

Quantum Advantage from Sampling Shallow Circuits: Beyond Hardness of Marginals

Daniel Grier^{*} Daniel M. Kane[†] Jackson Morris[‡] Anthony Ostuni[§] Kewen Wu[¶]

Abstract

We construct a family of distributions $\{\mathcal{D}_n\}_n$ with $\mathcal{D}_n$ over $\{0,1\}^n$ and a family of depth-7 quantum circuits $\{C_n\}_n$ such that $\mathcal{D}_n$ is produced exactly by C_n with the all zeros state as input, yet any constant-depth classical circuit with bounded fan-in gates evaluated on any binary product distribution has total variation distance $1 - e^{-\Omega(n)}$ from $\mathcal{D}_n$. Moreover, the quantum circuits we construct are geometrically local and use a relatively standard gate set: Hadamard, controlled-phase, CNOT, and Toffoli gates. All previous separations of this type suffer from some undesirable constraint on the classical circuit model or the quantum circuits witnessing the separation.

Our family of distributions is inspired by the Parity Halving Problem of Watts, Kothari, Schaeffer, and Tal (STOC, 2019), which built on the work of Bravyi, Gosset, and König (Science, 2018) to separate shallow quantum and classical circuits for relational problems.

1 Introduction

One of, if not *the* primary direction in the study of quantum computing is to exhibit computational tasks that can be performed far more efficiently on a quantum computer than on a classical one. There are a number of promising candidates [Sho99, AA13, BFNV19], but the quantum superiority of many such algorithms relies on unproven assumptions about computational hardness.

To obtain *unconditional* quantum-classical separations, one must consider classical models of computation against which there are known unconditional lower bounds. Bravyi, Gosset, and König gave the first result of this kind by constructing a search problem which could be solved by constant-depth quantum circuits, but not constant-depth classical circuits [BGK18]. Formally, $\text{FQNC}^0 \not\subseteq \text{FNC}^0$. Since then, there have been many improvements to this result that consider stronger classical circuit families, different error models, and/or different topologies [WKST19, GS20, BGKT20, HLG21, CCRK23].

Nevertheless, these results still fundamentally use the search paradigm for separating the quantum and classical circuit models (or, in fact, sometimes generalizations of search [GS20, GJS21]). Intuitively, one can think of these search problems as follows: the input to the problem is both the number of qubits n and a specification of a constant-depth quantum circuit Q , and the goal is to output any bit string in the support of the distribution after measuring $Q|0^n\rangle$ in the computational basis. One might wonder if the specification of the quantum circuit is even necessary. That is, is

^{*}UC San Diego. Email: dgrier@ucsd.edu.

[†]UC San Diego. Email: dakane@ucsd.edu. Supported in part by NSF Medium Award CCF-2107079.

[‡]UC San Diego. Email: jrm035@ucsd.edu.

[§]UC San Diego. Email: aostuni@ucsd.edu.

[¶]Institute for Advanced Study. Email: shlw.kevin@hotmail.com. Supported by the National Science Foundation under Grant No. DMS-2424441, and by the IAS School of Mathematics.

there a single quantum circuit for every n that gives rise to a hard-to-sample distribution? In fact, Bravyi, Gosset, and König asked exactly this question in their original work [BGK18, Section 5].

There are a few reasons why we might want such a separation. First, one goal for proofs of quantum advantage is to help distill the core aspects of quantum computers that make them more powerful than their classical counterparts. Clearly then, a separation from a single family of distributions is desirable in its simplicity. Moreover, such results give complexity-theoretic support for certain quantum advantage experiments in which changing the underlying circuit is extremely difficult [ZWD⁺20, DGL⁺23, YGE⁺24].

Watts and Parham [WP23] were the first to answer the challenge of [BGK18] by constructing a family of constant-depth quantum circuits with output distributions that cannot be sampled (even approximately) by constant-depth classical circuits with bounded fan-in gates. Unfortunately, their result has two significant caveats. First, it imposes a strict requirement on the number of input bits to the classical circuit. Second, the quantum circuits they construct contain more-or-less arbitrary single-qubit gates (at least outside the Clifford hierarchy).

These two properties combine to make the “quantum” contribution to the quantum-classical separation less clear. To see this, first notice that the usual method of converting between gate sets does not apply in the constant-depth regime, since the Solovay-Kitaev theorem incurs a poly-logarithmic depth overhead [Kup23]. This implies that the choice of which single-qubit gates to allow in the quantum circuit model could ultimately affect which kinds of separations are possible. This consideration has been put into sharp relief by recent work that gives a *product* distribution which cannot be sampled (even approximately) by constant-depth classical circuits with uniformly random input bits [Vio23, KOW24].

In other words, it is possible to obtain a quantum vs. classical separation with a quantum circuit model that has no entangling gates (as only single-qubit rotation gates are needed to sample from a product distribution), undermining the claim that the separation is related to the powers of quantum mechanics. Indeed, if instead we allowed our classical circuit to have random inputs of arbitrary bias, then they, too, could easily produce the desired distribution. While the result of [WP23] does allow for classical circuits with biased input bits, the restriction on the number of input bits leaves open the possibility that larger classical circuits may still be able to sample from the distribution.

The main contribution of this work is the construction of a family of distributions that achieves the best properties from all prior works:

Theorem 1.1 (Informal Version of Theorem 2.1). *There is a uniform family of constant-depth quantum circuits $\{Q_n\}_n$ such that*

- Discrete gate set: Q_n is constructed from Hadamard, controlled-phase, CNOT, and Toffoli gates. Furthermore, Q_n has a depth-7, geometrically local implementation.
- Quantum advantage: Let $\{C_n: \{0,1\}^* \rightarrow \{0,1\}^n\}_n$ be a family of constant-depth classical circuits (i.e., NC^0), and consider the following two distributions: C_n applied to any product distribution; and measuring $Q_n|0^n\rangle$ in the computational basis. The total variation distance between these two distributions is $1 - e^{-\Omega(n)}$.

Our distribution in Theorem 1.1 is based on a relational problem given by Watts, Kothari, Schaeffer, and Tal [WKST19] to strengthen the previously mentioned separation between NC^0 and QNC^0 [BGK18]. Despite this similar construction, our results are incomparable, as they lower bound the stronger class of AC^0 , but our results are in the distributional, rather than relational, setting.

[Theorem 1.1](#) may also be of modest philosophical interest. Recall that randomness extractors convert weak sources of randomness into a near uniform distribution. In influential work, Trevisan and Vadhan provided extractors for distributions produced by polynomial size circuits, claiming that these “sampl[e]able distributions are a reasonable model for distributions actually arising in nature” [\[TV00\]](#). A recent follow up by Ball, Goldin, Dachman-Soled, and Mutreja instead argues that a better choice for “natural sources” are those generated by quantum circuits, since the universe is governed by quantum phenomena [\[BGDSM23\]](#). Our main result shows that even in the extremely restricted circuit regime, these two beliefs dramatically differ.

Open Problems. The obvious next question in this line of inquiry, raised earlier in [\[WP23, Section 2\]](#), is whether a similar distributional separation exists between the classes of AC^0 and QNC^0 . In fact, it appears even the weaker task of separating AC^0 from QAC^0 (for sampling distributions) is open. There are several known distributions based on pseudorandom objects that cannot be accurately sampled in AC^0 [\[LV11, BIL12, Vio14, Vio20\]](#); it is unclear whether shallow quantum circuits can sample them. We remark that while our distribution is based on a problem from [\[WKST19\]](#) which separates AC^0 and QNC^0 for relational problems, our distribution *can* be sampled by an AC^0 circuit (see [Remark 5.10](#)).

Another direction is to refine the quantum gate set. The quantum circuits in our main separation result only require Hadamard, controlled-phase, and Toffoli gates, as opposed to the rotation gates required to generate the $(1/3)$ -biased product distribution used in previous separations [\[Vio23, KOW24\]](#). Still, one may wish to further limit the gate set, especially in light of the fact that Hadamard and Toffoli gates are quantum universal [\[Aha03\]](#). Unfortunately, the standard techniques to simulate the controlled-phase gates in this manner do not naively work in our setting (see [Subsection 4.1](#)), and we leave the minimal gate set required to separate NC^0 and QNC^0 for sampling distributions as an open question.

One final direction deserving of further investigation is hardness amplification for sampling. Our proof of [Theorem 1.1](#) crucially uses a direct product theorem for sampling in NC^0 (see [Subsection 5.4](#)), which allows us to amplify a weak separation between NC^0 and QNC^0 . A similar direct product theorem (or more generally, a hardness amplification result) for sampling in AC^0 would likely be useful in addressing open separations. Note that such a theorem was asked for by Chattopadhyay, Goodman, and Zuckerman [\[CGZ22\]](#) who gave an analogous result for read-once branching programs.

Paper Overview. We provide an overview of the proof of a precise version of [Theorem 1.1](#) in [Section 2](#). [Section 3](#) contains background material and several useful results applied in later sections. The quantum sampleability of [Theorem 1.1](#) is given in [Section 4](#), while the classical hardness of [Theorem 1.1](#) is in [Section 5](#). [Section 5](#) also contains various sampling schemes for related distributions and a direct product theorem for sampling in NC^0 .

2 The Proof Outline

In this section, we provide an overview of the proof of [Theorem 2.1](#) – a more precise and quantitative version of [Theorem 1.1](#) parameterized by *locality*. A function $f: \{0,1\}^* \rightarrow \{0,1\}^n$ is d -local if no output bit depends on more than d input bits. Note that any family of NC^0 circuits computes functions of constant locality. We will often refer directly to a distribution as d -local if it is the result of applying a d -local function to random inputs drawn from a product distribution.

Theorem 2.1. *Let $d \geq 1$ be an integer. There exists a constant $c_d > 0$ depending only on d such that the following holds. There is a uniform family of distributions $\{\mathcal{D}_n\}_{n \geq c_d}$ with $\mathcal{D}_n$ over $\{0, 1\}^n$ such that*

- *There exists a family of geometrically local depth-7 quantum circuits $\{C_n\}_{n \geq c_d}$ where $\mathcal{D}_n$ is produced exactly by C_n on input $|0^{2n}\rangle$. In addition, the quantum circuits only uses Hadamard, controlled-phase, CNOT, and Toffoli gates, and measurements in the computational basis. Moreover, Hadamard gates are only applied in the first and last layers, i.e., $\{C_n\}_n$ is in the second level of the Fourier Hierarchy [Shi05].*
- *For all $n \geq c_d$, $\mathcal{D}_n$ has total variation distance $1 - e^{-n/c_d}$ from any d -local distribution with any binary product distribution as input.*

Remark 2.2. Given Theorem 2.1, it is natural to wonder whether every distribution produced by NC^0 circuits can be sampled by QNC^0 circuits. The following example shows that this is not the case. Consider the distribution $\mathcal{P}$ over $\{0, 1\}^n$ which takes value 0^n with probability $1/2$ and 1^n otherwise. A classical circuit can easily produce $\mathcal{P}$ by having each output bit mirror the same input bit. QNC^0 circuits, however, cannot generate $\mathcal{P}$, as doing so is equivalent to preparing a nekomata (first defined in [Ros21]), i.e., a state of the form

$$|\psi\rangle = \frac{|0^n\rangle |\psi_0\rangle + |1^n\rangle |\psi_1\rangle}{\sqrt{2}}.$$

A lightcone argument shows that $\Omega(\log n)$ depth is necessary to prepare such a state, as is shown in [WKST19].

In Subsection 2.1, we will review the Parity Halving Problem of [WKST19], and explain how to derive a distributional version of the problem that can be exactly sampled by a shallow quantum circuit, but seemingly cannot be accurately sampled by a function of low locality. In Subsection 2.2, we will sketch a proof that this distribution has constant distance from every d -local distribution. That is, there is a distribution which exhibits a constant distance separation between classical and quantum sampling with shallow circuits. To boost this separation to an optimal one, we highlight and apply a direct product theorem implicit in [KOW24] in Subsection 2.3.

2.1 Quantum Sampling and a Classical Reduction

As mentioned, the authors of [WKST19] define the *Parity Halving Problem* (PHP): a relation problem over bit strings which is solvable by a shallow quantum circuit, but any randomized AC^0 (and therefore NC^0) circuit can only succeed on a trivial fraction of inputs. It is defined as follows:

Definition 2.3 (Parity Halving Problem). Given $x \in \{0, 1\}^n$ with $|x| \equiv 0 \pmod{2}$, return $y \in \{0, 1\}^n$ which satisfies $|y| \equiv \frac{|x|}{2} \pmod{2}$.

Their initial observation is that the PHP can be solved with certainty on all instances by a QNC^0 circuit with polynomial size quantum advice, i.e., PHP is in the class $\text{QNC}^0/\text{qpoly}$. This circuit is shown on the left in Figure 1.

To see that this circuit does indeed solve the PHP, note that after the CS gates are applied the resulting state is

$$|x\rangle \otimes \frac{|0^n\rangle + i^{x_1+\dots+x_n} |1^n\rangle}{\sqrt{2}} = |x\rangle \otimes \frac{|0^n\rangle + i^{|x|} |1^n\rangle}{\sqrt{2}} = \begin{cases} |x\rangle \otimes \frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}} & \text{if } |x| \equiv 0 \pmod{4}, \\ |x\rangle \otimes \frac{|0^n\rangle - |1^n\rangle}{\sqrt{2}} & \text{if } |x| \equiv 2 \pmod{4}. \end{cases}$$

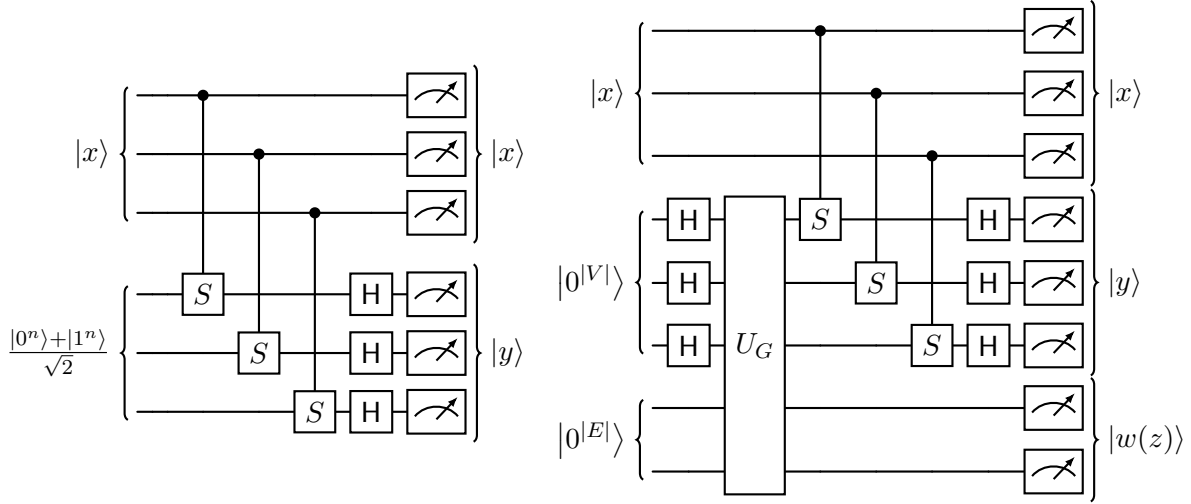


Figure 1: On the left is a $\text{QNC}^0/\text{qpoly}$ circuit which solves the Parity Halving Problem and on the right is a QNC^0 circuit which solves the Relaxed Parity Halving Problem over a graph $G = (V, E)$. Here U_G is the $(|V| + |E|)$ -qubit unitary which acts as $U_G |z\rangle |b\rangle = |z\rangle \bigotimes_{e=(u,v) \in E} |b_e \oplus z_u \oplus z_v\rangle$ for all $z \in \{0, 1\}^V$ and $b \in \{0, 1\}^E$.

Finally, applying $H^{\otimes n}$ to $\frac{|0^n\rangle + (-1)^b |1^n\rangle}{\sqrt{2}}$ yields a uniform superposition over bit strings of parity b .

In order to obtain a relational separation between NC^0 and QNC^0 without the need for quantum advice¹, the authors of [WKST19] define a variant of the PHP as follows:

Definition 2.4 (Relaxed Parity Halving Problem). Fix a graph $G = (V, E)$. Given $x \in \{0, 1\}^V$ with $|x| \equiv 0 \pmod{2}$, return $y \in \{0, 1\}^V$ and $w \in \{0, 1\}^E$ for which there exists $z \in \{0, 1\}^V$ such that

$$z_u \oplus z_v = w_{(u,v)} \quad \forall (u, v) \in E \quad \text{and} \quad |y| \equiv \langle z, x \rangle + \frac{|x|}{2} \pmod{2}.$$

If G has a cycle then it may not be the case that for each $w \in \{0, 1\}^E$ there exists a z such that w and z together satisfy the first condition above. However, when the underlying graph G is a tree then such a z exists for each w and preparing a “poor man’s cat state” suffices to solve the Relaxed Parity Halving Problem over G . A poor man’s cat state is a state proportional to $|z\rangle + |\bar{z}\rangle$ where $\bar{z}$ is the bitwise negation of z . The key observation is that there *is* a QNC^0 circuit which prepares a poor man’s cat state, conditioned on the measurement outcome of another register. Indeed, the state $\frac{1}{\sqrt{2^{|V|-1}}} \sum_{z \in \{0, 1\}^n, z_1=0} |w(z)\rangle \otimes \frac{|z\rangle + |\bar{z}\rangle}{\sqrt{2}}$ (where $w(z)$ and z satisfy the first constraint of Definition 2.4) can be prepared by a QNC^0 circuit so long as the maximum degree of G is constant. Finally, applying the PHP circuit, treating the Z register of the poor man’s cat state as if it were the cat state, yields a uniformly random string of parity $\frac{|x|}{2} + \langle x, z \rangle$.

This circuit is shown on the right in Figure 1. In order to obtain lower bounds against NC^0 for the (R)PHP, standard locality arguments apply.

Recall our goal is to construct a *distributional* separation. A reasonable first attempt might be to consider the distribution $\mathcal{D}_{\text{RPHP}}$ which is uniform over tuples (x, y, w) satisfying the relation. If generating this distribution is as hard as computing the RPHP relation, then classical hardness

¹Actually, the Relaxed Parity Halving Problem even serves to separate QNC^0 and AC^0 , but we make mention of it here as it serves as motivation for our sampling separation.

follows. Unfortunately, this is not the case. To gain some intuition, consider the classical PARITY function, which cannot be computed by shallow classical circuits [Hås86, Smo87], and yet, a simple NC⁰ circuit can sample from the distribution $(X, \text{PARITY}(X))$ where X is a uniformly random bit string [Bab87, BL87]. Specifically, one can map the random bits

$$y_1, y_2, \dots, y_n \rightarrow ((y_1 \oplus y_2) \circ (y_2 \oplus y_3) \circ \dots \circ (y_{n-1} \oplus y_n), y_1 \oplus y_n),$$

where $\circ$ denotes concatenation [Bab87, BL87]. In fact, a similar construction classically samples from $\mathcal{D}_{\text{RPHP}}$ (see Subsection 5.2).

We briefly digress to remark that this example is not an outlier. Indeed, the past decade or two has seen the study of sampling distributions blossom into a rich area, in many ways independent of computation, with exciting connections to fields such data structures [Vio12a, LV11, BIL12, Vio23, YZ24, KOW24], extractors [TV00, DW12, Vio12b, Vio14, BGDSM23], pseudorandom generators [Vio12a, LV11], and coding theory [SS24]. We refer the interested reader to the recent works [FLRS23, Vio23, KOW24, YZ24, SS24, KOW25] and references within for more details.

To overcome the above barrier, consider the strings (x, y, w) subject to the constraint $|x| \equiv 1 \pmod{2}$. The simple-but-key observation is that on input x with odd Hamming weight, the quantum circuit shown on the left in Figure 1 yields a uniformly random bit string y . (Note that w is always uniformly random.) Hence, if we replace $|x\rangle$ with some other state, we can now run our quantum circuit without necessarily invoking the promise on the Hamming weight of x , which gives us some added flexibility in our choice of distribution. In fact, we will simply replace each qubit with the single-qubit state $\sqrt{3/4}|0\rangle + \sqrt{1/4}|1\rangle$. That is, if we were to measure the qubits of the x -register, we would obtain the $(1/4)$ -biased distribution for each bit. It is exactly this distribution of inputs for which we can show classical hardness. In the following subsection, we will highlight exactly *why* this distribution does not suffer from the same shortcoming as the PARITY example.

Formally, the distribution witnessing the separation is defined as follows:

Definition 2.5 (The $\mathcal{D}_{\text{host}}(\mathcal{T})$ Distribution). Let $\mathcal{T} = (V, E)$ be a tree with undirected edges. A sample $(X, Y, W) \sim \mathcal{D}_{\text{host}}(\mathcal{T})$ is drawn as follows: first sample $X \sim \mathcal{U}_{1/4}^V$ and $Z \sim \mathcal{U}_{1/2}^V$. Define $W \in \{0, 1\}^E$ by setting $W_e = Z_u \oplus Z_v$ for each $e = \{u, v\} \in E$. If X has odd Hamming weight, then sample $Y \in \{0, 1\}^V$ uniformly at random; otherwise, sample Y as a uniform $|V|$ -bit string of parity $\langle Z, X \rangle + |X|/2 \pmod{2}$.

In Section 4, we show how to sample $\mathcal{D}_{\text{host}}(\mathcal{T})$ exactly using QNC⁰ circuits with the help of ancilla. The circuit is obtained by slightly modifying the construction given in [WKST19] for the RPHP:

Proposition 2.6. *Let $\mathcal{T} = (V, E)$ be a tree and let $\Delta \geq 2$ be its maximum vertex degree. Then there exists a geometrically local quantum circuit C such that the following holds.*

- *C has depth $2\Delta + 1$ and only uses Hadamard, controlled-phase, CNOT, and Toffoli gates. Moreover, Hadamard gates are only applied in the first and last layers.*
- *Let $\mathcal{P}$ be the distribution obtained by measuring $C|0^{|V|-1}\rangle$ in the computational basis. Then the marginal distribution of the first $3|V| - 1$ coordinates of $\mathcal{P}$ is exactly $\mathcal{D}_{\text{host}}(\mathcal{T})$.*

We refer to the target distribution as $\mathcal{D}_{\text{host}}$ because it essentially “hosts” the following distribution, $\mathcal{D}_{\text{hard}}(n, m)$, defined below:

Definition 2.7 (The $\mathcal{D}_{\text{hard}}(n, m)$ Distribution). A sample $(x, y) \sim \mathcal{D}_{\text{hard}}(n, m)$ is drawn as follows: first sample $x \sim \mathcal{U}_{1/4}^n$ according to the $(1/4)$ -biased product distribution. If x has odd Hamming weight, then sample $y \in \{0, 1\}^m$ uniformly at random; otherwise x has even Hamming weight, and sample y as a uniform m -bit string of parity $|x|/2 \pmod{2}$.

$\mathcal{D}_{\text{hard}}$ is the distribution which we are able to prove classical hardness for in a more straightforward way. Observe that the relationship between $\mathcal{D}_{\text{hard}}$ and $\mathcal{D}_{\text{host}}$ is analogous to that between the PHP and RPHP. The reduction from $\mathcal{D}_{\text{host}}$ to $\mathcal{D}_{\text{hard}}$ is given in [Subsection 5.3](#).

Lemma 2.8. *Let $\mathcal{T} = (V, E)$ be a tree and let $v^* \in V$ be arbitrary. Define $K = \sum_{v \in V} |P_v|$, where P_v is the set of edges on the unique path between v^* and v . Then there exists a 5-local function $\text{red}: \{0, 1\}^{3|V|-1} \times \{0, 1\}^* \rightarrow \{0, 1\}^{2|V|+K}$ such that*

$$\text{red}(\mathcal{D}_{\text{host}}(\mathcal{T}), \mathcal{U}_{1/2}^*) = \mathcal{D}_{\text{hard}}(|V|, |V| + K).$$

2.2 Classical Hardness

The classical lower bound of [Theorem 2.1](#) is largely derived from the following hardness result. Let $\text{tow}(x)$ denote the tower of 2's of height x (e.g., $\text{tow}(3) = 2^{2^2}$).

Theorem 2.9. *Let $d \geq 1$ be an integer. Assume $n \geq \text{tow}(30d)$ and $m \leq n^2/\text{tow}(30d)$. Then any d -local distribution has total variation distance at least 0.24 from $\mathcal{D}_{\text{hard}}(n, m)$.*

Combining [Theorem 2.9](#) with [Lemma 2.8](#) easily gives the following corollary.

Corollary 2.10. *Let $\mathcal{T} = (V, E)$ be a tree and let $v^* \in V$ be arbitrary. Define $K = \sum_{v \in V} |P_v|$, where P_v is the set of edges on the unique path between v^* and v . Additionally, let $d \geq 1$ be an integer, and assume $|V| \geq \text{tow}(30(d+5))$ and $|V| + K \leq |V|^2/\text{tow}(30(d+5))$. Then any d -local distribution has total variation distance at least 0.24 from $\mathcal{D}_{\text{host}}(\mathcal{T})$.*

Proof. Assume by contradiction there exists a d -local function $f: \{0, 1\}^* \rightarrow \{0, 1\}^{3|V|-1}$ and a product distribution Π over $\{0, 1\}^*$ such that the distribution of f applied to samples drawn from Π , denoted $f(\Pi)$, is δ -close to $\mathcal{D}_{\text{host}}(\mathcal{T})$ for some $\delta < 0.24$. Define a new function $g: \{0, 1\}^* \rightarrow \{0, 1\}^{2|V|+K}$ by

$$g(\Pi) = \text{red}(f(\Pi), \{0, 1\}^*),$$

where red is defined as in [Lemma 2.8](#). Then g is $(d+5)$ -local by [Lemma 2.8](#) and δ -close to $\mathcal{D}_{\text{hard}}(|V|, |V| + K)$ by the data processing inequality. This contradicts [Theorem 2.9](#). $\square$

Before sketching the main ideas behind the proof of [Theorem 2.9](#), a few remarks are in order. First, a tighter analysis can yield distance $\frac{1}{4} - \varepsilon$, assuming $m \leq O_\varepsilon(n^2/\text{tow}(30d))$; this is near optimal, as the 2-local² distribution $\mathcal{U}_{1/4}^n \times \mathcal{U}_{1/2}^m$ achieves distance $\frac{1}{4} - o(1)$. Second, the quadratic upper bound on m in [Theorem 2.9](#) is necessary; we show $\mathcal{D}_{\text{hard}}(n, m)$ is $O(1)$ -local when $m \geq \Omega(n^2)$ in [Proposition 5.8](#). Finally, it is necessary that $x \sim \mathcal{U}_{1/4}^n$ and not $x \sim \mathcal{U}_{1/2}^n$, as the latter can be exactly sampled (see [Proposition 5.9](#)), though any bias other than 0, 1, or 1/2 will be hard.

Let us now provide an overview of [Theorem 2.9](#)'s proof. Fix an arbitrary d -local function $f: \{0, 1\}^* \rightarrow \{0, 1\}^{n+m}$ and an arbitrary product distribution Π over $\{0, 1\}^*$ as input. Our goal is to show that the distribution $f(\Pi)$ is 0.24-far from $\mathcal{D}_{\text{hard}}(n, m)$. One immediate challenge in working with d -local functions is that the locality constraint is “one-sided.” Even though no output bit is influenced by many input bits, there may exist an input bit that affects every single output bit. The resulting output distribution, then, can have complicated correlations, which muddle the analysis.

²The distribution is 2-local if the input bits are unbiased coins. When we allow input bits with mixed bias of 1/4 and 1/2, the distribution is 1-local.

The Structured Case: A First Attempt. To warm-up, we first consider the idealized setting where there are r “non-connected” output bits, by which we mean no two such output bits depend on a common input bit. In particular, the r marginal distributions of $f(\Pi)$ projected onto the individual coordinates are independent. Here, one should view r as large, say $\Omega_d(n)$. We proceed via a concentration vs. anticoncentration dichotomy, present in various forms in the works [Vio12a, FLRS23, Vio23, KOW24, KOW25]. Specifically, we classify each of the r output bits according to how their corresponding marginal distribution compares to the marginal distribution of the target distribution.

At a high level, we would like to argue that either many of these output bits have marginal distributions which are far from those of the target distribution, in which case we can combine the marginal errors, or many of these output bits are close to the “correct” marginal distribution, in which case a more complicated anticoncentration argument shows that a specific potential function highlights a noticeable discrepancy between the two distributions. To this end, we call an output bit b **Type-1** if the marginal distribution $f(\Pi)|_b$ is δ -far in total variation distance from the marginal distribution $\mathcal{D}_{\text{hard}}(n, m)|_b$, and call it **Type-2** otherwise. Here, $\delta = O_d(1)$ is some small threshold parameter.

Suppose at least $r/2$ of the non-connected output bits are **Type-1**. Note that since total variation distance is closed under projection, a single **Type-1** neighborhood already gives distance δ . To strengthen the bound, one can take advantage of independence and apply standard concentration inequalities, as in the proof of [KOW24, Lemma 4.2], to conclude $f(\Pi)$ has distance roughly $1 - e^{-\delta^2 \cdot r}$ from $\mathcal{D}_{\text{hard}}(n, m)$.³ For $r \gg 1/\delta^2$, this is at least 0.24, as desired.

The more involved case is when at least $r/2$ output bits are **Type-2**. Here, rather than directly comparing $f(\Pi)$ to $\mathcal{D}_{\text{hard}}(n, m)$, we compare the expectation of a complex-valued potential function $h(x, y) = i^{|x|+2|y|}$ over samples (x, y) drawn from the two distributions. Direct calculations show that $\mathbb{E}_{x,y}[h(x, y)] \approx 1/2$ for $(x, y) \sim \mathcal{D}_{\text{hard}}(n, m)$ (see Claim 5.3) and that $|\mathbb{E}[i^A]|$ is bounded away from 1 for any integral random variable A suitably far from constant modulo 4 (see Claim 5.5). It is tempting to argue that by the independence of the non-connected output bits, we can fix the value of the input bits not affecting any **Type-2** output bits to view $\mathbb{E}_{x,y}[h(x, y)]$ as a product of many independent random variables with magnitudes bounded away from 1. Then we could conclude that for each of these input conditionings, $|\mathbb{E}_{x,y}[h(x, y)]| \ll 0.01$ for $(x, y) \sim f(\Pi)$, which would give the desired distance of 0.24 (using Lemma 3.4).

The problem, however, is that the contributions of the remaining output bits can compensate for those of the non-connected output bits. For example, consider the string $z_1, 1 - z_1, z_2, 1 - z_2, \dots, z_k, 1 - z_k$, where the z_k ’s are independent random bits. There are k independent bits, yet the string’s Hamming weight is fixed at k . Thus, we cannot reason about $\mathbb{E}_{x,y}[h(x, y)]$ solely from the non-connected output bits. Instead, we need to consider the *neighborhood* of each output bit b , i.e., the set of output bits that are also influenced by the input bits determining b .

The Structured Case: Refining the Output Structure. To fix our analysis, let us change our assumption from there being r non-connected output bits to there being r non-connected neighborhoods. Here, we refer to two neighborhoods N_1, N_2 as non-connected if for every pair of output bits $b_1 \in N_1$ and $b_2 \in N_2$, the input bits that determine b_1 are disjoint from those that determine b_2 . We can similarly classify each neighborhood as **Type-1** or **Type-2** depending on the distance of its marginal distribution to that of the target distribution. The analysis in the case of

³There is a small subtlety here, in that if the set of **Type-1** output bits fully contains the last m output bits, then those output bits are not a product distribution in $\mathcal{D}_{\text{hard}}(n, m)$. For simplicity, we will assume that this does not occur, although the full statement of [KOW24, Lemma 4.2] is robust enough to still apply in that scenario.

many **Type-1** neighborhoods is performed almost identically to the previous scenario, but now we are able to reason more carefully when there are many **Type-2** neighborhoods.

Indeed, consider a **Type-2** neighborhood $N = (x', y')$, where x' is the output bits contained in the first n indices (corresponding to x) and y' is the output bits contained in the latter m indices (corresponding to y). If we can show that $|x'| + 2|y'| \pmod{4}$ is not too close to being a constant, then the potential function argument sketched above can actually be carried out. To this end, let b be the output bit that defines the neighborhood $N = N(b)$, and consider the effect of conditioning on $b = 0$ vs. on $b = 1$.

First suppose b is in the x part. In this case, we can write $x' = (b, x'')$ and express $|x'| + 2|y'| \pmod{4}$ as $b + |x''| + 2|y'| \pmod{4}$. Recall that N is a **Type-2** neighborhood, so it should resemble a product distribution. In particular, the distribution of $|x''| + 2|y'| \pmod{4}$ conditioned on $b = 0$ should be roughly the same as when conditioned on $b = 1$. Observe then, that $1 + |x''| + 2|y'| \pmod{4}$ and $|x''| + 2|y'| \pmod{4}$ should have noticeably different distributions, as we are essentially comparing a binomial distribution with its shift. Since b should be close to $(1/4)$ -biased, it takes both values with constant probability, so $|x'| + 2|y'| \pmod{4}$ cannot be too close to any fixed value. A similar analysis shows that if b is in the y part, then we are comparing the density of $|x'| + 2|y'| \pmod{4}$ and $|x'| + 2(|y'| + 1) \pmod{4}$.

Unfortunately, there is a problem with this latter case. Suppose the neighborhood N does not contain any bits in the x part. Then we are comparing the density of $2|y'| \pmod{4}$ and $2(|y'| + 1) \pmod{4}$, or equivalently, $|y'| \pmod{2}$ and $|y'| + 1 \pmod{2}$. The y part is $(1/2)$ -biased, so $|y'| \pmod{2}$ *can* have the same distribution as $|y'| + 1 \pmod{2}$! Note that it is this fact which allows for the previously described sampling algorithm for (X, PARITY) . Hence, we must make one further refinement to our assumption.

The Structured Case: A Final Adjustment. Now instead of simply assuming there are r non-connected neighborhoods, we insist that all r neighborhoods are generated by output bits in the x part. Moreover, we will only require the non-connectedness property on bits in the x part of the neighborhoods. This second condition actually makes the analysis more challenging, but we will later see it is necessary for this model case to be obtainable. We once more redefine **Type-1** and **Type-2** neighborhoods; this time we classify neighborhoods based only on their marginals on the first n output bits. The case of many **Type-1** neighborhoods essentially works as before (see [Lemma 5.2](#)), so it remains to address the case where at least $r/2$ of the neighborhoods are **Type-2**.

To obtain some structure in the y part, we exploit our assumption on the size of m . Since we have $m \leq n^2/\text{tow}(30d)$, most pairs of neighborhoods do not intersect in the last m output bits. Quantitatively, we can find $C \approx r^2/(md^2) \gg 1$ non-connected **Type-2** neighborhoods that do not intersect in the y part. Without loss of generality, assume they are $N(1), N(2), \dots, N(C)$. By fixing the value of all the input bits that do not affect $1, 2, \dots, C$, the contributions to h from these neighborhoods are now independent. In particular, the expectation of h becomes a product of expectations over the output of the neighborhood. As noted above, we can conclude the expectation over the neighborhood $N = (x', y')$ is bounded away from 1 if $|x'| + 2|y'| \pmod{4}$ is not too close to any fixed value.

This ends up being a bit difficult to show directly, since while the C neighborhoods are disjoint in the y part, they may be connected. Fortunately, the variance of $|x'| + 2|y'| \pmod{4}$ over a random such fixing of the input bits follows from that of $|x'| \pmod{2}$, where we do have non-connectedness in the x part. By the previous argument of considering $|x'|$ conditioned on the output bit b being 0 vs. being 1, we are able to prove $|x'| \pmod{2}$ is typically not too close to constant (see [Claim 5.7](#)). This concludes the analysis of many **Type-2** neighborhoods (see [Lemma 5.6](#)), as well as the proof

of [Theorem 2.1](#) under certain ideal assumptions.

Reduction to the Structured Case. Previously, we assumed a rather strong structure: $r = \Omega_d(n)$ many output bits generating neighborhoods that are non-connected in $[n]$. This, of course, is not a structure readily present in an arbitrary d -local function f . To reduce to this case, a standard approach (appearing in, e.g., [[Vio12a](#), [BGK18](#), [Vio20](#), [FLRS23](#), [Vio23](#), [KOW24](#), [KOW25](#)]) is to strategically condition on bits to express an arbitrary d -local function as a convex combination of functions with the desired structure. In other words, if we can find some set S of input bits whose removal induces many non-connected neighborhoods of the form we want, then we can express $f(\Pi)$ as

$$f(\Pi) = \mathbb{E}_{\rho \in \{0,1\}^S} [f_\rho(\Pi)],$$

where $f_\rho: \{0,1\}^* \rightarrow \{0,1\}^{n+m}$ is defined as f with the input bits in S fixed to their values in ρ . Observe that each f_ρ has the structured form we already know how to analyze, regardless of the actual values the bits in S are set to. More formally, we have:

1. If most of the non-connected neighborhoods are **Type-1**, then $f_\rho(\Pi)$ is $\approx (1 - e^{-\Omega_d(r)})$ -far from $\mathcal{D}_{\text{hard}}(n, m)$, and
2. Otherwise, $\mathbb{E}_{(x,y) \sim \mathcal{D}_{\text{hard}}(n,m)}[h(x, y)] - \mathbb{E}_{(x,y) \sim f_\rho(\Pi)}[h(x, y)] \geq 0.49$.

By a union bound argument (see [Lemma 3.4](#)), these results on the conditioned functions can be combined to obtain $\|f(\Pi) - \mathcal{D}_{\text{hard}}(n, m)\|_{\text{TV}} \gtrsim 0.245 - 2^{|S|} \cdot e^{-\Omega_d(r)}$. Then as long as $r \gg |S|$, we obtain the desired distance bound of 0.24.

At this point, the remaining task is combinatorial. We construct a bipartite graph whose left side is the first n output bits, and whose right side is the input bits. Note that each left vertex has maximum degree d . We want to remove s right vertices to obtain r non-connected neighborhoods of the prescribed form, where $r \gg s$. Ideally, we would like r to be as large as possible to maximize the total variation distance. Fortunately, this task has already been done for us. By [[KOW24](#), Corollary 4.11], we can take $s \ll r$ and $r = \Omega_d(n)$, as desired.

For the sake of completeness, we briefly highlight the main idea behind the proof of [[KOW24](#), Corollary 4.11]. The key observation is that locality, while only explicitly constraining the left vertices, also constrains the right ones, since it upper bounds the number of edges by dn . Thus while we cannot forbid high-degree right vertices, there cannot be many of them. This implies that we can “affordably” remove all right vertices above a particular degree threshold, and greedily find non-connected vertices on the left side. A more involved analysis (see [[KOW24](#), Corollary 4.8]) provides better parameters than one could obtain via this naive approach, and an even more involved analysis guarantees non-connected left neighborhoods, rather than just vertices. Still, the proofs morally operate in a similar way to the strategy described. This completes the sketch of the proof of [Theorem 2.1](#); the full details can be found in [Section 5](#).

We conclude by remarking that the above analysis is fairly robust, and it allows one to rule out the sampleability of a number of simple distributions by shallow circuits. Thus, the specific distributions we have chosen to consider are primarily a function of what can be produced by shallow quantum circuits, rather than what can be forbidden for shallow classical ones.

2.3 Boosting the Separation

Combining our results thus far produces a separation with constant total variation distance. In order to prove the stronger separation in [Theorem 2.1](#), we consider the distribution $\mathcal{D}_{\text{host}}(\mathcal{T})^k =$

$\mathcal{D}_{\text{host}}(\mathcal{T}) \times \cdots \times \mathcal{D}_{\text{host}}(\mathcal{T})$. Certainly, if our quantum circuit can generate $\mathcal{D}_{\text{host}}(\mathcal{T})$, then it can also generate $\mathcal{D}_{\text{host}}(\mathcal{T})^k$. Moreover, we can apply the following direct product theorem implicit in [KOW24] (and formalized in Subsection 5.4) to show the overlap of the target distribution with that produced by classical circuits decays exponentially quickly.

Theorem 2.11 (Direct Product Theorem). *Let $d, \ell \geq 1$ be integers, and let $\mathcal{D}$ be a distribution over $\{0, 1\}^\ell$. Suppose that for any d -local function $f: \{0, 1\}^* \rightarrow \{0, 1\}^\ell$ and binary product distribution Π on $\{0, 1\}^*$, we have*

$$\|f(\Pi) - \mathcal{D}\|_{\text{TV}} \geq \delta.$$

Then for any integer $k \geq 1$, d -local function $g: \{0, 1\}^ \rightarrow \{0, 1\}^{\ell k}$, and binary product distribution Ξ on $\{0, 1\}^*$, we have*

$$\|g(\Xi) - \mathcal{D}^k\|_{\text{TV}} \geq 1 - 4 \exp \left\{ - \left(\frac{\delta^2}{16d\ell} \right)^{4d\ell} \cdot k \right\}.$$

The proof of Theorem 2.11, much like the proof of Theorem 2.1, uses a graph elimination result derived in [KOW24]. In this context, such a result allows one to find many independent groups of output bits corresponding to instances of $\mathcal{D}$. Since the marginal distributions of $\mathcal{D}$ and $f(\Pi)$ disagree on each group, we can use a standard concentration inequality to derive a strong error bound.

Proof of Theorem 2.1. Let $n = \text{tow}(40d)$, and let $\mathcal{T} = (V, E)$ be the spanning tree of the $\sqrt{n} \times \sqrt{n}$ square grid obtained by including all the edges in the first row, as well as all the edges in each column. Observe that the diameter of $\mathcal{T}$ is $3\sqrt{n}$, so K (as defined in Corollary 2.10) is at most $3n^{3/2}$. In particular, our choice of n guarantees $|V| + K \leq |V|^2 / \text{tow}(30(d+5))$. Thus, Corollary 2.10 implies any d -local distribution is at least 0.24-far from $\mathcal{D}_{\text{host}}(\mathcal{T})$. Applying Theorem 2.11, we can boost this error to conclude that any d -local distribution has distance from $\mathcal{D}_{\text{host}}(\mathcal{T})^k$ at least

$$1 - 4 \exp \left\{ - \left(\frac{0.24^2}{16d(3n-1)} \right)^{4d(3n-1)} \cdot k \right\}.$$

Let $c_d > 0$ be a sufficiently large constant depending only on d . For any integer $N \geq c_d$, express $N = k \cdot (3n-1) + r$ with $0 \leq r < 3n-1$, and define the distribution $\mathcal{D}_N = \mathcal{D}_{\text{host}}(\mathcal{T})^k \times 0^r$. Since total variation distance is closed under projection, we find that any d -local distribution has distance from $\mathcal{D}_N$ at least

$$1 - 4 \exp \left\{ - \left(\frac{0.24^2}{16d(3n-1)} \right)^{4d(3n-1)} \cdot \frac{N-r}{3n-1} \right\} \geq 1 - e^{-N/c_d}$$

for large enough c_d .

We conclude by noting that Proposition 2.6 gives a depth-7 quantum circuit that exactly samples $\mathcal{D}_{\text{host}}(\mathcal{T})^k$ on input $|0^{k(5n-1)}\rangle$ by considering the marginal distribution on $k(3n-1)$ specific coordinates. By padding with r extra zeros, a similar circuit on $k(5n-1) + r \leq 2N$ inputs can also sample $\mathcal{D}_N$. $\square$

Remark 2.12. Our setting of $\mathcal{T}$ is motivated by common topological choices in implementations. One could alternatively set $\mathcal{T}$ to be a balanced binary tree to minimize K , but this would not affect the final bound.

3 Preliminaries

In this section, we collect a number of definitions, notation, and useful results, many of which are taken from [KOW24].

We use $\mathbb{C}, \mathbb{R}, \mathbb{Z}, \mathbb{N}$ to denote the set of complex, real, integer, and natural numbers, respectively. For a positive integer n , we use $[n]$ to denote the set $\{1, 2, \dots, n\}$, and use $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$ to denote the additive group modulo n . We use i to denote the imaginary unit satisfying $i^2 = -1$. For a binary string x , we use $|x|$ to denote its Hamming weight. We use $\log(x)$ to denote the logarithm with base 2. For $x \in \mathbb{N}$, we use $\text{tow}(x)$ to denote the power tower of base 2 and order x , where

$$\text{tow}(x) = \begin{cases} 1 & x = 0, \\ 2^{\text{tow}(x-1)} & x \geq 1. \end{cases}$$

Asymptotics. We use the standard $O(\cdot), \Omega(\cdot), \Theta(\cdot)$ notation, and emphasize that in this paper they only hide universal positive constants that do not depend on any parameter. Occasionally we will use subscripts to suppress a dependence on particular variable (e.g., $O_d(1)$).

Probability. For $\gamma \in [0, 1]$, we use $\mathcal{U}_\gamma$ to denote the γ -biased distribution, i.e., $\mathcal{U}_\gamma(1) = \gamma = 1 - \mathcal{U}_\gamma(0)$. Let $\mathcal{P}$ be a (discrete) distribution. We use $x \sim \mathcal{P}$ to denote a random sample x drawn from the distribution $\mathcal{P}$. If $\mathcal{P}$ is a distribution over a product space, then we say $\mathcal{P}$ is a product distribution if its coordinates are independent. In addition, for any non-empty set $S \subseteq [n]$, we use $\mathcal{P}|_S$ to denote the marginal distribution of $\mathcal{P}$ on coordinates in S . For a deterministic function f , we use $f(\mathcal{P})$ to denote the output distribution of $f(x)$ given a random $x \sim \mathcal{P}$.

For every event $\mathcal{E}$, we define $\mathcal{P}(\mathcal{E})$ to be the probability that $\mathcal{E}$ happens under distribution $\mathcal{P}$, and we use $\mathcal{P}(x)$ to denote the probability mass of x under $\mathcal{P}$. We will make use the following standard concentration inequality.

Fact 3.1 (Chernoff's Inequality). *Assume $X_1, \dots, X_n$ are independent random variables such that $X_i \in [0, 1]$ holds for all $i \in [n]$. Let $\mu = \sum_{i \in [n]} \mathbb{E}[X_i]$. Then for all $\delta \in [0, 1]$, we have*

$$\Pr \left[\sum_{i \in [n]} X_i \leq (1 - \delta)\mu \right] \leq \exp \left\{ -\frac{\delta^2 \mu}{2} \right\}.$$

Let $\mathcal{P}_1, \dots, \mathcal{P}_t$ be distributions. Then $\mathcal{P}_1 \times \dots \times \mathcal{P}_t$ is a distribution denoting the product of $\mathcal{P}_1, \dots, \mathcal{P}_t$. We also use $\mathcal{P}^t$ to denote $\mathcal{P}_1 \times \dots \times \mathcal{P}_t$ if each $\mathcal{P}_i$ is the same distribution as $\mathcal{P}$. For a finite set S , we use $\mathcal{P}^S$ to emphasize that coordinates of $\mathcal{P}^{|S|}$ are indexed by elements in S . We say a distribution $\mathcal{P}$ is a convex combination, or mixture, of $\mathcal{P}_1, \dots, \mathcal{P}_t$ if there exist $\alpha_1, \dots, \alpha_t \in [0, 1]$ such that $\sum_{i \in [t]} \alpha_i = 1$ and $\mathcal{P} = \sum_{i \in [t]} \alpha_i \cdot \mathcal{P}_i$. That is, $\mathcal{P}(\mathcal{E}) = \sum_{i \in [t]} \alpha_i \cdot \mathcal{P}_i(\mathcal{E})$ for every event $\mathcal{E}$.

Let $\mathcal{Q}$ be a distribution. We use $\|\mathcal{P} - \mathcal{Q}\|_{\text{TV}} = \frac{1}{2} \sum_x |\mathcal{P}(x) - \mathcal{Q}(x)|$ to denote their total variation distance.⁴ We say $\mathcal{P}$ is ε -close to $\mathcal{Q}$ if $\|\mathcal{P}(x) - \mathcal{Q}(x)\|_{\text{TV}} \leq \varepsilon$, and ε -far otherwise.

Fact 3.2. *Total variation distance has the following equivalent characterizations:*

$$\|\mathcal{P} - \mathcal{Q}\|_{\text{TV}} = \max_{\text{event } \mathcal{E}} \mathcal{P}(\mathcal{E}) - \mathcal{Q}(\mathcal{E}) = \min_{\substack{\text{random variable } (X, Y) \\ X \text{ has marginal } \mathcal{P} \text{ and } Y \text{ has marginal } \mathcal{Q}}} \Pr[X \neq Y].$$

⁴To evaluate total variation distance, we need two distributions to have the same sample space. This will be clear throughout the paper and thus we omit it for simplicity.

We will later need the following basic results about total variation distance. The first says that two distributions on a product space must be far apart if their individual marginals are far apart. The proof is a straightforward application of Hoeffding's inequality.

Lemma 3.3 ([KOW24, Lemma 4.2]). *Let $\mathcal{P}$ and $\mathcal{W}$ be distributions over an n -dimensional product space, and let $B \subseteq [n]$ be a non-empty set of size b . Assume*

- $\mathcal{P}|_B$ and $\mathcal{W}|_B$ are product distributions, and
- $\|\mathcal{P}|_{\{i\}} - \mathcal{W}|_{\{i\}}\|_{\text{TV}} \geq \varepsilon$ holds for all $i \in B$.

Then

$$\|\mathcal{P} - \mathcal{W}\|_{\text{TV}} \geq 1 - 2 \cdot e^{-\varepsilon^2 b/2}.$$

The second result says that if multiple distributions are either far from a specific distribution in total variation distance or in expectation of a potential function, then so too is any convex combination of those distributions. It follows from a union bound argument.

Lemma 3.4 ([KOW25, Lemma 4.7]⁵). *Let $\mathcal{P}_1, \dots, \mathcal{P}_\ell$ and $\mathcal{Q}$ be distributions. Let ϕ be a function with output range $[a, b]$ where $a < b$. Assume for each $i \in [\ell]$,*

$$\text{either } \|\mathcal{P}_i - \mathcal{Q}\|_{\text{TV}} \geq 1 - \eta_1 \quad \text{or} \quad \mathbb{E}_{X \sim \mathcal{Q}}[\phi(X)] - \mathbb{E}_{X \sim \mathcal{P}_i}[\phi(X)] \geq \eta_2,$$

where $\eta_2 \leq b - a$. Then for any distribution $\mathcal{P}$ expressible as a convex combination of $\mathcal{P}_1, \dots, \mathcal{P}_\ell$, we have

$$\|\mathcal{P} - \mathcal{Q}\|_{\text{TV}} \geq \frac{\eta_2}{b - a} - (\ell + 1) \cdot \eta_1.$$

Finally, we will require the following standard fact that two distributions which are close in total variation distance remain close after conditioning. A proof can be found in [KOW24, Appendix C].

Fact 3.5. *Assume $\mathcal{P}$ is ε -close to $\mathcal{Q}$, and let $\mathcal{P}', \mathcal{Q}'$ be the distributions of $\mathcal{P}, \mathcal{Q}$ conditioned on some event $\mathcal{E}$, respectively. Then for any function f ,*

$$\|f(\mathcal{P}') - f(\mathcal{Q}')\|_{\text{TV}} \leq \frac{2\varepsilon}{\mathcal{Q}(\mathcal{E})}.$$

Locality. Let $\{0, 1\}^*$ denote the set of finite length bit strings. Throughout the paper, we will often be working with functions of the form $g: \{0, 1\}^* \rightarrow \{0, 1\}^n$. Here, however, we will fix the domain size for concreteness and clarity. That is, let $f: \{0, 1\}^m \rightarrow \{0, 1\}^n$. For each output bit $i \in [n]$, we use $I_f(i) \subseteq [m]$ to denote the set of input bits that the i^{th} output bit depends on. We say f is a d -local function if $|I_f(i)| \leq d$ holds for all $i \in [n]$. Define $N_f(i) = \{i' \in [n]: I_f(i) \cap I_f(i') \neq \emptyset\}$ to be the neighborhood of i , which contains all the output bits that have potential correlation with the i^{th} output bit.

We say output bit i_1 is connected to i_2 if $I_f(i_1) \cap I_f(i_2) \neq \emptyset$. We say neighborhood $N_f(i_1)$ is connected to $N_f(i_2)$ if there exist $i'_1 \in N_f(i_1)$ and $i'_2 \in N_f(i_2)$ such that $I_f(i'_1) \cap I_f(i'_2) \neq \emptyset$. As such, every output bit is independent of any non-connected output bit, and the output of a neighborhood has no correlation with any non-connected neighborhood of it. When f is clear from the context, we will drop subscripts in $I_f(i), N_f(i)$ and simply use $I(i), N(i)$.

In some abuse of standard terminology, we will often discuss the locality of *distributions*. We may say a certain property holds for d -local distributions, by which we mean that property holds for $f(\Pi)$ for every d -local function $f: \{0, 1\}^* \rightarrow \{0, 1\}^n$ and binary product distribution Π over $\{0, 1\}^*$.

⁵This lemma is not present in the most up-to-date arXiv version of [KOW25], but it can be found in <https://arxiv.org/pdf/2411.08183v1>, which matches the version originally published in STOC'25.

Bipartite Graphs. We sometimes take an alternative view, using bipartite graphs to model the dependency relations in f . Let $G = (V_1, V_2, E)$ be an undirected bipartite graph. For each $i \in V_1$, we use $I_G(i) \subseteq V_2$ to denote the set of adjacent vertices in V_2 . We say G is d -left-bounded if $|I_G(i)| \leq d$ holds for all $i \in V_1$. Define $N_G(i) = \{i' \in V_1 : I_G(i) \cap I_G(i') \neq \emptyset\}$ to be the left neighborhood of i .

We say left vertex i_1 is connected to i_2 if $I_G(i_1) \cap I_G(i_2) \neq \emptyset$. We say left neighborhood $N_G(i_1)$ is connected to $N_G(i_2)$ if there exist $i'_1 \in N_G(i_1)$ and $i'_2 \in N_G(i_2)$ such that $I_G(i'_1) \cap I_G(i'_2) \neq \emptyset$. When G is clear from the context, we will drop subscripts in $I_G(i)$, $N_G(i)$ and simply use $I(i)$, $N(i)$.

It is easy to see that the dependency relation in $f: \{0, 1\}^m \rightarrow \{0, 1\}^n$ can be visualized as a bipartite graph $G = G_f$ where $[n]$ is the left vertices (representing output bits of f) and $[m]$ is the right vertices (representing input bits of f), and an edge $(i, j) \in [n] \times [m]$ exists if and only if $j \in I_f(i)$. The notation and definitions of $I_f(i)$ and $N_f(i)$ are then equivalent to those of $I_G(i)$ and $N_G(i)$.

We will require the following two “graph elimination” results of [KOW24]. They first lets us find many non-connected vertices, while the second lets us find many non-connected neighborhoods.

Lemma 3.6 ([KOW24, Corollary 4.8]). *Let $\beta, \lambda \geq 1$ be parameters (not necessarily constant), and let $G = ([n], [m], E)$ be a d -left-bounded bipartite graph with $d \geq 1$. If*

$$\lambda \geq 2d \cdot (2d\beta + 1)^{2d},$$

then there exists $S \subseteq [m]$ such that deleting those right vertices (and their incident edges) produces a bipartite graph with r non-connected left vertices satisfying

$$|S| \leq \frac{r}{\beta} \quad \text{and} \quad r \geq \frac{n}{\lambda}.$$

Lemma 3.7 ([KOW24, Corollary 4.11]). *Let $\lambda, \kappa \geq 1$ be parameters (not necessarily constant), $F(\cdot)$ be an increasing function, and $G = ([n], [m], E)$ be a d -left-bounded bipartite graph with $d \geq 1$. Define*

$$\tilde{F}(x) = \frac{1}{d} \cdot \exp \{32d^4 x^2 \cdot F(2d \cdot x)\}.$$

Assume $H(\cdot)$ is an increasing function and $H(x) \geq \tilde{F}(x)$ for all $x \geq L$ where $L \geq 1$ is some parameter not necessarily constant. If $H(x) \geq 2x$ for all $x \geq L$ and

$$F(x) \geq 1 \text{ holds for all } x \geq 1 \quad \text{and} \quad \kappa \geq \lambda \geq d \cdot H^{(2d+2)}(L),$$

where $H^{(k)}$ is the iterated H of order k ,⁶ then there exists $S \subseteq [m]$ such that deleting those right vertices (and their incident edges) produces a bipartite graph with r non-connected left neighborhoods of size at most t satisfying

$$|S| \leq \frac{r}{F(t)} \quad \text{and} \quad r \geq \frac{n}{\lambda} \quad \text{and} \quad t \leq \kappa.$$

Classical and Quantum Circuits. Throughout this work we will (mostly implicitly) consider Boolean circuits which consist of AND, OR, and NOT gates. Moreover, we will be primarily concerned with NC circuits, i.e., those circuits where the number of ingoing wires to any gate in the circuit is bounded by a constant. Further, we shall focus on families of circuits of constant depth. Formally,

⁶ $H^{(1)}(x) = H(x)$ and $H^{(k)}(x) = H(H^{(k-1)}(x))$ for $k \geq 2$.

Definition 3.8 (NC⁰ Circuits). Let $\mathcal{C} = \{C_n\}_{n \geq 1}$ be a family of circuits where C_n takes n input bits and produces $m(n)$ output bits for some $m: \mathbb{N} \rightarrow \mathbb{N}$. $\mathcal{C}$ is said to be an NC⁰ family of circuits if there exists a constant d such that the depth of C_n is at most d for all $n \geq 1$.

We will occasionally specify a circuit family as *(logspace) uniform*, by which we mean every gate can be specified by a deterministic computation using $O(\log n)$ space.

We will also be interested in the quantum analogue of NC⁰ circuits. Quantum circuits are unitary operators that act on $(\mathbb{C}^2)^{\otimes n}$ where $\mathbb{C}^2$ is spanned by $\{|0\rangle, |1\rangle\}$ here. An n -qubit quantum state is any vector $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ with unit ℓ_2 -norm. For $x \in \{0, 1\}^n$ we use $|x\rangle$ to denote the element $|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$, and the set $\{|x\rangle\}_{x \in \{0, 1\}^n}$ will be referred to as the *computational basis*.

In general, a quantum circuit is any unitary operator obtained by composing several layers of non-overlapping gates from some prescribed set of unitary operators, i.e., the *gate set*. The *depth* of a quantum circuit is the number of layers of gates which make up the circuit. In this work we are interested in the restricted class of quantum circuits called QNC⁰ circuits:

Definition 3.9. Let $\mathcal{C} = \{C_n\}_{n \geq 1}$ be a family of quantum circuits where C_n acts on n qubits. $\mathcal{C}$ is said to be a QNC⁰ family of circuits if there exist constants c_1 and c_2 such that for all $n \geq 1$, C_n consists only of gates acting on at most c_1 qubits and C_n has depth at most c_2 .

While these circuits may in general consist of arbitrary gates of constant locality, we will only consider QNC⁰ circuits with a very particular gate set. These gates are defined as follows:

- H, the Hadamard gate, acts on a single qubit as $H|b\rangle = \frac{|0\rangle + (-1)^b|1\rangle}{\sqrt{2}}$ for $b \in \{0, 1\}$
- CNOT, the Controlled-Not gate, acts on two qubits as $\text{CNOT}|a\rangle|b\rangle = |a\rangle|a \oplus b\rangle$ for $a, b \in \{0, 1\}$
- Tof, the Toffoli gate, acts on three qubits as $\text{Tof}|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|(a \wedge b) \oplus c\rangle$ for $a, b \in \{0, 1\}$
- CS, the controlled-phase gate, acts on two qubits as $\text{CS}|a\rangle|b\rangle = i^{a \wedge b}|a\rangle|b\rangle$ for $a, b \in \{0, 1\}$

When physically realizing a quantum circuit the property of *geometric locality* is often very desirable. A quantum circuit is said to be geometrically local if the circuit can be implemented on a 2D grid of qubits with all multi-qubit gates acting on adjacent qubits.

4 The QNC⁰ Upper Bound

In this section, we show how to exactly generate the distribution $\mathcal{D}_{\text{host}}$ with a shallow quantum circuit.

Proposition 2.6. Let $\mathcal{T} = (V, E)$ be a tree and let $\Delta \geq 2$ be its maximum vertex degree. Then there exists a geometrically local quantum circuit C such that the following holds.

- C has depth $2\Delta + 1$ and only uses Hadamard, controlled-phase, CNOT, and Toffoli gates. Moreover, Hadamard gates are only applied in the first and last layers.
- Let $\mathcal{P}$ be the distribution obtained by measuring $C|0^{|V|-1}\rangle$ in the computational basis. Then the marginal distribution of the first $3|V| - 1$ coordinates of $\mathcal{P}$ is exactly $\mathcal{D}_{\text{host}}(\mathcal{T})$.

Proof. Let $v^* \in V$ be arbitrary. We start with $|0^{|V|}\rangle_X |0^{|V|}\rangle_Z |0^{|E|}\rangle_W |0^{2|V|}\rangle_A$ where A is an ancilla register. The circuit proceeds as follows: first, apply $H^{\otimes 2|V|}$ on $|0^{2|V|}\rangle_A$, followed by 3-qubit Toffoli gates to compute $|V|$ 3-bit ANDs on X on uniform inputs. If the X and A registers are measured in

the computational basis, we obtain $X = x$ and $A = (a, a')$. Note that x is $(1/4)$ -biased and (a, a') is uniform conditioned on $a \wedge a' = x$ (where the $\wedge$ is taken bit-wise). Next, we apply $H^{\otimes |V|}$ to the Z -register to obtain $|+\rangle_Z^{|V|} |0\rangle_W^{|E|}$. For each $v \in V$ and each edge $e = (v, u) \in E$ which is incident to v we apply a **CNOT** gate from the Z -register qubit corresponding to v onto the W -register qubit corresponding to edge $e = (u, v)$. Note that each edge qubit is the target of exactly two **CNOT** gates.

Consider a coloring of the edges of the graph such that no two edges which share a vertex are assigned the same color. By Brooks' Theorem any bipartite graph admits such a coloring which uses at most Δ colors. Since none of the edges of the same color are overlapping, we can apply the corresponding **CNOT** gates in two layers. Hence, all **CNOT** gates can be applied in depth 2Δ . After these **CNOTs** are applied we are left with

$$|x\rangle \otimes U_{\mathcal{T}} \left(|+\rangle^{\otimes |V|} |0\rangle^{|E|} \right) = |x\rangle \otimes \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}} |z\rangle |w(z)\rangle,$$

where $w(z)_{(u,v)} = z_u \oplus z_v$ for all $(u, v) \in E$ and $U_{\mathcal{T}}$ is the previously described sequence of **CNOTs**. Observe that $w(z) = w(\bar{z})$ where $\bar{z}_v = z_v \oplus 1$. Hence, this state can be written as

$$|x\rangle \otimes \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}} |z\rangle_Z |w(z)\rangle = |x\rangle \otimes \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}, z_1=0} (|z\rangle + |\bar{z}\rangle) |w(z)\rangle.$$

Next, for each qubit of x we apply a controlled-phase gate between it and the corresponding qubit in the Z register. This yields

$$|x\rangle \otimes \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}, z_1=0} (i^{\langle x, z \rangle} |z\rangle + i^{\langle x, \bar{z} \rangle} |\bar{z}\rangle) |w(z)\rangle.$$

Finally, we apply $H^{\otimes n}$ to the Z register after which all qubits are measured in the computational basis. A diagram of this circuit is shown in [Figure 2](#). The Toffoli gates and $U_{\mathcal{T}}$ can be applied in parallel as they act on non-overlapping qubits, yielding a final depth count of $2\Delta + 1$.

It remains to show that random variables corresponding to the measurement outcomes obtained on the X, Z , and W registers are distributed according to $\mathcal{D}_{\text{host}}$. The state just on the Z register before applying the last layer of Hadamard gates is

$$\begin{aligned} \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}, z_1=0} i^{\langle x, z \rangle} |z\rangle + i^{\langle x, \bar{z} \rangle} |\bar{z}\rangle &= \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}, z_1=0} i^{\langle x, z \rangle} (|z\rangle + i^{|x|-2\langle x, \bar{z} \rangle} |\bar{z}\rangle) \\ &= \frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}, z_1=0} i^{\langle x, z \rangle} (|z\rangle + (-1)^{|x|/2 - \langle x, \bar{z} \rangle} |\bar{z}\rangle). \end{aligned}$$

Recall that for any $z \in \{0,1\}^n$

$$\begin{aligned} H^{\otimes n} \frac{|z\rangle + (-1)^b |\bar{z}\rangle}{\sqrt{2}} &= \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} ((-1)^{\langle y, z \rangle} + (-1)^{b + \langle y, \bar{z} \rangle}) |y\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{\langle y, z \rangle} (1 + (-1)^{b + |y|}) |y\rangle. \end{aligned}$$

The result is a superposition over strings of parity b , meaning that measuring after the last layer of Hadamards on the Z register yields a bit string of parity $\frac{|x|}{2} + \langle x, z \rangle$ whenever $|x|$ is even. If $|x|$ is odd then the state on Z before applying the final layer of Hadamards is

$$\frac{1}{\sqrt{2^{|V|}}} \sum_{z \in \{0,1\}^{|V|}, z_1=0} i^{x,z} (|z\rangle + i^{|x|-2\langle x, \bar{z} \rangle} |\bar{z}\rangle).$$

Note that for any $z \in \{0,1\}^{|V|}$ and $b \in \{0,1\}$

$$H^{\otimes n} \frac{|z\rangle + i^{2b+1} |\bar{z}\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^{|V|}}} \sum_{y \in \{0,1\}^{|V|}} \frac{(-1)^{\langle x, z \rangle} + i^{2(b+\langle x, \bar{z} \rangle)+1}}{\sqrt{2}} |y\rangle.$$

Hence, when $|x|$ is odd, measuring the Z register will yield a uniformly random outcome - in either case the string, w , measured on the W -register will satisfy $w_{(u,v)} = z_u \oplus z_v$ for all $(u,v) \in E$; the final layer of Hadamards on Z will not affect this. This means that the X, Z , and W registers of $C |0^{5|V|-1}\rangle$ are distributed exactly as $\mathcal{D}_{\text{host}}$ when measured in the computational basis. $\square$

It should be noted that the Toffoli gates in our construction are only used to produce a state whose single-qubit marginals are $(1/4)$ -biased, i.e., measure $|0\rangle$ with probability $3/4$ and $|1\rangle$ with probability $1/4$. These Toffoli gates may be replaced by any other gate which produces such a bias, like $R_Y(\pi/6) = \begin{pmatrix} \sqrt{3/4} & -1/2 \\ 1/2 & \sqrt{3/4} \end{pmatrix}$, and the construction presented would work much the same. In fact, the resulting measurement distribution on all qubits would be exactly $\mathcal{D}_{\text{host}}$, i.e., we would not need to ignore any qubits. One slightly undesirable property of the $R_Y(\pi/6)$ gate (and any other single-qubit gate which generates the desired $1/4$ -biased marginal) is that this gate may be used to obtain states whose amplitudes do not have magnitude which squares to a dyadic rational. Explicitly, one can obtain a constant-depth quantum circuit using R_Y and H which samples exactly from a product distribution which is only hard for NC^0 because the one-bit marginal bias is irrational: $HR_Y |0\rangle = \frac{\sqrt{3}+1}{2\sqrt{2}} |0\rangle + \frac{\sqrt{3}-1}{2\sqrt{2}} |1\rangle$.

This issue does not arise with the Toffoli gate; the unitary computed by the circuit shown in [Figure 2](#) has entries with magnitudes that square to dyadic rational values. As such, the resulting separation does not rely on any sort of precision limitation inherent in classical sampling circuits.

Further, our construction can be made geometrically local, where all gates only act on adjacent sets of qubits with the qubits arranged on a 2D grid layout.

4.1 Toward A Minimal Gate Set?

In the previous construction the gate set used is $\{H, \text{CS}, \text{CNOT}, \text{Tof}\}$. Note that CNOT can be simulated by applying Tof with an additional ancilla set to $|1\rangle$, i.e.,

$$\text{Tof} |1\rangle |a, b\rangle = (\mathbb{I} \otimes \text{CNOT}) |1\rangle |a, b\rangle.$$

Thus, one can construct a constant-depth circuit consisting only of gates from the set $\{H, \text{CS}, \text{Tof}\}$ whose output distribution is not NC^0 -sampleable. This begs the question: *Is this gate set a minimal set for achieving such a separation?* It is well known that H and Tof are sufficient for universal quantum computation [[Aha03](#)], so it may be tempting to simulate the CS gate in our construction via H and Tof . The standard method for such a simulation involves representing arbitrary n -qubit states as $(n+1)$ -qubit states which only have real amplitudes in the following way:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \rightarrow \sum_{x \in \{0,1\}^n} |x\rangle \otimes (\Re(\alpha_x) |0\rangle + \Im(\alpha_x) |1\rangle) = |\psi'\rangle.$$

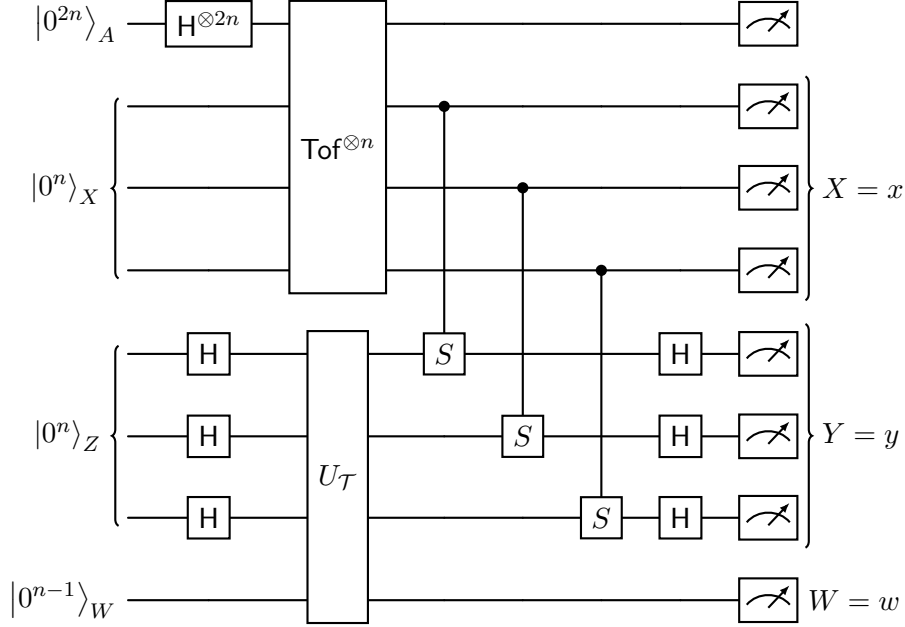


Figure 2: A depiction of the QNC^0 circuit whose measurement distribution on the last $3n - 1$ qubits is exactly $\mathcal{D}_{\text{host}}(\mathcal{T})$. Here $U_{\mathcal{T}}$ is the $(2n - 1)$ -qubit unitary which acts as $U_{\mathcal{T}}|z\rangle|b\rangle = |z\rangle \bigotimes_{e=(u,v)\in E} |b_e \oplus z_u \oplus z_v\rangle$ - as shown in the proof of [Proposition 2.6](#) $U_{\mathcal{T}}$ can be implemented via CNOTs in depth 2Δ . While the circuit shown above is not geometrically local, a rearrangement of the qubit wires would allow for all CNOT, Tof, and CS gates to act only on adjacent qubits in a $2D$ -grid architecture.

Indeed, if C is the circuit from [Proposition 2.6](#) with $C|0^m\rangle = |\psi\rangle$ and C' satisfies $C'|0^{m'}\rangle = |\psi'\rangle$, then the measurement distribution of $|\psi'\rangle$ would be identical to that of $|\psi\rangle$ on the appropriate subset of qubits. Recall that CS acts as $\text{CS}|x, y\rangle = i^{x \wedge y} |x, y\rangle$, so the 3-qubit real unitary which it corresponds to acts as

$$\text{CS}'|x, y, z\rangle = (-1)^{x \wedge y \wedge z} |x, y, z \oplus (x \wedge y)\rangle.$$

In our construction we apply CS on n disjoint pairs of qubits in a single layer, but doing so with the standard simulation technique of [\[Aha03\]](#) would require super-constant depth as these CS' gates would overlap on the last qubit (that qubit which maintains the real and imaginary parts of each amplitude). Hence, it remains unclear if the $\{\text{H}, \text{CS}, \text{Tof}\}$ gate set is minimal for the separation exhibited here. We leave this direction for future work.

5 The NC^0 Lower Bound

The goal of this section is to establish the classical results required for the separation in [Theorem 2.1](#). In [Subsection 5.1](#), we prove that any bounded locality distribution must have constant distance from $\mathcal{D}_{\text{hard}}$ (i.e., [Theorem 2.9](#)). [Subsection 5.2](#) contains some sampling algorithms that justify our parameter choices in [Theorem 2.9](#). We then prove [Lemma 2.8](#) in [Subsection 5.3](#) to reduce the hardness of $\mathcal{D}_{\text{host}}$ to that of $\mathcal{D}_{\text{hard}}$. Finally, we formalize a direct product theorem in [Subsection 5.4](#) to boost the distance from constant to $1 - o(1)$.

5.1 A Weak Lower Bound

We begin by proving [Theorem 2.9](#), restated below.

Theorem 2.9. *Let $d \geq 1$ be an integer. Assume $n \geq \text{tow}(30d)$ and $m \leq n^2/\text{tow}(30d)$. Then any d -local distribution has total variation distance at least 0.24 from $\mathcal{D}_{\text{hard}}(n, m)$.*

Let $f: \{0, 1\}^* \rightarrow \{0, 1\}^{n+m}$ be an arbitrary d -local function, and let Π be an arbitrary product distribution on $\{0, 1\}^*$. Our goal is to show $f(\Pi)$ is at least 0.24-far from $\mathcal{D}_{\text{hard}}(n, m)$.

Recall that for each $i \in [n + m]$, $I(i)$ is the set of input bits that the i^{th} output bit depends on, and $N(i)$ is the neighborhood of the i^{th} output bit, i.e., the set of output bits sharing common input bits with i . Let S be a subset of input bits. We define $I_S(i) = I(i) \setminus S$ and use $N_S(i)$ to denote the neighborhood of the i^{th} output bit after fixing the inputs in S . Note that these definitions do not depend on how we fix the bits in S .

Our first step in proving [Theorem 2.9](#) is to obtain a choice of S such that conditioning on the bits in S reduces $f(\Pi)$ to a more structured distribution.

Lemma 5.1. *There exist*

$$s \leq \frac{r}{2^{20t}}, \quad r \geq \frac{n}{\text{tow}(20d)}, \quad t \leq \text{tow}(20d)$$

and distinct indices $i_1, \dots, i_r \in [n]$ and a subset S of size $|S| \leq s$ such that the following holds.

1. $I_S(u) \cap I_S(v) = \emptyset$ for all distinct $j, j' \in [r]$, any $u \in N_S(i_j) \cap [n]$, and any $v \in N_S(i_{j'}) \cap [n]$.
2. Each $N_S(i_j) \cap [n]$ has size at most t .

Proof. Recall we may associate to f a bipartite graph whose right and left parts are the set of input and output bits, respectively. Here, we take the left part to only consist of the output bits in $[n]$. The conclusion will then follow from [Lemma 3.7](#). Set $F(x) = 2^{20x}$ so that

$$\tilde{F}(x) = \frac{1}{d} \cdot \exp \left\{ 32d^4 x^2 \cdot 2^{40dx} \right\}.$$

Define $H(x) = 2^{2^{2x}}$, $L = 10 \log(2d)$, and $\kappa = \lambda = \text{tow}(20d)$. Then $H(x) \geq \tilde{F}(x) \geq 2x$ for all $x \geq L$, $F(x) \geq 1$ for all $x \geq 1$, and $\kappa, \lambda \geq H^{(2d+2)(L)}$, so we can apply [Lemma 3.7](#) to conclude the proof. $\square$

For each conditioning $\rho \in \{0, 1\}^S$ on the bits in S , define the restricted function f_ρ as f but with the input bits in S fixed to ρ . We split our analysis into two cases depending on the behavior of the marginal distributions of $N_S(i_j) \cap [n]$ for $i_1, \dots, i_r$ from [Lemma 5.1](#). For each $j \in [r]$, we say i_j is **Type-1** in f_ρ if the marginal distribution of $f_\rho(\Pi)$ on $N_S(i_j) \cap [n]$ is 2^{-5t} -far from the $(1/4)$ -biased product distribution; we say i_j is **Type-2** in f_ρ otherwise.

We first handle the easy case where **Type-1** indices are abundant.

Lemma 5.2. *If there are at least $r/2$ Type-1 indices in f_ρ , then $f_\rho(\Pi)$ is $(1 - 2 \exp \{-r/2^{12t}\})$ -far from $\mathcal{D}_{\text{hard}}(n, m)$.*

The proof is similar to that of [\[KOW24, Lemma 5.14\]](#).

Proof. By rearranging the indices if necessary, we may assume without loss of generality that $1, 2, \dots, r/2$ are **Type-1** indices in f_ρ . That is,

$$\|f_\rho(\Pi)|_{N_S(i) \cap [n]} - \mathcal{D}_{\text{hard}}(n, m)|_{N_S(i) \cap [n]}\|_{\text{TV}} \geq 2^{-5t}$$

for all $i \in [r/2]$. Let $R = [n] \setminus (N_S(1) \cup \dots \cup N_S(r/2))$ be the output bits in $[n]$ that are not contained in any of the first $r/2$ neighborhoods. We will apply [Lemma 3.3](#) with $\mathcal{P}, \mathcal{W}, B$ defined as follows:

- $\mathcal{P}$ is $f_\rho(\Pi)$ restricted to the output bits in $[n]$, but with each neighborhood and R viewed as individual coordinates. That is,

$$\mathcal{P} = (f_\rho(\Pi)|_{N_S(1) \cap [n]}, f_\rho(\Pi)|_{N_S(2) \cap [n]}, \dots, f_\rho(\Pi)|_{N_S(r/2) \cap [n]}, R)$$

is a distribution over a product space of $(r/2) + 1$ coordinates.

- $\mathcal{W}$ is the $(1/4)$ -biased product distribution over $[n]$, but grouped in the same way as $\mathcal{P}$.
- $B = [r/2]$.

Observe that $\mathcal{P}|_B$ and $\mathcal{W}|_B$ are both product distributions, since any pair of restricted neighborhoods $N_S(i) \cap [n]$ and $N_S(j) \cap [n]$ for distinct $i, j \in [r/2]$ do not share input bits by [Lemma 5.1](#). Thus, we may apply [Lemma 3.3](#) with the parameters defined above, as well as the data processing inequality, to conclude

$$\|f_\rho(\Pi) - \mathcal{D}_{\text{hard}}(n, m)\|_{\text{TV}} \geq 1 - 2 \exp\left\{-(2^{-5t})^2 \cdot r/4\right\} \geq 1 - 2 \exp\left\{-r \cdot 2^{-12t}\right\}. \quad \square$$

To analyze Type-2 indices, we will use the following potential function $h: \{0, 1\}^{n+m} \rightarrow \mathbb{C}$:

$$h(x, y) = i^{|x|}(-1)^{|y|} = i^{|x|+2|y|}, \quad \text{where } x \in \{0, 1\}^n, y \in \{0, 1\}^m.$$

We will show that $\mathbb{E}[h(x, y)] \approx 1/2$ when $(x, y) \sim \mathcal{D}_{\text{hard}}(n, m)$, but $\mathbb{E}[h(x, y)]$ is far from $1/2$ when $(x, y) \sim f_\rho(\Pi)$. Later, we will leverage this discrepancy using [Lemma 3.4](#).

Claim 5.3. Assume $(x, y) \sim \mathcal{D}_{\text{hard}}(n, m)$. Then $\mathbb{E}_{x, y}[h(x, y)] = \frac{1}{2} + \left(\frac{1}{2}\right)^{n+1}$.

Proof. If $|x|$ is even, then $h(x, y) \equiv 1$; otherwise $\mathbb{E}_y[h(x, y)] = 0$. Thus,

$$\begin{aligned} \mathbb{E}_{x, y}[h(x, y)] &= \mathbf{Pr}_x[|x| \text{ is even}] = \frac{1}{2} + \frac{\mathbf{Pr}_x[|x| \text{ is even}] - \mathbf{Pr}_x[|x| \text{ is odd}]}{2} \\ &= \frac{1}{2} + \frac{\sum_{i=0}^n \binom{n}{i} (-1)^i (1/4)^i (3/4)^{n-i}}{2} \\ &= \frac{1}{2} + \frac{((-1/4) + (3/4))^n}{2} = \frac{1}{2} + \frac{1}{2^{n+1}}. \quad \square \end{aligned}$$

To analyze h for $f_\rho(\Pi)$, we will need the following lemma. It essentially says that two coupled $(1/4)$ -biased vectors will differ in Hamming weight modulo 2 a noticeable fraction of time, as long as part of the vectors are independent. Note that the statement and proof are similar to that of [\[KOW24, Lemma 4.4\]](#).

Lemma 5.4. Let (A, B, C, D) be a random variable where $A, C \in \{0, 1\}$ and $B, D \in \{0, 1\}^{t-1}$. Assume

- A is independent from (B, D) and B is independent from (A, C) ,
- (A, C) and (B, D) have the same marginal distribution and are 2^{-5t} -close to $\mathcal{U}_{1/4}^t$.

Then we have

$$\mathbf{Pr}[A + |C| \equiv B + |D| \pmod{2}] \leq 1 - 2^{-3t}.$$

Proof. If $t = 1$ then $\Pr[A + |C| \equiv B + |D| \pmod{2}] = \Pr[A = B]$. Since A and B are independent and of the same distribution 2^{-5t} -close to $\mathcal{U}_{1/4}^1$, we have $\Pr[A = 1] = \Pr[B = 1] \in [1/4 - 2^{-5t}, 1/4 + 2^{-5t}]$. Hence,

$$\Pr[A = B] = \Pr[A = 1]^2 + (1 - \Pr[A = 1])^2 \leq \left(\frac{1}{4} - 2^{-5t}\right)^2 + \left(1 - \frac{1}{4} + 2^{-5t}\right)^2 \leq 1 - 2^{-2t}. \quad (1)$$

Now we assume $t \geq 2$. Expand $\Pr[A + |C| \equiv B + |D| \pmod{2}]$ as

$$\sum_{a,b \in \{0,1\}} \Pr[A = a, B = b] \Pr[a + |C| \equiv b + |D| \pmod{2} | A = a, B = b]. \quad (2)$$

For fixed a and b , consider the distribution of $a + |C| \pmod{2}$ conditioned on $A = a, B = b$. Since B is independent from (A, C) , it is the same as the distribution, denoted by $\mathcal{P}_a$, of $a + |C| \pmod{2}$ conditioned on $A = a$. Similarly define $\mathcal{Q}_b$ as the distribution of $b + |D| \pmod{2}$ conditioned on $B = b$ (or equivalently, conditioned on $B = b, A = a$).

Since (A, C) is 2^{-5t} -close to $\mathcal{U}_{1/4}^t$, by [Fact 3.5](#), $\mathcal{P}_0$ is $(3 \cdot 2^{-5t})$ -close to $\mathcal{D}_0$, the distribution of $|V| \pmod{2}$ for $V \sim \mathcal{U}_{1/4}^{t-1}$. Similarly, $\mathcal{Q}_1$ is $(8 \cdot 2^{-5t})$ -close to $\mathcal{D}_1$, the distribution of $1 + |V| \pmod{2}$ for $V \sim \mathcal{U}_{1/4}^{t-1}$. Hence,

$$\begin{aligned} \Pr[|C| \equiv 1 + |D| \pmod{2} | A = 0, B = 1] &\leq 1 - \|\mathcal{P}_0 - \mathcal{Q}_1\|_{\text{TV}} && \text{(by Fact 3.2)} \\ &\leq 1 + 11 \cdot 2^{-5t} - \|\mathcal{D}_0 - \mathcal{D}_1\|_{\text{TV}}. \end{aligned}$$

Note that

$$\|\mathcal{D}_0 - \mathcal{D}_1\|_{\text{TV}} = \Pr_{V \sim \mathcal{U}_{1/4}^{t-1}}[|V| \text{ is even}] - \Pr_{V \sim \mathcal{U}_{1/4}^{t-1}}[|V| \text{ is odd}] = \left(\frac{1}{2}\right)^{t-1},$$

where the final equality follows from an identical calculation to that within the proof of [Claim 5.3](#). Substituting into the previous inequality yields

$$\Pr[|C| \equiv 1 + |D| \pmod{2} | A = 0, B = 1] \leq 1 + 2^{-5t+4} - 2^{-t+1}.$$

The same bound holds for $\Pr[1 + |C| \equiv |D| \pmod{2} | A = 1, B = 0]$. Plugging back into (2) and using (1), we have

$$\begin{aligned} \Pr[A + |C| \equiv B + |D| \pmod{2}] &\leq \Pr[A = B] + \Pr[A \neq B] \cdot (1 + 2^{-5t+4} - 2^{-t+1}) \\ &\leq 1 - 2^{-2t} \cdot (2^{-t+1} - 2^{-5t+4}) \\ &\leq 1 - 2^{-3t}. \end{aligned} \quad \square$$

We also need the following fact which shows deficiency in taking expectation of h for a slightly biased random source.

Claim 5.5. Let A be an integral random variable. Assume $\max_{a \in \mathbb{Z}/4\mathbb{Z}} \Pr[A \equiv a \pmod{4}] \leq 1 - \eta$. Then

$$|\mathbb{E}[i^A]| \leq 1 - \frac{\eta}{4}.$$

Proof. By a simple averaging argument, we must have $\eta \leq 3/4$. For each $a \in \{0, 1, 2, 3\}$, define $p_a = \Pr[A \equiv a \pmod{4}]$. Assume without loss of generality that $p_1, p_2, p_3 \leq p_0 \leq 1 - \eta$. Then

$$|\mathbb{E}[i^A]|^2 = |(p_0 - p_2) + (p_1 - p_3) \cdot i|^2 = (p_0 - p_2)^2 + (p_1 - p_3)^2$$

$$\begin{aligned}
&\leq p_0^2 + \max\{p_1^2, p_3^2\} \leq p_0^2 + \max\{p_1, p_2, p_3\}^2 \\
&\leq (1 - \eta)^2 + \eta^2 = 1 - 2\eta(1 - \eta) \\
&\leq 1 - \frac{\eta}{2},
\end{aligned}$$

where we used $\eta \leq 3/4$ in the last line. Thus, $|\mathbb{E}[i^A]| \leq \sqrt{1 - \frac{\eta}{2}} \leq 1 - \frac{\eta}{4}$. $\square$

Now we show that $\mathbb{E}[h(x, y)]$ cannot be close to $\frac{1}{2}$ in $f_\rho(\Pi)$ if it has many **Type-2** indices.

Lemma 5.6. *If there are at least $r/2$ **Type-2** indices in f_ρ , then we have*

$$\left| \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x, y)] \right| \leq 2 \exp \left\{ -\frac{r^2}{m \cdot d^2 \cdot 2^{3t+9}} \right\}.$$

Proof. By rearranging the indices if necessary, we may assume without loss of generality that $1, 2, \dots, r/2$ are **Type-2** indices in f_ρ . That is,

$$\|f_\rho(\Pi)|_{N_S(i) \cap [n]} - \mathcal{D}_{\text{hard}}(n, m)|_{N_S(i) \cap [n]}\|_{\text{TV}} \leq 2^{-5t}$$

for all $i \in [r/2]$. We now build a bipartite graph G between $[r/2]$ and $[n+m] \setminus [n]$ by connecting $i \in [r/2]$ and $j \in [n+m] \setminus [n]$ if and only if $I_S(i) \cap I_S(j) \neq \emptyset$, or equivalently, $j \in N_S(i)$. (Note that this bipartite graph is different from the one we often associate with a local function to visualize its input/output bit dependencies.)

Since f (and thus f_ρ) is d -local and $I_S(i) \cap I_S(j) = \emptyset$ for all distinct $i, j \in [r/2]$, each $j \in [n+m] \setminus [n]$ has degree at most d in G . Hence G has at most dm edges. Therefore there are at most

$$\frac{4md^2C}{r} \leq \frac{r}{4} \tag{3}$$

indices $i \in [r/2]$ with degree more than $\frac{r}{4dC}$, where $C \geq 1$ is a parameter satisfying (3) to be tuned later. We discard these high degree indices and continue with the at least $r/4$ remaining ones. By construction, each remaining index connects to at most $\frac{r}{4dC}$ many $j \in [n+m] \setminus [n]$, and each $j \in [n+m] \setminus [n]$ connects to at most d different $i \in [r/2]$, so we can greedily find C indices $i \in [r/2]$ that have disjoint neighborhoods in G .

Without loss of generality, assume these indices are $1, 2, \dots, C$. In summary, they satisfy the following conditions.

1. $I_S(u) \cap I_S(v) = \emptyset$ for all distinct $i, i' \in [C]$, any $u \in N_S(i) \cap [n]$, and any $v \in N_S(i') \cap [n]$.

This comes from [Lemma 5.1](#) directly.

2. $N_S(i) \cap [n]$ has size at most t for all $i \in [C]$.

This comes from [Lemma 5.1](#) directly.

3. In $f_\rho(\Pi)$, the marginal distribution on $N_S(i) \cap [n]$ is 2^{-5t} -close to the $(1/4)$ -biased product distribution for all $i \in [C]$.

This comes from the definition of a **Type-2** index.

4. $N_S(i) \cap N_S(i') = \emptyset$ for all distinct $i, i' \in [C]$.

This comes from [Lemma 5.1](#) and the selection procedure above.

For each $i \in [C]$, let $T_i = N_S(i) \cap [n]$ and $T'_i = N_S(i) \cap [n+m] \setminus [n]$; and let $X_i \in \{0,1\}^{T_i}$, $X'_i \in \{0,1\}^{T'_i}$ be the output bits of $f_\rho(\Pi)$ in T_i, T'_i respectively. Additionally, define $R = [n] \setminus \left(\bigcup_{i \in [C]} T_i\right)$ and $R' = ([n+m] \setminus [n]) \setminus \left(\bigcup_{i \in [C]} T'_i\right)$; and let $Y \in \{0,1\}^R$, $Y' \in \{0,1\}^{R'}$ be the output bits of $f_\rho(\Pi)$ in R, R' respectively. Then for $(x, y) \sim f_\rho(\Pi)$, we have

$$h(x, y) = \left(\prod_{i \in [C]} i^{|X_i|+2|X'_i|} \right) \cdot i^{|Y|+2|Y'|}.$$

Let J be the set of input bits outside $\bigcup_{i \in [C]} I(i)$, so that fixing the bits in J will fix Y and Y' . For each $\sigma \in \{0,1\}^J$ and $i \in [C]$, define

$$p_{\sigma,i} = \max_{a \in \mathbb{Z}/4\mathbb{Z}} \Pr[|X_i| + 2|X'_i| \equiv a \pmod{4} \mid \sigma].$$

Note that if σ is fixed, then the (X_i, X'_i) 's are pairwise independent by [Item 4](#). Hence we have

$$\begin{aligned} \left| \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x, y) \mid \sigma] \right| &= \left| \mathbb{E}_{X_i, X'_i, \forall i \in [C]} \left[\prod_{i \in [C]} i^{|X_i|+2|X'_i|} \mid \sigma \right] \right| && \text{(since } \sigma \text{ fixes } Y, Y') \\ &= \prod_{i \in [C]} \left| \mathbb{E}_{X_i, X'_i} [i^{|X_i|+2|X'_i|} \mid \sigma] \right| && \text{(by independence)} \\ &\leq \prod_{i \in [C]} \left(1 - \frac{1 - p_{\sigma,i}}{4} \right) && \text{(by Claim 5.5)} \\ &\leq \exp \left\{ -\frac{1}{4} \sum_{i \in [C]} (1 - p_{\sigma,i}) \right\}, && (4) \end{aligned}$$

where the final inequality uses $1 - c \leq e^{-c}$.

It remains to show that $\sum_{i \in [C]} (1 - p_{\sigma,i})$ is typically not too small (i.e., for most restrictions σ and indices i , the value of $|X_i| + 2|X'_i| \pmod{4}$ has reasonable variance). For this, we first analyze the related quantities

$$q_{\sigma,i} = \max_{a \in \mathbb{Z}/2\mathbb{Z}} \Pr[|X_i| \equiv a \pmod{2} \mid \sigma].$$

The benefit of working with $q_{\sigma,i}$'s is that they are independent with respect to randomly chosen σ , since the X_i 's depend on disjoint sets of input bits by [Item 1](#). This will be necessary later to apply standard concentration inequalities. Note that such independence may not hold for $p_{\sigma,i}$'s, as we have only shown that the neighborhoods $N_S(i)$ are pairwise disjoint for $i \in [C]$, but they could still depend on common input bits. The upshot is that we can easily relate $p_{\sigma,i}$ and $q_{\sigma,i}$. Fix an arbitrary $\sigma \in \{0,1\}^J$ and index $i \in [C]$, and let $a \in \mathbb{Z}/4\mathbb{Z}$ maximize $p_{\sigma,i}$. Observe that we can write $a = b_1 + 2b_2$ for some $b_1, b_2 \in \{0,1\}$. Then,

$$\begin{aligned} p_{\sigma,i} &= \Pr[|X_i| + 2|X'_i| \equiv a \pmod{4} \mid \sigma] \\ &= \Pr[|X_i| \equiv b_1 + 2(b_2 - |X'_i|) \pmod{4} \mid \sigma] \\ &\leq \Pr[|X_i| \equiv b_1 \pmod{2} \mid \sigma] \leq q_{\sigma,i}. \end{aligned} \tag{5}$$

We are now free to focus on analyzing $q_{\sigma,i}$. From here, the remainder of the proof is similar to that of [\[KOW24, Lemma 5.15\]](#). Below, we will consider σ as being sampled according to the marginal distribution of Π projected onto the coordinates in J .

Claim 5.7. For each $i \in [C]$, we have $\mathbb{E}_\sigma \left[(q_{\sigma,i})^2 \right] \leq 1 - 2^{-3t}$.

For clarity, we will complete the proof of [Lemma 5.6](#) before proving [Claim 5.7](#). By Jensen's inequality, [Claim 5.7](#) implies

$$\mathbb{E}_\sigma [1 - q_{\sigma,i}] \geq 1 - \sqrt{\mathbb{E}_\sigma \left[(q_{\sigma,i})^2 \right]} \geq 2^{-3t-1}.$$

As noted above, the $q_{\sigma,i}$'s are pairwise independent, so we may apply Chernoff's inequality ([Fact 3.1](#)) with $\delta = 1/2$ to obtain

$$\Pr_\sigma \left[\sum_{i \in [C]} (1 - q_{\sigma,i}) \leq \frac{1}{2} \cdot 2^{-3t-1} \cdot C \right] \leq \exp \left\{ -\frac{C}{2^{3t+4}} \right\}. \quad (6)$$

We say σ is *bad* if the above event occurs and *good* otherwise. Then,

$$\begin{aligned} \left| \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x,y)] \right| &\leq \mathbb{E}_\sigma \left| \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x,y) \mid \sigma] \right| && \text{(by triangle inequality)} \\ &\leq \Pr_\sigma [\sigma \text{ is bad}] + \mathbb{E}_{\text{good } \sigma} \left| \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x,y) \mid \sigma] \right| \\ &\leq \exp \left\{ -\frac{C}{2^{3t+4}} \right\} + \mathbb{E}_{\text{good } \sigma} \left[\exp \left\{ -\frac{1}{4} \sum_{i \in [C]} (1 - p_{\sigma,i}) \right\} \right] && \text{(by (6) and (4))} \\ &\leq \exp \left\{ -\frac{C}{2^{3t+4}} \right\} + \mathbb{E}_{\text{good } \sigma} \left[\exp \left\{ -\frac{1}{4} \sum_{i \in [C]} (1 - q_{\sigma,i}) \right\} \right] && \text{(by (5))} \\ &\leq \exp \left\{ -\frac{C}{2^{3t+4}} \right\} + \exp \left\{ -\frac{1}{4} \cdot \frac{1}{2} \cdot 2^{-3t-1} \cdot C \right\} && \text{(by def'n of good } \sigma) \\ &= 2 \exp \left\{ -\frac{C}{2^{3t+4}} \right\}. \end{aligned}$$

To complete the proof it remains to set the value of C . We would like to choose C as large as possible subject to the constraint in (3); that is

$$C = \left\lfloor \frac{1}{m} \cdot \left(\frac{r}{4d} \right)^2 \right\rfloor \geq \frac{1}{2m} \cdot \left(\frac{r}{4d} \right)^2,$$

which is at least 1 by our assumption on m and [Lemma 5.1](#). Plugging into the previous inequality, we conclude

$$\left| \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x,y)] \right| \leq 2 \exp \left\{ -\frac{C}{2^{3t+4}} \right\} \leq 2 \exp \left\{ -\frac{r^2}{m \cdot d^2 \cdot 2^{3t+9}} \right\}. \quad \square$$

We now complete the proof of [Claim 5.7](#), showing that $|X_i|$ is unlikely to be fixed modulo 2 by a random σ . The proof is similar to [[KOW24](#), Claim 5.16].

Proof of Claim 5.7. By [Item 4](#), the distribution of $|X_i|$ conditioned on σ is the same as the distribution conditioned on all input bits outside of $I(i)$, denoted $\overline{I(i)}$. Let $Z = (Z_1, Z_2, \dots)$ denote the input bits to f_ρ . Then we can write

$$\mathbb{E}_\sigma \left[(q_{\sigma,i})^2 \right] = \mathbb{E}_{Z_j: j \in \overline{I(i)}} \left[\max_{a \in \mathbb{Z}/2\mathbb{Z}} \Pr \left[|X_i| \equiv a \pmod{2} \mid Z_j : j \in \overline{I(i)} \right]^2 \right]. \quad (7)$$

Consider a new input Z' obtained from Z by resampling the bits in $I(i)$, and let $\tilde{X}_i$ be the new output neighborhood on the same indices as X_i . Then for any $a \in \mathbb{Z}/2\mathbb{Z}$, we have

$$\begin{aligned} \Pr \left[|X_i| \equiv a \pmod{2} \mid Z_j : j \in \overline{I(i)} \right]^2 &= \Pr \left[|X_i| \equiv |\tilde{X}_i| \equiv a \pmod{2} \mid Z_j : j \in \overline{I(i)} \right] \\ &\quad (X_i \text{ and } \tilde{X}_i \text{ are conditionally independent}) \\ &\leq \Pr \left[|X_i| \equiv |\tilde{X}_i| \pmod{2} \mid Z_j : j \in \overline{I(i)} \right]. \end{aligned}$$

Substituting into (7) gives $\mathbb{E}_\sigma \left[(q_{\sigma,i})^2 \right] \leq \Pr \left[|X_i| \equiv |\tilde{X}_i| \pmod{2} \right]$.

We conclude by applying [Lemma 5.4](#) with $A = (X_i)|_i, B = (\tilde{X}_i)|_i, C = (X_i)|_{(N_S(i) \cap [n]) \setminus \{i\}}$, and $D = (\tilde{X}_i)|_{(N_S(i) \cap [n]) \setminus \{i\}}$. Note that the conditions of the lemma are met, since resampling the input bits in $I(i)$ decouples A from (B, D) and B from (A, C) , and (A, C) and (B, D) have the same marginal distribution 2^{-5t} -close to the $(1/4)$ -biased product distribution. Thus,

$$\mathbb{E}_\sigma \left[(q_{\sigma,i})^2 \right] \leq \Pr \left[|X_i| \equiv |\tilde{X}_i| \pmod{2} \right] \leq 1 - 2^{-3t},$$

where we used [Item 2](#) to bound the size of $N_S(i) \cap [n]$. $\square$

At this point, we are ready to prove [Theorem 2.9](#).

Proof of Theorem 2.9. Recall our goal is to show that the distribution $\mathcal{D}_{\text{hard}}(n, m)$ is 0.24-far from $f(\Pi) = \mathbb{E}_\rho[f_\rho(\Pi)]$. This will follow from [Lemma 3.4](#) by showing that each restricted function $f_\rho(\Pi)$ is either far from $\mathcal{D}_{\text{hard}}(n, m)$ in total variation distance or in expectation of the potential function $h(x, y)$. Fix an arbitrary ρ , and consider the r indices guaranteed by [Lemma 5.1](#). If at least $r/2$ of them are [Type-1](#), then

$$\|f_\rho(\Pi) - \mathcal{D}_{\text{hard}}(n, m)\|_{\text{TV}} \geq 1 - 2 \exp \left\{ -\frac{r}{2^{12t}} \right\}$$

by [Lemma 5.2](#). Otherwise, at least $r/2$ of them are [Type-2](#), and we find that

$$\begin{aligned} \mathbb{E}_{(x,y) \sim \mathcal{D}_{\text{hard}}(n,m)} [h(x, y)] - \mathbb{E}_{(x,y) \sim f_\rho(\Pi)} [h(x, y)] &\geq \frac{1}{2} + \left(\frac{1}{2} \right)^{n+1} - 2 \exp \left\{ -\frac{r^2}{m \cdot d^2 \cdot 2^{3t+9}} \right\} \\ &\geq \frac{1}{2} - 2 \exp \left\{ -\frac{r^2}{m \cdot d^2 \cdot 2^{12t}} \right\} \end{aligned}$$

by [Claim 5.3](#) and [Lemma 5.6](#). Thus [Lemma 3.4](#) yields

$$\begin{aligned} \|f(\Pi) - \mathcal{D}_{\text{hard}}(n, m)\|_{\text{TV}} &\geq \frac{1}{2} \left(\frac{1}{2} - 2 \exp \left\{ -\frac{r^2}{m \cdot d^2 \cdot 2^{12t}} \right\} \right) - \left(2^{|S|} + 1 \right) \cdot 2 \exp \left\{ -\frac{r}{2^{12t}} \right\} \\ &\geq \frac{1}{4} - \exp \left\{ -\frac{r^2}{m \cdot d^2 \cdot 2^{12t}} \right\} - \exp \left\{ 3|S| - \frac{r}{2^{12t}} \right\}. \end{aligned}$$

Recall from our assumption on m and the bounds on $r, |S|, t$ given by [Lemma 5.1](#) that

$$m \leq \frac{n^2}{\text{tow}(30d)}, \quad |S| \leq \frac{r}{2^{20t}}, \quad r \geq \frac{n}{\text{tow}(20d)}, \quad t \leq \text{tow}(20d).$$

Continuing the previous chain of inequalities, we have

$$\|f(\Pi) - \mathcal{D}_{\text{hard}}(n, m)\|_{\text{TV}} \geq \frac{1}{4} - \exp \left\{ -\frac{(n/\text{tow}(20d))^2}{m \cdot d^2 \cdot 2^{12 \cdot \text{tow}(20d)}} \right\} - \exp \left\{ 3 \left(\frac{r}{2^{20t}} \right) - \frac{r}{2^{12t}} \right\}$$

$$\begin{aligned}
&\geq \frac{1}{4} - \exp \left\{ -\frac{1}{m} \cdot \frac{n^2}{\text{tow}(25d)} \right\} - \exp \left\{ -\frac{r}{2^{15t}} \right\} \\
&\geq \frac{1}{4} - \exp \left\{ -\frac{\text{tow}(30d)}{\text{tow}(25d)} \right\} - \exp \left\{ -\frac{n}{\text{tow}(25d)} \right\},
\end{aligned}$$

which is at least 0.24 for $n \geq \text{tow}(30d)$. $\square$

5.2 The NC⁰ Upper Bounds

In this subsection, we provide sampling schemes that highlight the necessity of the constraints in [Theorem 2.9](#). We begin by showing that we must take $m \leq O(n^2)$; otherwise, one may produce the distribution $\mathcal{D}_{\text{hard}}(n, m)$ with constant locality.

Proposition 5.8. *If $m \geq \binom{n+1}{2}$, then $\mathcal{D}_{\text{hard}}(n, m)$ is a 6-local distribution with unbiased random bits as inputs.*

Proof. We describe the sampling algorithm as follows.

- Sample a uniform m -bit string z of even Hamming weight. This is 2-local by sampling as in the PARITY example in [Subsection 2.1](#) (e.g., output $r_1 \oplus r_2, r_2 \oplus r_3, \dots, r_{m-1} \oplus r_m, r_m \oplus r_1$ where $r_1, r_2, \dots$ are unbiased random bits from the input).
- Sample $x \sim \mathcal{U}_{1/4}^n$ and define $\tilde{x} \in \{0, 1\}^{n+1}$ by setting $\tilde{x} = (x, b)$ where b is an unbiased random bit. This is 2-local.
- Prepare an m -bit string w by putting the products $\tilde{x}_i \tilde{x}_j$ for all pairs $1 \leq i < j \leq n+1$ on the first $\binom{n+1}{2}$ entries (in any order) and padding the rest with zeros. Define $y = z \oplus w$ and output (x, y) .

Since each bit of y depends on one bit of z and at most two bits of $\tilde{x}$, the total locality of the above construction is 6. Let us now verify correctness. It is clear that x has the correct distribution, so it remains to check y . The parity of $|y|$ is given by

$$|z| + |w| \equiv \sum_{1 \leq i < j \leq n+1} \tilde{x}_i \tilde{x}_j \equiv \sum_{1 \leq i < j \leq n} x_i x_j + \sum_{i=1}^n x_i b \equiv \binom{|x|}{2} + b|x| \pmod{2}.$$

Observe that for any fixed $x \in \{0, 1\}^n$ of odd Hamming weight, flipping the unbiased random bit b flips the parity of $|y|$, so the parity of $|y|$ must also be unbiased. Furthermore, for any fixed $x \in \{0, 1\}^n$ of even Hamming weight, the parity of $|y|$ is equal to the parity of $\binom{|x|}{2} \equiv |x|/2 \pmod{2}$. We conclude by noting that the addition of z acts to “symmetrize” the distribution over y ; each output string is equally likely, conditioned on the Hamming weight having the correct parity. $\square$

Note that if we are willing to add several of the $\tilde{x}_i \tilde{x}_j$ terms to each y entry, we can sample $\mathcal{D}_{\text{hard}}(n, m)$ with a d -local function of unbiased random bits so long as m is at least a sufficiently large constant multiple of n^2/d .

We now show that in the definition of $\mathcal{D}_{\text{hard}}(n, m)$ it is necessary for $x \sim \mathcal{U}_{1/4}^n$ rather than $\mathcal{U}_{1/2}^n$, which a priori may appear a more natural choice. Below, let $\mathcal{D}_{\text{hard}}^*(n, m)$ be the analogous version of $\mathcal{D}_{\text{hard}}(n, m)$ where $x \sim \mathcal{U}_{1/2}^n$. That is, a sample $(x, y) \sim \mathcal{D}_{\text{hard}}^*(n, m)$ is drawn by first sampling $x \sim \mathcal{U}_{1/2}^n$ and then choosing y to be a uniform random m -bit string when $|x|$ is odd and otherwise a uniform random m -bit string with parity $|x|/2 \pmod{2}$.

Proposition 5.9. *If $m \geq n - 1$, then $\mathcal{D}_{\text{hard}}^*(n, m)$ is a 6-local distribution with unbiased random bits as inputs.*

Proof. We describe the sampling algorithm as follows.

- Sample a uniform n -bit string x_{odd} of odd Hamming weight, and a uniform random m -bit string y_{odd} . The former is 2-local, and the latter is 1-local.
- Sample a uniform n -bit string x_{even} of even Hamming weight by setting $(x_{\text{even}})_i = r_i \oplus r_{i+1}$ where $r_1 = r_{n+1} = 0$ and $r_2, r_3, \dots, r_n$ are unbiased random bits from the input. This is 2-local.
- Sample a uniform m -bit string z of even Hamming weight. This is 2-local.
- Prepare an m -bit string w by putting $r_i \oplus r_i r_{i+1}$ for all $2 \leq i \leq n$ on the first $n - 1$ entries (in any order) and padding the rest with zeros. Define $y_{\text{even}} = z \oplus w$.
- Sample a uniform random bit b and output $(x_{\text{even}}, y_{\text{even}})$ if $b = 0$ and $(x_{\text{odd}}, y_{\text{odd}})$ otherwise.

Each output bit depends on a bit of x_{odd} or y_{odd} , a bit of x_{even} or y_{even} , and b , and so depends on at most 6 input bits. Via a similar analysis to that of [Proposition 5.8](#), the correctness of this sampling scheme will follow from proving the distribution of $|y|$'s parity is correct. The case of odd $|x|$ is immediate, so let us consider the case of a fixed $x \in \{0, 1\}^n$ with even Hamming weight. Here, the parity of $|y|$ is given by

$$\begin{aligned}
|z| + |w| &\equiv \sum_{i=2}^n r_i \oplus r_i r_{i+1} \pmod{2} \\
&\equiv \sum_{i \in [n]} r_i + \sum_{i \in [n]} r_i r_{i+1} \pmod{2} && (\text{since } r_1 = 0) \\
&\equiv \frac{\sum_{i \in [n]} (r_i + r_{i+1} - 2r_i r_{i+1})}{2} \pmod{2} && (\text{since } r_1 = r_{n+1}) \\
&\equiv \frac{\sum_{i \in [n]} (r_i \oplus r_{i+1})}{2} \pmod{2} \\
&\equiv \frac{|x|}{2} \pmod{2}.
\end{aligned}$$

□

Note that $\mathcal{D}_{\text{hard}}^*(n, m)$ can in fact be shown to be 5-local by reusing the bits used to compute y_{even} and y_{odd} .

Remark 5.10. The sampling schemes in both [Proposition 5.8](#) and [Proposition 5.9](#) can be extended to smaller m , even beyond the improvement mentioned after [Proposition 5.8](#), at the cost of increased locality. For example, suppose $m \geq n - C$ for some arbitrary integer $C \geq 1$. Then we may sample $\mathcal{D}_{\text{hard}}^*(n, m)$ as follows:

- Sample $x_1 \sim \mathcal{U}_{1/2}^{C-1}$.
- If $|x_1|$ is even, then sample (x_2, y) where $x_2 \sim \mathcal{U}_{1/2}^{n-C+1}$ and y is a uniform random m -bit string when $|x_2|$ is odd and otherwise a uniform random m -bit string with parity $(|x_1| + |x_2|)/2 \pmod{2}$.
- If $|x_1|$ is odd, then sample (x_2, y) where $x_2 \sim \mathcal{U}_{1/2}^{n-C+1}$ and y is a uniform random m -bit string when $|x_2|$ is even and otherwise a uniform random m -bit string with parity $(|x_1| + |x_2|)/2 \pmod{2}$.

- In either case, set $x = x_1 \circ x_2$, where $\circ$ denotes concatenation, and output (x, y) .

This requires $C - 1$ bits of locality to determine whether to perform the second or third item. Observe that $m \geq (n - C + 1) - 1$, so [Proposition 5.9](#) provides a constant locality sampling procedure for either item. Thus, $\mathcal{D}_{\text{hard}}^*(n, m)$ can be sampled with $C + O(1)$ bits of locality.

Similarly, $\mathcal{D}_{\text{hard}}(n, m)$ with $m \geq \binom{n+1}{2} - C$ can be sampled with $C + O(1)$ bits of locality using [Proposition 5.8](#). In particular, $\mathcal{D}_{\text{hard}}(n, m)$ (and $\mathcal{D}_{\text{hard}}^*(n, m)$) can be sampled by AC^0 circuits for any choice of n, m . This is in stark contrast to the setting of relational problems, where the Parity Halving Problem (i.e., the inspiration for $\mathcal{D}_{\text{hard}}(n, m)$) cannot be computed by functions in AC^0 [[WKST19](#)].

5.3 The NC^0 Reduction

In this subsection, we provide a constant locality reduction from the $\mathcal{D}_{\text{host}}$ distribution (recall [Definition 2.5](#)) to the $\mathcal{D}_{\text{hard}}$ distribution. In conjunction with [Theorem 2.9](#), this implies that $\mathcal{D}_{\text{host}}$ is also difficult to classically sample.

Lemma 2.8. *Let $\mathcal{T} = (V, E)$ be a tree and let $v^* \in V$ be arbitrary. Define $K = \sum_{v \in V} |P_v|$, where P_v is the set of edges on the unique path between v^* and v . Then there exists a 5-local function $\text{red}: \{0, 1\}^{3|V|-1} \times \{0, 1\}^* \rightarrow \{0, 1\}^{2|V|+K}$ such that*

$$\text{red}(\mathcal{D}_{\text{host}}(\mathcal{T}), \mathcal{U}_{1/2}^*) = \mathcal{D}_{\text{hard}}(|V|, |V| + K).$$

Proof. Let (X, Y, W) be a sample from $\mathcal{D}_{\text{host}}(\mathcal{T})$, which also implicitly samples Z in [Definition 2.5](#). Observe that

$$\begin{aligned} \langle Z, X \rangle \pmod{2} &= \bigoplus_{v \in V} Z_v X_v = \bigoplus_{v \in V} X_v \left(Z_{v^*} \oplus \bigoplus_{e \in P_v} W_e \right) && \text{(by def'n of } W \text{ and } P_v) \\ &= \left(\bigoplus_{v \in V} X_v Z_{v^*} \right) \oplus \left(\bigoplus_{v \in V, e \in P_v} X_v W_e \right). \end{aligned}$$

Sample an unbiased coin b . We will need the following random strings:

- Y' is a uniform $|V|$ -bit string of parity b . This is 3-local with bounded fan-out.
- $\tilde{Y}$ is a uniform K -bit string of parity $b \oplus \bigoplus_{v \in V, e \in P_v} X_v W_e$. Given X, W , and b , this is 5-local with bounded fan-out.

Now we show that $(X, Y \oplus Y', \tilde{Y})$ is distributed as $\mathcal{D}_{\text{hard}}(|V|, |V| + K)$:

- If X has even Hamming weight, then Y has parity $\langle Z, X \rangle + |X|/2 \pmod{2}$ as $(X, Y, W) \sim \mathcal{D}_{\text{host}}(\mathcal{T})$. Note that in this case $\bigoplus_{v \in V} X_v Z_{v^*} \equiv 0$ and thus $\langle Z, X \rangle \equiv b \oplus |\tilde{Y}| \pmod{2}$. Hence $(Y \oplus Y', \tilde{Y})$ has parity $|X|/2 \pmod{2}$.

Since b re-randomizes⁷ the parity of Y , $(Y \oplus Y', \tilde{Y})$ is uniform with parity $|X|/2 \pmod{2}$.

- If X has odd Hamming weight, then Y is simply uniform as $(X, Y, W) \sim \mathcal{D}_{\text{host}}(\mathcal{T})$ and hence $Y \oplus Y'$ is uniform. In addition, since b re-randomizes⁸ the parity of $\tilde{Y}$, $\tilde{Y}$ is independent from Y and is also uniform.

This concludes the proof. □

⁷This is necessary as Y is always even if $X \equiv 0^V$.

⁸This is also necessary as $\bigoplus_{v \in V, e \in P_v} X_v W_e$ may be forced to zero for some X .

5.4 Hardness Amplification for Sampling in NC^0

In this subsection, we formalize a direct product theorem for sampling in NC^0 (Theorem 2.11), which is largely implicit in [KOW24]. This allows us to “amplify” the hardness from Corollary 2.10 by taking multiple copies. Note that a similar theorem for read-once branching programs is also known [CGZ22]. For a distribution $\mathcal{D}$, recall $\mathcal{D}^k = \mathcal{D} \times \cdots \times \mathcal{D}$ denotes the k -fold product distribution of $\mathcal{D}$. We restate Theorem 2.11 below for convenience.

Theorem 2.11 (Direct Product Theorem). *Let $d, \ell \geq 1$ be integers, and let $\mathcal{D}$ be a distribution over $\{0, 1\}^\ell$. Suppose that for any d -local function $f: \{0, 1\}^* \rightarrow \{0, 1\}^\ell$ and binary product distribution Π on $\{0, 1\}^*$, we have*

$$\|f(\Pi) - \mathcal{D}\|_{\text{TV}} \geq \delta.$$

Then for any integer $k \geq 1$, d -local function $g: \{0, 1\}^ \rightarrow \{0, 1\}^{\ell k}$, and binary product distribution Ξ on $\{0, 1\}^*$, we have*

$$\left\|g(\Xi) - \mathcal{D}^k\right\|_{\text{TV}} \geq 1 - 4 \exp \left\{ - \left(\frac{\delta^2}{16d\ell} \right)^{4d\ell} \cdot k \right\}.$$

Proof. Fix a function $g: \{0, 1\}^* \rightarrow \{0, 1\}^{\ell k}$ and a binary product distribution Ξ . By viewing the ℓk output bits as k “chunks” of ℓ consecutive bits, g becomes a $(d\ell)$ -local function with k output symbols. Let $g_i: \{0, 1\}^* \rightarrow \{0, 1\}^\ell$ denote the i^{th} such symbol, and recall that $g_i(\Xi)$ is δ -far from $\mathcal{D}$ by assumption. To obtain a stronger bound for $g(\Xi)$, we will reduce to the case where many g_i ’s are independent.

By recalling the graph theoretic view of local functions, we may apply Lemma 3.6 with $\beta = 4/\delta^2$ and $\lambda = (4d\ell\beta)^{2d\ell+1}$. This guarantees a set S such that any fixing ρ of the input bits in S reduces g to a $d\ell$ -local function g_ρ with r non-connected output symbols, where

$$|S| \leq \frac{\delta^2 \cdot r}{4} \quad \text{and} \quad r \geq \frac{k}{(16d\ell/\delta^2)^{2d\ell+1}}.$$

We then apply Lemma 3.3 for each ρ to deduce

$$\left\|g_\rho(\Xi) - \mathcal{D}^k\right\|_{\text{TV}} \geq 1 - 2 \exp \left\{ - \frac{\delta^2 \cdot r}{2} \right\}.$$

Finally, Lemma 3.4 implies

$$\begin{aligned} \left\|g(\Xi) - \mathcal{D}^k\right\|_{\text{TV}} &\geq 1 - \left(2^{|S|} + 1\right) \cdot 2 \exp \left\{ - \frac{\delta^2 \cdot r}{2} \right\} \\ &\geq 1 - 4 \exp \left\{ - \frac{\delta^2 \cdot k}{4 \cdot (16d\ell/\delta^2)^{2d\ell+1}} \right\} \\ &\geq 1 - 4 \exp \left\{ - \left(\frac{\delta^2}{16d\ell} \right)^{4d\ell} \cdot k \right\}. \end{aligned} \quad \square$$

Acknowledgements

AO thanks Farzan Byramji for suggestions improving the presentation. KW thanks David Gosset for helpful discussions motivating the problem.

References

- [AA13] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. *Theory OF Computing*, 9(4):143–252, 2013. [1](#)
- [Aha03] Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. *arXiv preprint quant-ph/0301040*, 2003. [3](#), [17](#), [18](#)
- [Bab87] Lászió Babai. Random oracles separate PSPACE from the polynomial-time hierarchy. *Information Processing Letters*, 26(1):51–53, 1987. [6](#)
- [BFNV19] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019. [1](#)
- [BGDSM23] Marshall Ball, Eli Goldin, Dana Dachman-Soled, and Saachi Mutreja. Extracting randomness from samplable distributions, revisited. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1505–1514. IEEE, 2023. [3](#), [6](#)
- [BGK18] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018. [1](#), [2](#), [10](#)
- [BGKT20] Sergey Bravyi, David Gosset, Robert König, and Marco Tomamichel. Quantum advantage with noisy shallow circuits. *Nature Physics*, 16(10):1040–1045, 2020. [1](#)
- [BIL12] Chris Beck, Russell Impagliazzo, and Shachar Lovett. Large deviation bounds for decision trees and sampling lower bounds for AC0-circuits. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 101–110. IEEE, 2012. [3](#), [6](#)
- [BL87] Ravi B Boppana and Jeffrey C Lagarias. One-way functions and circuit complexity. *Information and Computation*, 74(3):226–240, 1987. [6](#)
- [CCRK23] Libor Caha, Xavier Coiteux-Roy, and Robert König. A colossal advantage: 3D-local noisy shallow quantum circuits defeat unbounded fan-in classical circuits. *arXiv preprint arXiv:2312.09209*, 2023. [1](#)
- [CGZ22] Eshan Chattopadhyay, Jesse Goodman, and David Zuckerman. The space complexity of sampling. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, 2022. [3](#), [29](#)
- [DGL⁺23] Yu-Hao Deng, Yi-Chao Gu, Hua-Liang Liu, Si-Qiu Gong, Hao Su, Zhi-Jiong Zhang, Hao-Yang Tang, Meng-Hao Jia, Jia-Min Xu, Ming-Cheng Chen, et al. Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage. *Physical review letters*, 131(15):150601, 2023. [2](#)
- [DW12] Anindya De and Thomas Watson. Extractors and lower bounds for locally samplable sources. *ACM Transactions on Computation Theory (TOCT)*, 4(1):1–21, 2012. [6](#)
- [FLRS23] Yuval Filmus, Itai Leigh, Artur Riazanov, and Dmitry Sokolov. Sampling and certifying symmetric functions. In *Approximation, Randomization, and Combinatorial Optimization. (APPROX/RANDOM)*, 2023. [6](#), [8](#), [10](#)

- [GJS21] Daniel Grier, Nathan Ju, and Luke Schaeffer. Interactive quantum advantage with noisy, shallow Clifford circuits. *arXiv preprint arXiv:2102.06833*, 2021. [1](#)
- [GS20] Daniel Grier and Luke Schaeffer. Interactive shallow Clifford circuits: quantum advantage against NC^1 and beyond. In *Proceedings of the 52nd Annual ACM Symposium on Theory of Computing*, pages 875–888, 2020. [1](#)
- [Hås86] Johan Håstad. *Computational limitations for small depth circuits*. PhD thesis, Massachusetts Institute of Technology, 1986. [6](#)
- [HLG21] Atsuya Hasegawa and François Le Gall. Quantum advantage with shallow circuits under arbitrary corruption. In *32nd International Symposium on Algorithms and Computation (ISAAC 2021)*, pages 74–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021. [1](#)
- [KOW24] Daniel M Kane, Anthony Ostuni, and Kewen Wu. Locality bounds for sampling Hamming slices. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1279–1286, 2024. [2](#), [3](#), [4](#), [6](#), [8](#), [10](#), [11](#), [12](#), [13](#), [14](#), [19](#), [20](#), [23](#), [24](#), [29](#)
- [KOW25] Daniel M Kane, Anthony Ostuni, and Kewen Wu. Locally sampleable uniform symmetric distributions. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 1807–1816, 2025. [6](#), [8](#), [10](#), [13](#)
- [Kup23] Greg Kuperberg. Breaking the cubic barrier in the Solovay-Kitaev algorithm. *arXiv preprint arXiv:2306.13158*, 2023. [2](#)
- [LV11] Shachar Lovett and Emanuele Viola. Bounded-depth circuits cannot sample good codes. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 243–251. IEEE, 2011. [3](#), [6](#)
- [Ros21] Gregory Rosenthal. Bounds on the QAC^0 complexity of approximating parity. In *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, pages 32–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021. [4](#)
- [Shi05] Yaoyun Shi. Quantum and classical tradeoffs. *Theoretical computer science*, 344(2-3):335–345, 2005. [4](#)
- [Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. [1](#)
- [Smo87] Roman 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*, pages 77–82, 1987. [6](#)
- [SS24] Ronen Shaltiel and Jad Silbak. Explicit codes for poly-size circuits and functions that are hard to sample on low entropy distributions. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 2028–2038, 2024. [6](#)
- [TV00] Luca Trevisan and Salil Vadhan. Extracting randomness from samplable distributions. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 32–42. IEEE, 2000. [3](#), [6](#)

- [Vio12a] Emanuele Viola. The complexity of distributions. *SIAM Journal on Computing*, 41(1):191–218, 2012. [6](#), [8](#), [10](#)
- [Vio12b] Emanuele Viola. Extractors for Turing-machine sources. In *International Workshop on Approximation Algorithms for Combinatorial Optimization*, pages 663–671. Springer, 2012. [6](#)
- [Vio14] Emanuele Viola. Extractors for circuit sources. *SIAM Journal on Computing*, 43(2):655–672, 2014. [3](#), [6](#)
- [Vio20] Emanuele Viola. Sampling lower bounds: boolean average-case and permutations. *SIAM Journal on Computing*, 49(1):119–137, 2020. [3](#), [10](#)
- [Vio23] Emanuele Viola. New sampling lower bounds via the separator. In *38th Computational Complexity Conference (CCC 2023)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2023. [2](#), [3](#), [6](#), [8](#), [10](#)
- [WKST19] Adam Bene Watts, Robin Kothari, Luke Schaeffer, and Avishay Tal. Exponential separation between shallow quantum circuits and unbounded fan-in shallow classical circuits. In *Proceedings of the 51st Annual ACM Symposium on Theory of Computing*, pages 515–526, 2019. [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [28](#)
- [WP23] Adam Bene Watts and Natalie Parham. Unconditional quantum advantage for sampling with shallow circuits. *arXiv preprint arXiv:2301.00995*, 2023. [2](#), [3](#)
- [YGE⁺24] Aaron W Young, Shawn Geller, William J Eckner, Nathan Schine, Scott Glancy, Emanuel Knill, and Adam M Kaufman. An atomic boson sampler. *Nature*, 629(8011):311–316, 2024. [2](#)
- [YZ24] Huacheng Yu and Wei Zhan. Sampling, flowers and communication. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, pages 100–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024. [6](#)
- [ZWD⁺20] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020. [2](#)