is a predicate of the final state. Applying [Lemma 7.1](#) with  $L = T = N$  and  $b = 1$  gives depth  $h_1 + 1$  and logarithmic size

$$O_{h_1} \left( N^{1/h_1} (\log N)^{1-1/h_1} + \log N \right). \quad (7.3)$$

The polynomial number of required output bits adds only  $O(\log N)$  to the logarithmic size. This stage includes all Frobenius maps and basis changes.

**Multiplication at each evaluation point.** For each  $\ell$ , read the  $N - 1$  logarithms and zero flags as blocks of  $s + 1$  bits. Maintain their logarithm sum modulo  $|K| - 1$  and the OR of the zero flags, using  $s + 1$  state bits. If a zero flag has occurred, output zero; otherwise the terminal predicate outputs  $\lambda_\ell(\gamma^a)$ , where  $a$  is the accumulated sum. The transitions may be defined arbitrarily on invalid logarithm encodings, which do not arise from the first stage. Here  $L = (N - 1)(s + 1)$  and  $b = w = s + 1$ . Thus [Lemma 7.1](#) gives depth  $h_2 + 1$  and logarithmic size

$$O_{h_2} \left( N^{1/h_2} \log N + \log N \right). \quad (7.4)$$

There are only  $M$  parallel computations. Although their formal inputs are correlated outputs of the first stage, the circuit is exact on every assignment to those formal inputs, so substitution is valid.

**The final parity.** Apply [Lemma 7.1](#) to parity on the  $M$  scalar outputs in Eqn. (7.2), using one state bit. This gives depth  $h_3 + 1$  and logarithmic size

$$O_{h_3} \left( N^{2/h_3} + \log N \right). \quad (7.5)$$

*Proof of Theorem 1.3.* Each stage has alternating gate layers and is available with either root type, for both output polarities. At a stage boundary, implement each input literal of the next stage by a circuit whose root type agrees with that next stage's bottom gate. Merge the adjacent gates of the same type. Both polarities are available, so this introduces no internal negation. The two boundaries save one layer each, giving depth

$$(h_1 + 1) + (h_2 + 1) + (h_3 + 1) - 2 = h_1 + h_2 + h_3 + 1.$$

Combining Eqns. (7.3)–(7.5) gives logarithmic size  $O_{\mathbf{h}}(\Phi_{\mathbf{h}}(N))$ . Gate sharing is allowed. Even if merging increases the wire count, the total number of distinct wires is at most quadratic in the number of gates and inputs before merging, which preserves this estimate.

The full DNF gives size  $2^{O(N)}$  and depth two. Taking the best construction among the finitely many triples allowed at a fixed depth  $d$  proves Eqn. (1.3). The allocations  $(h_1, h_2, h_3) = (2, 2, 3)$  and  $(2, 2, 4)$  give Eqn. (1.4); choosing  $(h, h, 2h)$  gives Eqn. (1.5). The case  $N = 1$  is immediate. Finally,  $F_n$  ignores all but its first  $N$  bits, where  $N \leq n < 2N$ , so the same circuits give the asserted bounds in  $n$ .  $\square$

Thus inverse trace has exact circuits of size  $2^{o(n)}$  at each fixed depth  $d \geq 8$ . For every fixed  $\varepsilon > 0$ , choosing an integer  $h > 1/\varepsilon$  in Eqn. (1.5) gives size  $2^{O_\varepsilon(n^\varepsilon)}$  at depth  $4h + 1$ . These estimates give sufficient depths and sizes; they do not establish optimality or exclude exponential hardness at depths three through seven.

## 8 Consequences and limits of the representation

The point-list theorem concerns descriptions of sets. It allows an exponential number of pieces, can require exact counts of satisfying assignments to find them, and permits many clauses per piece. Its use here is to make simultaneous probabilistic estimates possible. [Appendix E](#) derives a bound on the correlation of inverse trace with width- $k$  CNFs.

There is an intrinsic list-length cost. If  $J = \text{cl}_b(A) \neq \emptyset$ ,  $1 \leq b \leq m$ , and  $|A| \leq L$ , then every  $b$ -coordinate projection of  $J$  has at most  $L$  values. Shearer’s entropy inequality gives

$$|J| \leq L^{m/b}.$$

Consequently any exact signed representation  $\mathbf{1}_H = \sum_i c_i \mathbf{1}_{\text{cl}_b(A_i)}$  with  $|A_i| \leq L$  satisfies

$$\sum_i |c_i| \geq 2^{h - (m/b) \log L}, \quad h = \log |H|. \quad (8.1)$$

[Appendix E](#) proves both statements. For high-entropy  $H$ , coefficient mass  $2^{\varepsilon m}$  forces  $\log L \geq b(h/m - \varepsilon)$ . Exponential dependence on width is therefore unavoidable for this dictionary.

In the inverse-trace union bound, the character-sum error term requires  $mL = O(N)$ . Together with Eqn. (8.1), this limits the useful width to logarithmic size. The worst-case proof also needs  $m = \Omega_d(\log S)$ . At depth three these constraints yield  $\log S$  of order  $\sqrt{N \log N}$ ; changing a constant in the partition cannot turn this argument into an exponential lower bound.

There is a separate higher-depth limitation of this covering route. If the outer restriction keeps each bit with probability  $q$ , then on any cube of free variables of dimension  $v$  a singleton is a width-one CNF of absolute correlation  $2^{-v}$  with any sign function. Hence

$$\mathbf{E}_\phi \kappa_k(g_\phi) \geq \mathbf{E}_\phi 2^{-v} = (1 - q/2)^N = 2^{-O(Nq)}.$$

To make this smaller than  $S^{-A_d}$  with  $q = \Theta_d((\log S)^{-(d-3)})$  requires  $(\log S)^{d-2} = O_d(N)$ . This is a restriction on the method, not a general upper bound on circuit complexity. For the trilinear function a specific upper bound  $2^{O_d(n^{2/d})}$  is known [[Chu26](#), Theorem 5.1], precluding truly exponential lower bounds at fixed  $d \geq 3$  for that target. For inverse trace, [Theorem 1.3](#) rules out a size lower bound  $2^{\Omega(n)}$  at every fixed depth  $d \geq 8$ . It leaves open the corresponding question at depths three through seven, and its upper bounds remain above the lower-bound scale of [Theorem 1.1](#). Distinguishing these upper bounds on the functions from limitations of the proof method is essential when assessing the remaining gap in Eqn. (1.6).

## Acknowledgments

This work was carried out during the authors’ visit to the Simons Institute for the Theory of Computing. The authors thank the Institute for its hospitality and support during the program Pseudorandomness and High-Dimensional Expansion in Fall 2026.

**AI disclosure.** The authors initiated this project by investigating properties of the inverse-trace function relevant to circuit lower bounds. OpenAI Codex was used substantially, through iterative exchanges with the authors, to explore proof ideas and assist with exposition, proof auditing, and reference checking.

## References

- [Ajt83] M. Ajtai, “ $\Sigma_1^1$ -formulae on finite structures,” *Annals of Pure and Applied Logic*, vol. 24, no. 1, pp. 1–48, 1983.
- [CIP06] Chris Calabro, Russell Impagliazzo, and Ramamohan Paturi. A duality between clause width and clause density for SAT. In *21st IEEE Conference on Computational Complexity (CCC 2006)*, pages 252–260, 2006. [Author version](#).
- [Chu26] Nikolai Chukhin. Breaking the parity barrier for constant-depth circuits. ECCC Report TR26-248, 2026. <https://eccc.weizmann.ac.il/report/2026/248/>.
- [FW25] Lei Fu and Daqing Wan. A class of incomplete character sums. *Quarterly Journal of Mathematics* 65(4):1195–1211, 2014; corrected arXiv version 3, January 6, 2025. <https://arxiv.org/abs/1303.3650v3>.
- [FSS84] Merrick Furst, James B. Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, 1984. <https://doi.org/10.1007/BF01744431>.
- [GT18] Oded Goldreich and Avishay Tal. Matrix rigidity of random Toeplitz matrices. *Computational Complexity* 27(2):305–350, 2018. [doi:10.1007/s00037-016-0144-9](https://doi.org/10.1007/s00037-016-0144-9).
- [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)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:20. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021.
- [GRSS23] Mika Göös, Artur Riazanov, Anastasia Sofronova, and Dmitry Sokolov. Top-down lower bounds for depth-four circuits. In *Proceedings of the 64th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1048–1055, 2023. <https://doi.org/10.1109/FOCS57990.2023.00063>.
- [Hås89] Johan Håstad. Almost optimal lower bounds for small depth circuits. In *Randomness and Computation*, Advances in Computing Research, volume 5, pages 143–170, 1989.
- [Hås14] Johan Håstad. On the correlation of parity and small-depth circuits. *SIAM Journal on Computing* 43(5):1699–1708, 2014. [doi:10.1137/120897432](https://doi.org/10.1137/120897432).
- [HJP95] Johan Håstad, Stasys Jukna, and Pavel Pudlák. Top-down lower bounds for depth-three circuits. *Computational Complexity*, 5(2):99–112, 1995.
- [HV05] Alexander Healy and Emanuele Viola. Constant-depth circuits for arithmetic in finite fields of characteristic two. *Electronic Colloquium on Computational Complexity*, Report TR05-087, 2005. [ECCC TR05-087](https://eccc.weizmann.ac.il/reports/2005/087/).
- [IPZ01] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences* 63(4):512–530, 2001. [doi:10.1006/jcss.2001.1774](https://doi.org/10.1006/jcss.2001.1774).
- [KR26] Gülce Kardeş and Benjamin Rossman. On top-down and local lower bounds for  $AC^0$  circuits. *arXiv preprint arXiv:2609.01759*, 2026. <https://arxiv.org/abs/2609.01759>.
- [Kor26] Oliver Korten. Top-down lower bounds for all depths. *arXiv preprint arXiv:2609.38677*, 2026. <https://arxiv.org/abs/2609.38677>.
- [LR26] Victor Lecomte and Prasanna Ramakrishnan. Optimal Shallow Circuits for Majority. *arXiv preprint arXiv:2609.34029*, 2026. <https://arxiv.org/abs/2609.34029>.
- [LY22] Jiayu Li and Tianqi Yang.  $3.1n - o(n)$  circuit lower bounds for explicit functions. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC)*, pages 1180–1193, 2022. <https://doi.org/10.1145/3519935.3519976>.

- [MS26] Om Swostik Mishra and Rahul Santhanam. An Explicit  $3.5n - o(n)$  Size Lower Bound against General Boolean Circuits. *Electronic Colloquium on Computational Complexity (ECCC)*, Technical Report TR26-260, 2026.
- [OAI26] OpenAI. Beyond the square-root exponent for depth-three Boolean circuits. OpenAI Math Release preprint, September 23, 2026. [Preprint and source files](#).
- [Raz87] A. A. Razborov, “Lower bounds on the size of bounded-depth circuits over a complete basis containing the logical addition,” *Mathematical Notes of the Academy of Sciences of the USSR*, vol. 41, no. 4, pp. 333–338, 1987.
- [Smol87] R. Smolensky, “Algebraic methods in the theory of lower bounds for Boolean circuit complexity,” in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pp. 77–82, 1987.
- [Tal17] Avishay Tal. Tight bounds on the Fourier spectrum of  $AC^0$ . In *32nd Computational Complexity Conference (CCC 2017)*, LIPIcs 79, Article 15, pages 15:1–15:31, 2017. [doi:10.4230/LIPIcs.CCC.2017.15](https://doi.org/10.4230/LIPIcs.CCC.2017.15).
- [Val77] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In Jozef Gruska, editor, *Mathematical Foundations of Computer Science 1977*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977. [https://doi.org/10.1007/3-540-08353-7\\_135](https://doi.org/10.1007/3-540-08353-7_135).
- [Val83] Leslie G. Valiant. Exponential lower bounds for restricted monotone circuits. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing (STOC 1983)*, pages 110–117. ACM, 1983.
- [Vio09] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.
- [Yao85] A. C.-C. Yao, “Separating the polynomial-time hierarchy by oracles,” in *26th Annual Symposium on Foundations of Computer Science (FOCS 1985)*, pp. 1–10, IEEE, 1985.

## A Deterministic switching parameters

We prove [Proposition 5.2](#), including its handling of shared gates and shallow leaves. Put  $s = d - 2$ ,  $U_0 = S$ , and recursively set

$$t_i = \lceil \log(2U_{i-1}) \rceil, \quad k_i = \max\{k_{i-1}, t_i\}, \quad p_i = \frac{1}{96k_{i-1}}, \quad U_i = 2^{t_i+2}U_{i-1}, \quad 1 \leq i \leq s. \quad (\text{A.1})$$

These quantities depend only on  $S, d$ . Since  $2^{t_i} \leq 4U_{i-1}$ ,

$$U_i \leq 16U_{i-1}^2 \leq U_{i-1}^6, \quad U_i \leq S^{6^i}. \quad (\text{A.2})$$

In particular  $U_i \leq 2^{A^\ell}$  for  $A = 6^d$ .

At an active leaf of depth at least three, consider each second-layer subcircuit. Switching it to the opposite depth-two form permits its outer gate to merge with its parent, decreasing the whole circuit depth by one. An ordinary decision tree of depth at most  $t_i$  supplies both forms with at most  $2^{t_i}$  terms or clauses. Replacing all at most  $U_{i-1}$  second-layer gates fits the size bound  $U_i$ . If a gate has several parents, all use the same replacement; only wires are duplicated. Each individual residual circuit therefore stays within  $U_i$  gates.

A leaf already at depth at most two is frozen. It retains its current CNF or DNF under later random restrictions, without new tree queries. The maximum in the definition of  $k_i$  ensures that this width remains allowed, including when  $k_0 > t_1$ .

At every stage draw one fresh global  $p_i$ -restriction on all currently free coordinates, including variables absent from the simplified circuit. Continue drawing after any failure. The unconditional composition  $\phi$  has restriction parameter

$$q = \prod_{i=1}^s p_i, \quad k = k_s. \quad (\text{A.3})$$

For fixed  $d$ , both  $k = \Theta_d(\ell)$  and  $q = \Theta_d(\ell^{-s})$  follow directly from these parameters.

### A.1 The switching lemma

Condition on any successful prior history. At stage  $i$ , union over at most  $U_{i-1}$  active second-layer functions. Its conditional failure probability is at most

$$U_{i-1}(5/96)^{t_i} \leq U_{i-1}16^{-t_i} \leq 2^{-4}U_{i-1}^{-3} \leq 2^{-3\ell}.$$

After  $s$  successful stages the output is a width- $k$  CNF or DNF. A CNF has correlation at most  $\kappa_k$ . A DNF equals  $1 - H$  with  $H$  a width- $k$  CNF, and therefore has correlation at most  $2\kappa_k$ , because the constant-one test is also included. The restricted target need not be balanced. Use the Boolean bound one on failure and enlarge the successful expectation to the unconditional expectation over  $\phi$ . This proves [Eqn. \(5.2\)](#).

### A.2 Common partial decision trees

Fix a positive integer  $D_0$ . Define

$$R_0 = 0, \quad D_i = R_{i-1} + D_0, \quad R_i = R_{i-1} + D_i = (2^i - 1)D_0. \quad (\text{A.4})$$

After stage  $i - 1$ , maintain a restriction tree of depth at most  $R_{i-1}$ . Every active leaf has depth reduced by  $i - 1$ , size at most  $U_{i-1}$ , and bottom fan-in at most  $k_{i-1}$ . Frozen leaves satisfy the same bounds.

Condition on earlier randomness. An old leaf has a fixed path restriction  $\tau$ . On coordinates outside  $\text{dom } \tau$ , the next global random restriction is an independent  $p_i$ -random restriction. Apply the multi-switching lemma to the at most  $U_{i-1}$  second-layer functions of that cofactor, requesting depth  $D_i$  and residual depth at most  $t_i$ . Require this to succeed for every old leaf, even those that the new random restriction will make incompatible. A union bound over at most  $2^{R_{i-1}}$  leaves gives conditional failure at most

$$2^{R_{i-1}} U_{i-1} (24p_i k_{i-1})^{D_i} \leq 2^{R_{i-1}} U_{i-1} 4^{-D_i} = U_{i-1} 2^{-R_{i-1}-2D_0}. \quad (\text{A.5})$$

Frozen leaves need no call.

Restrict the old tree by the global random restriction and delete incompatible paths. At each surviving active leaf splice in its new common tree, which queries only coordinates outside that old path. The resulting tree has depth at most  $R_i$ . Switching the residual depth-two functions to their opposite forms reduces circuit depth by one at each new leaf. The size and bottom fan-in bounds follow from Eqn. (A.1). This proves the induction.

Crucially, the  $2^{R_{i-1}}$  factor is charged only to failure probability. It does not multiply the size of an individual leaf circuit or its bottom fan-in. We use a product distribution only for the unconditional composition of the global random restrictions in Eqn. (A.3).

Summing Eqn. (A.5) over  $s$  stages bounds total failure by  $s2^{A\ell-2D_0}$ . On success, Lemma 5.1 bounds the final correlation by  $2^{R_{s+1}} \kappa_k(g_{V,\phi})$ , even though its atoms depend on the full history. Enlarge to the unconditional expectation to obtain Eqn. (5.3).

## B Uniform parameter checks for average-case hardness

We give explicit depth constants to substantiate the uniform size range, rather than hide endpoint conditions in asymptotic notation. Let

$$\begin{aligned} s &= d - 2, & K &= 9 \cdot 6^d, & A &= 6^d, \\ Q &= (96K)^{-s}, & a &= \frac{Q}{2^{20}K}, & J &= 2^{d+10}, \\ M_d &= 4JA, & \zeta &= \frac{1}{16M_d}, & c_* &= (a/128)^{1/(d-1)}. \end{aligned}$$

The symbol  $M_d$  here is a depth constant, not an input dimension. For all sufficiently large  $N$ , the deterministic bounds in Eqn. (A.1) satisfy

$$\ell \leq k_i \leq K\ell, \quad Q\ell^{-s} \leq q \leq (96\ell)^{-s}, \quad \ell \leq k \leq K\ell. \quad (\text{B.1})$$

Assume Eqn. (5.4). For any subcube of codimension less than  $N/4$ , set

$$b = \left\lfloor \frac{\log k}{2048} \right\rfloor, \quad p = \frac{b}{64k}, \quad m = (\dim V)qp, \quad \mathcal{R} = \frac{N \log \ell}{\ell^{d-1}}.$$

Uniformly in this range, eventually

$$\frac{\log \ell}{4096} \leq b \leq \frac{\log \ell}{1024}, \quad 3a\mathcal{R} \leq m \leq \frac{\mathcal{R}}{2^{16}96^s}. \quad (\text{B.2})$$

The lower bound uses  $\dim V \geq 3N/4$  and Eqn. (B.1); the upper bound uses  $\dim V \leq N$  and  $k \geq \ell$ . In particular  $k \geq b \geq 2$  eventually, and the upper-size constant ensures  $m \geq 128 \log \ell$ .

For the list-length bound in Eqn. (4.4),  $2^{512b} \leq k^{1/4}$  gives

$$L = O_d(\ell^{1/4} \log \ell \log N), \quad \log(8L) \leq \frac{1}{4} \log \ell + \log \log \ell + \log \log N + O_d(1) \leq 2 \log \ell. \quad (\text{B.3})$$

The last estimate uses  $\ell \geq \log N$ . Hence  $m \geq 16 \log(8L)$  and  $m \geq 2b$ . Also

$$\begin{aligned} \frac{mL}{N} &= O_d\left(\ell^{-(d-5/4)}(\log \ell)^2 \log N\right) \\ &\leq O_d\left(\ell^{-(d-9/4)}(\log \ell)^2\right) = o(1). \end{aligned}$$

This is uniform down to polynomial-size circuits: at  $\ell = \log N$  and  $d = 3$  the upper bound is  $O_d((\log \log N)^2/(\log N)^{3/4})$ . Thus  $mL \leq N/64$  eventually. Furthermore  $m = o(N)$  uniformly, and  $L$  is polynomially bounded in  $N$ .

All terms in  $\Delta$  in Eqn. (4.6) are eventually bounded by a constant multiple of  $\gamma = 2^{-3m/64}$ : the two dimension-tail contributions and the paired term have stronger exponents in  $m$ , and  $128L2^{-3N/16}$  is exponentially smaller since  $m = o(N)$ . In particular Eqn. (5.5) follows.

If  $m < M_d \ell$ , Eqns. (5.2) and (5.5) give

$$|\mathbf{E}_V[fC]| \leq s2^{-3m/M_d} + 10 \cdot 2^{-3m/64}.$$

If  $m \geq M_d \ell = 4JA\ell$ , set  $D_0 = \lfloor m/J \rfloor$ . For large  $N$ ,  $m \geq 2J$  and

$$A\ell - 2D_0 \leq -m/J, \quad R_s \leq 2^{d-2}m/J = m/4096.$$

The multi-switching estimate gives

$$|\mathbf{E}_V[fC]| \leq s2^{-m/J} + 10 \cdot 2^{-(3/64 - 1/4096)m}.$$

Since  $m \rightarrow \infty$  uniformly and  $\zeta = 1/(16M_d)$  is smaller than the displayed decay constants, both cases are at most  $2^{-\zeta m}$  eventually. Using  $m \geq a\mathcal{R}$  proves Proposition 5.3 with  $\theta_d = \zeta a$ .

Finally,  $\mathcal{R}/N = \log \ell / \ell^{d-1} \rightarrow 0$  uniformly. For large  $\ell$  the function  $\log \ell / \ell^{d-1}$  decreases, so its minimum over the range in Eqn. (5.4) is at the upper endpoint, where  $\mathcal{R} \geq c_*^{-(d-1)} \log \ell \rightarrow \infty$ . This justifies absorbing fixed factors and the cofactor-recursion remainder into a smaller exponent constant.

## C Uniform fields, general circuits, and padding

### C.1 A deterministic field tower

Start with  $E_0 = \mathbb{F}_2$  and  $\gamma_0 = 1$ . Recursively define

$$E_j = E_{j-1}[\theta_j]/(\theta_j^2 + \theta_j + \gamma_{j-1}), \quad \gamma_j = \gamma_{j-1}\theta_j.$$

Inductively  $\gamma_{j-1}$  has absolute trace one. In a binary field,  $z \mapsto z^2 + z$  has kernel  $\{0, 1\}$  and its image is the trace-zero subspace. Indeed trace vanishes on its image, and both spaces have codimension one. Therefore the displayed quadratic is irreducible. Its roots differ by one, so  $\text{Tr}_{E_j/E_{j-1}}(\theta_j) = 1$ . It follows that

$$\text{Tr}_{E_j/\mathbb{F}_2}(\gamma_j) = \text{Tr}_{E_{j-1}/\mathbb{F}_2}(\gamma_{j-1}) = 1.$$

Thus  $E_j$  has binary dimension  $N = 2^j$ . The recursive pair basis is deterministic. Multiplication uses at most five multiplications in the previous field and a linear number of bit additions, so its complexity is polynomial in  $N$ . Inversion by  $x^{2^N-2}$  for  $x \neq 0$ , and trace by  $N$  Frobenius iterates, are also polynomial time. No search for irreducible polynomials is needed. The finitely many small input lengths can be defined by the same inverse-trace rule.

## C.2 Layering a circuit without increasing its depth

Let a general circuit have size  $S_0 \geq N$  and depth at most  $d$ . First bypass paths of consecutive same-type gates by connecting each parent directly to its same-type descendants' frontier inputs. Retain a shared gate when it is still used by an opposite-type parent. This preserves the Boolean function without adding gates or increasing depth. Every remaining internal wire joins opposite gate types.

All gate-to-output path lengths from a given gate have parity determined by its type. Assign that gate its longest such path level. An internal wire skips a positive odd number of levels. Fill the skipped levels with alternating unary gates; similarly pad literal-to-gate wires. There are  $O((S_0 + N)^2)$  distinct wires and  $d$  is fixed, so this adds  $O_d(S_0^2)$  gates and does not increase depth. Unused layers, constants, and unary gates may be retained. This representation supports the fixed layer labels used in cofactor recursion.

For sufficiently large  $S_0$ , the deterministic budget  $S = S_0^3$  dominates the normalized size. With  $\ell = 3 \log S_0$ , the previous estimates apply for

$$N \leq S_0 \leq 2^{(c_*/3)N^{1/(d-1)}}.$$

Changing  $\log S_0$  to  $3 \log S_0$  alters  $N \log \log S_0 / (\log S_0)^{d-1}$  by depth-dependent constant factors. Eqn. (5.1) absorbs the factor two in passing to sign correlation.

## C.3 A single family at all lengths

For arbitrary  $n$ , let  $N$  be the largest power of two at most  $n$ , and define  $F_n$  to evaluate  $I_N$  on its first  $N$  input bits. Ignore the remaining bits. Then  $N \leq n < 2N$ , and this is one uniform polynomial-time family, independent of  $d, S$ .

Fixing the ignored bits of an  $n$ -input circuit leaves a circuit on  $N$  bits of no larger size or depth. The tower-length bound holds for every such fixing, so average and use the triangle inequality. Since  $S \geq n \geq N$  and  $N > n/2$ , reducing the size constant by a factor  $2^{1/(d-1)}$  and reducing the exponent constant by an absolute factor proves Theorem 1.2. For worst-case hardness, any exact circuit restricts to an exact circuit for  $I_N$ ; moreover  $N \log N = \Theta(n \log n)$ . This proves the padded part of Theorem 1.1. No pseudorandomness under translations in ignored directions is asserted or needed.

## D The two parameterized worst-case targets

### D.1 The trilinear function

Write  $g_z = (-1)^{T_a(\cdot, \cdot, z)}$ . We use the following two results of Chukhin [Chu26, Lemmas 4.2 and 4.3]. If  $T_y \subseteq \{0, \dots, a-1\}$  includes each index independently with probability  $m/a$ , where  $m \leq a^{3/5}$  and  $u \leq m^{1/4}$ , then except with probability  $a^{-\Omega(m)}$ ,

$$|B + T_y| \geq |B|(|T_y| - m/4) \quad \text{for all } B \subseteq \{0, \dots, a-1\}, |B| \leq u. \quad (\text{D.1})$$

If a fixed data restriction has  $|T_x| \geq 2u$ ,  $u$  even, and  $|B + T_y| \geq |B||T_y|/2$  for those  $B$ , then for every fixed Boolean indicator  $J$  on the cube of free variables,

$$\mathbf{E}_z |\mathbf{E}[g_{z,\sigma} J]|^u \leq 2^{-u|T_x|/4} + 2^{-u|T_y|/4}. \quad (\text{D.2})$$

The indicator can be arbitrary; a clause description is not needed for this moment input.

**Proposition D.1** (A hard trilinear slice). *Let  $k \geq b \geq 2$ ,  $0 < q \leq 1$ ,  $p = b/(64k)$ , and  $m = qpa$ . Let  $u$  be the largest even integer at most  $m^{1/4}$  and set*

$$L_* = \left\lceil 2^{2048b} [b \ln(8m+1) + 1] \right\rceil.$$

*If  $m$  is sufficiently large,  $m \leq a^{3/5}$ , and  $L_* \leq u/128$ , then some fixed  $z$  satisfies*

$$\mathbf{E}_{\phi} \kappa_k(g_{z,\phi}) \leq 5 \cdot 2^{-m/32},$$

*where  $\phi$  is a  $q$ -restriction of the  $2a$  data bits.*

*Proof.* Put  $\varepsilon = 2^{-m/32}$  and draw the fresh inner  $p$ -restriction. The numbers of free variables in the two blocks are in  $[m/2, 2m]$  except with probability at most  $2\varepsilon$  eventually. Eqn. (D.1) fails with probability at most  $\varepsilon$ . Outside these events, the total number of free variables  $v$  lies in  $[m, 4m]$ , the sumset hypothesis of Eqn. (D.2) holds, and  $|T_x| \geq 2u$ .

Markov's inequality at threshold  $2^{-m/16}$  bounds the failure probability for any fixed list test by  $2^{1-um/16}$ . Union over fewer than  $2^{vL_*+1}$  tests to get

$$2^{4mL_*+2-um/16} \leq 2^{2-um/32} \leq \varepsilon$$

eventually. On success, Theorem 2.1 with  $C = 2048$  gives for every width- $b$  CNF  $H$

$$|\mathbf{E}[g_{z,\phi\rho}H]| \leq 2^{v/128} 2^{-m/16} \leq \varepsilon.$$

The joint failure probability over  $z, \phi, \rho$  is at most  $4\varepsilon$ . Averaging fixes one  $z$  with failure probability at most  $4\varepsilon$ . Lemma 3.2 then gives  $5\varepsilon$ .  $\square$

To finish the lower bound, fix  $d \geq 3$  and let

$$\eta = \frac{1}{32 \cdot 2048(d-1)}, \quad b = \lfloor \eta \log a \rfloor, \quad \ell = c_d(a \log a)^{1/(d-1)}, \quad S = 2^\ell.$$

Use the worst-case depth-reduction parameters  $k, q$  from Section 6. For small fixed  $c_d > 0$ ,  $k \geq b$  eventually, and

$$m = \Theta_d(\eta c_d^{-(d-2)} (a \log a)^{1/(d-1)}).$$

Then  $m \leq a^{3/5}$  and

$$L_* \leq a^{1/[32(d-1)]} O_d((\log a)^2) = o(m^{1/4}).$$

Proposition D.1 applies. The constant-one CNF and restriction averaging give  $|\mathbf{E}g_z| \leq 5 \cdot 2^{-m/32}$ , so both level sets of the selected slice have density at least  $1/3$ . Lemma 6.1 would imply

$$\frac{1}{3} \leq \frac{1}{4} + 5S^{A_d} 2^{-m/32}.$$

Since  $m/\ell = \Theta_d(\eta c_d^{-(d-1)})$ , sufficiently small  $c_d$  gives a contradiction. The total input length is  $4a - 1$ , proving the trilinear part of Theorem 1.1.

## D.2 The original polynomial evaluator

We spell out the family to avoid changing its input accounting or hiding its parameter inputs. At total input length  $n$ , let  $a = \lfloor n/5 \rfloor$ ,  $r = \lceil a^{2/3} \rceil$ , and let  $t$  be the largest nonnegative even integer at most  $a^{1/6}$ . Reject if  $a < 64$  or if the following blocks do not fit. Otherwise parse:

- $a$  data bits  $x_1, \dots, x_a$  and  $a + r - 1$  hash bits  $u_1, \dots, u_{a+r-1}$ ;
- $r$  bits specifying the monic modulus  $P(Z) = Z^r + \sum_{i < r} p_i Z^i$ ;
- $tr$  coefficient bits specifying  $\beta_0, \dots, \beta_{t-1}$  in  $R_P = \mathbb{F}_2[Z]/(P)$ .

Their total is  $2a + (t + 2)r - 1 \leq n$  for all sufficiently large lengths. Ignore unused bits. Form

$$h_i(x) = \sum_{s=1}^a u_{i+s-1} x_s \pmod{2} \quad (1 \leq i \leq r), \quad h(x) = \sum_{i=1}^r h_i(x) Z^{i-1} \in R_P.$$

Let  $\lambda$  select the degree-zero coefficient. The evaluator accepts exactly when

$$\lambda \left( \sum_{j < t} \beta_j h(x)^j \right) = 0.$$

This is the original family of [OAI26]. Ring operations are defined for every monic input modulus, whether reducible or not, and the algorithm runs in polynomial time. No irreducibility search is part of computing the function.

For hardness analysis choose one irreducible modulus of degree  $r$ . For every nonzero difference  $w$  of data inputs, the hash  $h(w)$  is uniform over  $\mathbb{F}_2^r$  when  $u$  is uniform. To see this, let  $s$  be the largest coordinate with  $w_s = 1$ . Row  $i$  has the fresh pivot  $u_{i+s-1}$ , with all other indices smaller, so the  $r$  rows are independent linear forms in  $u$ . A  $v$ -dimensional coordinate subcube has at most  $2^v - 1$  nonzero differences; the hash fails to be injective on it with probability at most  $2^{v-r}$ .

Conditioned on an injective hash, evaluation at any at most  $t$  distinct hashes maps uniform coefficients to independent uniform field values. This follows from Lagrange interpolation with polynomials of degree at most  $t - 1$ . Applying the nonzero coordinate functional  $\lambda$  gives unbiased  $t$ -wise independent signs  $g$  on the cube of free variables. For any fixed indicator  $J$ , expand the even  $t$ th moment of  $Y = \sum_z g(z) J(z)$ . A tuple with a singly occurring point contributes zero. The remaining tuples have at most  $t/2$  distinct points and are covered by at most  $2^{vt/2} t^t$  descriptions. Therefore

$$\Pr_{\beta} [|E[gJ]| > 2^{-v/4}] \leq t^t 2^{-vt/4}. \quad (\text{D.3})$$

This argument derives the moment directly for arbitrary indicators; it does not invoke a source proposition outside its fixed-width quantifiers.

For an expected number of free variables  $m$ , set

$$L_* = \left\lceil 2^{512b} [b \ln(4m + 1) + 1] \right\rceil.$$

For  $v \in [m/2, 2m]$ , union over fewer than  $2^{vL_*+1}$  tests. By Eqn. (D.3), failure is at most  $2^{-vt/8}$  whenever

$$L_*/t \leq 1/32, \quad \frac{\log t}{m/2} \leq 1/32, \quad \frac{1}{(m/2)t} \leq 1/32.$$

Indeed these bounds leave the total positive exponent at most  $3vt/32 < vt/8$ . On success, the  $C = 512$  point-list partition gives  $\kappa_b(g) \leq 2^{v/32} 2^{-v/4} \leq 2^{-v/8}$ . If  $r \geq (2 + 1/16)m$ , the hash error is

at most  $2^{-m/16}$ . Each dimension tail is also at most  $2^{-m/16}$ . Thus joint failure is at most  $4 \cdot 2^{-m/16}$  eventually. Averaging fixes all non-data inputs before selecting any circuit or test, and [Lemma 3.2](#) gives a slice with

$$\mathbf{E}_\phi \kappa_k(g_\phi) \leq 5 \cdot 2^{-m/16}.$$

Finally choose  $b = \lfloor \log a / (64 \cdot 512) \rfloor$ ,  $\ell = c_d(a \log a)^{1/(d-1)}$ , and the worst-case parameters  $k, q$ ,  $p = b/(64k)$ . Then

$$m = \Theta_d(c_d^{-(d-2)}(a \log a)^{1/(d-1)}), \quad L_* \leq a^{1/64} O((\log a)^2) = o(t), \quad \log t = o(m), \quad r/m \rightarrow \infty.$$

All preceding conditions hold. The constant-one test gives output densities at least  $1/3$ . [Lemma 6.1](#) contradicts exact computation by size  $2^\ell$  when  $c_d$  is sufficiently small. Since  $a = \lfloor n/5 \rfloor$ , this proves the evaluator part of [Theorem 1.1](#) in total input length, with its original parameters unchanged.

## E Further consequences of the decomposition

### E.1 Bounded-width CNFs and monochromatic sets for inverse trace

**Corollary E.1.** *For all sufficiently large tower lengths  $N$ , set  $C_0 = 512$  and let*

$$(\log N)^2 \leq k \leq \frac{N}{4096C_0}, \quad b = \left\lfloor \frac{\log k}{4C_0} \right\rfloor.$$

*For  $f = (-1)^{I_N}$  and every width- $k$  CNF  $H$ ,*

$$|\mathbf{E}[fH]| \leq 5 \cdot 2^{-3Nb/(4096k)}.$$

*If  $H \neq \emptyset$  is monochromatic for  $I_N$ , then*

$$-\log \mathbf{Pr}[H = 1] \geq \frac{3Nb}{4096k} - \log 5 = \Omega(N \log k/k).$$

*Proof.* Use [Proposition 4.3](#) with  $q = 1$  and  $V = E$ , so  $m = Nb/(64k)$ . Its list-length bound obeys

$$L = O(k^{1/4} \log k \log N), \quad bL = O(k^{1/4} (\log k)^2 \log N) = o(k)$$

uniformly in the stated range. This gives  $mL \leq N/64$  eventually. For  $k \geq \sqrt{N}$ , the upper endpoint gives  $m \geq 64C_0b$ , while  $\log(8L) \leq 2C_0b$  eventually. For  $k < \sqrt{N}$ ,  $m \geq \sqrt{N}b/64 \gg \log L$ . Thus the remaining hypotheses hold. The terms of  $\Delta$  are bounded by four times  $2^{-3m/64}$  eventually. For a monochromatic CNF  $H$ , we have  $|\mathbf{E}[fH]| = \mathbf{Pr}[H = 1]$ .  $\square$

### E.2 The intrinsic list-length requirement

**Proposition E.2.** *Let  $1 \leq b \leq m$ . A nonempty  $J = \text{cl}_b(A)$  with  $|A| \leq L$  has  $|J| \leq L^{m/b}$ . If  $H \neq \emptyset$  has an exact signed representation by such tests, then Eqn. (8.1) holds.*

*Proof.* For  $X$  uniform on  $J$ , each projection  $X_U$ ,  $|U| = b$ , has entropy at most  $\log L$ . Expand every  $H(X_U)$  in coordinate order. Conditioning on only  $U \cap [i-1]$  cannot reduce the conditional entropy below  $H(X_i | X_{[i-1]})$ . Each coordinate appears in  $\binom{m-1}{b-1}$  subsets, whence

$$\log |J| = H(X) \leq \frac{1}{\binom{m-1}{b-1}} \sum_{|U|=b} H(X_U) \leq \frac{m}{b} \log L.$$

For a signed representation, sum its pointwise absolute upper bound over the cube:

$$|H| \leq \sum_i |c_i| |\text{cl}_b(A_i)| \leq L^{m/b} \sum_i |c_i|.$$

$\square$

## F Comparison with the Fourier-tail bound

For a binary character  $\chi_\xi(x) = (-1)^{\langle \xi, x \rangle}$ , nondegeneracy of the trace pairing supplies  $a \in E$  with  $\chi_\xi(x) = \psi(ax)$ . The case  $h = 1$  of [Lemma 4.1](#) gives

$$\max_{\xi} |\widehat{f}(\xi)| \leq 8 \cdot 2^{-N/2}.$$

For a sign-valued depth- $d$  circuit  $G$  of size  $S$ , Tal's Fourier-tail theorem [[Tal17](#), Theorem 1] gives, for a depth constant  $A_d$ ,

$$\sum_{|U| \geq k} \widehat{G}(U)^2 \leq 2 \cdot 2^{-k/(A_d(\log S)^{d-1})}.$$

Take  $k = \lfloor N/100 \rfloor$ . The Fourier mass of  $f$  below  $k$  is at most

$$64 \cdot 2^{-N} \sum_{j < k} \binom{N}{j} \leq 2^{-(1-h_2(1/100))N+O(1)}.$$

Split Parseval's identity at  $k$  and apply Cauchy–Schwarz to each part. Using the fact that each sign function has total Fourier mass one gives

$$|\mathbf{E}[fG]| \leq 2^{-\Omega(N)} + \sqrt{2} 2^{-k/(2A_d(\log S)^{d-1})}.$$

This is  $2^{-\Omega_d(N/(\log S)^{d-1})}$  when that exponent tends to infinity, with the displayed estimate valid also outside that regime. Padding works as in [Appendix C](#). The higher shift moments, point-list decomposition, and guarded-CNF argument supply the additional  $\log \log S$  factor in [Theorem 1.2](#).