THEORY OF COMPUTING, Volume 21 (12), 2025, pp. 1–42
www.theoryofcomputing.org

Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians

Anurag Anshu[*] Chinmay Nirkhe[†]

Received May 13, 2022; Revised October 12, 2022; Published November 27, 2025

Abstract. The No Low-energy Trivial States (NLTS) conjecture of Freedman and Hastings (*Quantum Info. Comput. 2014*) — which posits the existence of a local Hamiltonian with a super-constant quantum circuit lower bound on the complexity of all low-energy states — identifies a fundamental obstacle to the resolution of the quantum PCP conjecture. In this article we provide new techniques, based on entropic and local indistinguishability arguments, that prove circuit lower bounds for all the low-energy states of local Hamiltonians arising from quantum error-correcting codes.

For local Hamiltonians arising from nearly linear-rate or nearly linear-distance LDPC stabilizer codes, we prove super-constant circuit lower bounds for the complexity of all states of energy $o(n)$. Such codes are known to exist and are not necessarily

A conference version of this paper appeared in the Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022) [11].

[*] Supported by NSF Quantum Leap Challenges Institute Grant number OMA2016245 and part of this work was completed while he was a participant in the Simons Institute for the Theory of Computing program on *The Quantum Wave in Computing*.

[†] Supported by NSF Quantum Leap Challenges Institute Grant number OMA2016245 and part of this work was completed while he was a participant in the Simons Institute for the Theory of Computing program on *The Quantum Wave in Computing*.

ACM Classification: F.1.3

AMS Classification: 68Q17, 81P68

Key words and phrases: quantum PCPs, local Hamiltonians, error-correcting codes

DOI: 10.4086/toc.2025.v021a012

locally testable, a property previously suspected to be essential for the NLTS conjecture. Curiously, such codes can also be constructed on a two-dimensional lattice, showing that low-depth states cannot accurately approximate the ground-energy even in physically relevant systems. Here, by 'low-depth' states, we mean n-qubit quantum states that can be prepared using quantum circuits of constant depth, starting with the state $|0\rangle^{\otimes m}$, where $m \geq n$.

1 Introduction

Ground- and low-energy states of local Hamiltonians are the central objects of study in condensed matter physics. The QMA-complete local Hamiltonian problem is also the quantum analog of the NP-complete constraint satisfaction problem (CSP) and ground-states (and low-energy states) of local Hamiltonians correspond to solutions (near optimal solutions) of the problem. A sweeping insight into the computational properties of the low energy spectrum is embodied in the quantum PCP conjecture, which is arguably one of the most important open questions in quantum complexity theory. Just as the classical PCP theorem establishes that CSPs with a promise gap remain NP-complete, the quantum PCP conjecture asserts that local Hamiltonians with a promise gap remain QMA-complete. But despite numerous results providing evidence both for [2, 30, 27, 50, 47, 26] and against [20, 17, 4] the quantum PCP conjecture, the problem has remained open for nearly two decades.

The difficulty of the quantum PCP conjecture has motivated a flurry of research beginning with Freedman and Hastings' *No low-energy trivial states (NLTS) statement* [30]. The NLTS statement asserts that there exists a fixed constant $\epsilon > 0$ and a family of n qubit local Hamiltonians such that every state of energy $\leq \epsilon n$ requires a quantum circuit of super-constant depth to generate. The NLTS statement is a necessary consequence of the quantum PCP conjecture because QMA-complete problems are not expected to have NP solutions and a constant-depth quantum circuit generating a low-energy state would serve as a NP witness. Thus, this statement addresses the inapproximability of local Hamiltonians by classical means. Note that a proof of the NLTS statement was recently published by Anshu, Breuckmann, and Nirkhe [9] largely building on the present paper and [8].

In this paper, we show that for local Hamiltonians corresponding to LDPC stabilizer quantum error-correcting codes of linear rate and polynomial distance, every state of energy $\leq \epsilon n$ requires a quantum circuit of depth $\Omega(\log 1/\epsilon)$ to generate. We also show similar results for linear distance LDPC codes. Since the the publication of the conference version of this paper [11], constructions of quantum LDPC codes that are simultaneously linear rate and linear distance have been found. These constructions were shown in [9] to have the NLTS property. [9], however, only provides circuit lower bounds for a specific family of such optimal parameter code constructions. The results in this paper are far more general and provide circuit lower bounds for more general families of quantum codes.

1.1 Our results

We restrict our attention to quantum error-correcting codes and the low-energy states of the associated code Hamiltonians[1]. A code Hamiltonian is a local Hamiltonian whose ground-space is precisely the code-space, with the additional property that the energy of a state measures the number of violated code checks.

Examples of quantum error-correcting codes realized as the ground-spaces of local Hamiltonians already play a central role in our understanding of the physical phenomenon known as topological order [39, 33]. Call an error-correcting code an $[[n,k,d]]$ code with locality ℓ if it has n physical qubits, k encoded qubits (logical qubits), distance d and the corresponding code Hamiltonian has locality ℓ (these definitions are made precise in Section 2). Our main result refers to a subclass of codes known as *stabilizer codes* where the code Hamiltonian is commuting and each Hamiltonian term is the tensor product of Pauli operators.

Theorem 1.1. *Let C be a $[[n,k,d]]$ stabilizer code of constant locality $\ell = O(1)$ and let $H = \sum_i H_i$ be the corresponding code Hamiltonian with a term $H_i = (\mathbb{I} - C_i)/2$ for each code check C_i. For any $\epsilon > 0$ and any state ψ on n-qubits with energy $\leq \epsilon n$, the circuit depth of ψ is at least*

$$\Omega\left(\min\left\{\log d, \quad \log \frac{k+d}{n\sqrt{\epsilon \log \frac{1}{\epsilon}}}\right\}\right). \tag{1.1}$$

In the case of linear-rate and polynomial-distance codes such as the hypergraph product code of Tillich and Zémor [55], the theorem proves a circuit lower bound of $\Omega(\delta \log n)$ for any state of energy $O(n^{1-\delta})$. So for fixed δ, say $\delta = 0.01$, it provides a circuit lower bound of $\Omega(\log n)$ for all states of energy $O(n^{0.99})$. Furthermore, it proves a circuit lower bound of $\Omega(\log \log n)$ for any state of energy $O(n/\mathsf{poly}\log n)$ and a super-constant circuit lower bound for any state of energy $o(n)$. Recent developments [51, 35, 21] have shown quantum LDPC codes with near-linear distance $d = \Omega(n/\log n)$ (but with low rate $k = O(1)$). The theorem also provides a circuit lower bound of $\Omega(\log n)$ for all states of energy $O(n^{0.99})$ in such codes. For "reasonable" stabilizer codes of polynomial rate and polynomial distance, this theorem provides a non-trivial lower bound on the circuit complexity in the energy regime of $1/\mathsf{poly}(n)$.

Furthermore, for any constant $\delta > 0$, stabilizer code of rate $\geq n^{1-\delta}$, and distance at least $n^{\Omega(\delta)}$, the theorem still proves a circuit lower bound of $\Omega(\delta \log n)$ for any state of energy $O(n^{1-2\delta})$. Codes with these properties are known to exist on constant-dimensional lattices and are not locally testable; one example is the punctured 2D toric code[2] with $O(n^{1-\delta})$ punctures [19, 29]. Additionally, toric codes defined on hyperbolic manifolds where the manifold has constant negative curvature also have linear rate and small (yet polynomial) distance. Examples include the toric code defined on 4-dimensional arithmetic hyperbolic manifolds [31] or golden codes [45], for which our main result will also prove a super-constant circuit lower bound for all states of energy $o(n)$.

[1] The classical analog of this question, the circuit complexity of approximate sampling from the uniform distribution of a classical error-correcting code, is answered by Lovett and Viola [46].

[2] The punctured 2D toric code is known to saturate the information-distance tradeoff bound of [19].

1.2 Challenges and an overview of proof techniques

It is folklore that code-states of an error correcting code have a large circuit complexity $\sim \log d$, where d is the distance of the code; see Nirkhe [49] for a proof. This lower bound arises from the local indistinguishability property (see Fact 2.1), which means that for any size $< d$ subset S of the qubits, the reduced state ρ_S for any code-state ρ is an invariant of the code-space.

A natural notion of approximation to code-states is the class of low-error states. Such states resemble the code-states on a large number of physical qubits, differing arbitrarily on a small fraction (interpreted as an error). Prior work [27, 50], exploiting the error-correction property, showed that the low-error states also have a large circuit complexity. This generalized the aforementioned circuit lower bounds on code-states. However, as further demonstrated in [50], low error is a strictly weaker notion than low energy. Without invoking highly non-trivial properties such as local testability [27], it seems unclear if the low-energy states can be viewed as low-error. This leads to the central challenge towards the NLTS statement: capturing the circuit complexity of the low-energy states. The prior arguments, all of which rely on local indistinguishability (formalized by the code distance), do not seem to suffice.

We observe, for the first time, that another parameter plays a key role in circuit lower bounds: the rate of the code. Inspired by [19], we use novel entropic arguments to prove that states of low circuit complexity are significantly far in ℓ_1-distance from high rate code-spaces (established in Section 3). Formally, we show that all states of circuit complexity $\leq \log d$ are at a ℓ_1-distance of $\geq \Omega(\frac{k^2}{n^2})$ from the code-space.

This is proved using an information theory argument, which we sketch below. Consider a state ψ with small trace distance to the code. Below, we will use the notation $\approx$ to capture that ψ is close to a codestate in fidelity. Then, the reduced density matrices $\{\psi_S\}$ approximate the reduced density matrices of the closest state of C. By local indistinguishability, the $\{\psi_S\}$ in turn approximate the reduced density matrices for all code-states. In particular, they approximate the reduced density matrices of the encoded maximally mixed state Θ of the code. This state has entropy $S(\Theta)$ equal to the rate of the code, k. We now show that if ψ has low circuit complexity, then the entropy $S(\Theta)$ is bounded. Assume that ψ is the output of a low-depth circuit W, then for any qubit i,

$$\mathrm{tr}_{-\{i\}}(W^\dagger \psi W) \approx \mathrm{tr}_{-\{i\}}(W^\dagger \Theta W). \tag{1.2}$$

This is because (a) $\mathrm{tr}_{-L_i}(\psi) \approx \mathrm{tr}_{-L_i}(\Theta)$ where L_i is the support of the lightcone of qubit i with respect to W and (b) the value of the ith qubit of a W-rotated state only depends on the lightcone of the ith qubit. However, the left-hand side of Equation (1.2) equals the pure state $|0\rangle\langle 0|$ and so the entropy of $\mathrm{tr}_{-\{i\}}(W^\dagger \Theta W)$, the ith qubit of $W^\dagger \Theta W$, is small. This gives us an overall bound on the entropy of $W^\dagger \Theta W$, which equals that of Θ and also upper bounds the rate of the code.

This observation alone does not suffice to address the aforementioned central challenge: the space of low-energy states is much larger than the code-space or even its small neighborhood. A general strategy in earlier work [27, 26] was to build a low-depth decoding circuit to bring each low-energy state closer to the code-space. But this required assuming that the code was locally testable; such codes are not known to exist in the desired parameter regime. We instead appeal to the observation that every eigenspace of a stabilizer code Hamiltonian possesses the local indistinguishability property (Fact 2.1). Instead of attempting to construct a decoding circuit, we measure the syndrome using a constant-depth circuit (which uses the LDPC nature of the code Hamiltonian). This allows us to decohere the low energy state into a mixture of orthogonal states that live within each of the eigenspaces. A key realization is that measurement of the syndrome for low-energy states is a gentle measurement in that it does not perturb the state locally. This is used to show that a state of low energy satisfies an approximate version of locally indistinguishability. This, coupled with the argument for codes of high rate, completes the proof.

1.3 Separation of the NLTS statement from the QLDPC/QLTC conjectures

A quantum low-density parity-check (LDPC) code is an error-correcting code with a local Hamiltonian defining the code-space, such that each qubit participates in at most a constant number of Hamiltonian terms and each Hamiltonian term acts on at most a constant number of qubits (i. e., the bipartite interaction matrix has low density). The QLDPC conjecture posits the existence of LDPC codes that also have linear-rate and linear-distance. It was suspected that a QLDPC property would be necessary for NLTS Hamiltonians [30, 5, 34, 27, 50] coming from quantum codes. Our result perhaps breaks this intuition by showing that lower bound results are achievable even when the distance is a small polynomial; interestingly, it is the rate that needs to be almost linear for our result, a counter-intuitive property. Furthermore, our results show that entanglement persists at energy well past the distance threshold; a regime where one intuitively expects the stored information to be lost.

Furthermore, it was (incorrectly) believed that the QLDPC codes also need to be locally testable [5] for NLTS. This fact is formalized by Eldar and Harrow [27] who give a construction of an NLTS Hamiltonian from any locally testable CSS QLDPC code with constant soundness. Quantum locally testable codes (QLTCs) of constant soundness are not known to exist; the best constructions achieve a soundness factor of $O(1/\mathsf{poly}\log n)$ with a distance of $\Omega(\sqrt{n})$ [34, 44]. Our construction does not require local-testability; in fact, the hypergraph product code [55] with linear rate and polynomial distance is not locally testable as there are errors of size $\Omega(\sqrt{n})$ that violate only a single check [44, page 4]. In fact, the QLTC intuition was formally shown to be unnecessary as the construction in [9] may not be QLTC, but is QLDPC.

1.4 Spatially local Hamiltonians

A key property of an NLTS Hamiltonian is that it cannot live on a lattice of dimension D for a fixed constant D [3]. This is because of a "cutting" argument: Let H be a local Hamiltonian in D dimensions and Ψ a ground-state of H. For a fixed constant ϵ, partition the lattice into D dimensional rectangular chunks so that the side length of each rectangular chunk is $O((D\epsilon)^{-1/D})$. Let ρ_i be the reduced state of Ψ on a chunk i, and $\rho = \bigotimes_i \rho_i$ be a state over all the qubits. It's not hard to check that ρ violates at most a ϵ-fraction of the terms of H (only the boundary terms of the rectangular division) and yet has circuit complexity at most $\exp(((D\epsilon)^{-1/D})^D) = O(\exp(1/D\epsilon)) = O(1)$; so it is not NLTS.

This circuit complexity upper bound can be further improved for the specific case of stabilizer Hamiltonians on a lattice, due to the result of Aaronson and Gottesman [1]. Since the circuit complexity of each chunk is at most logarithmic in its size $O(1/\epsilon^{1/D})$, the aforementioned quantum state ρ can actually be prepared by a circuit of depth $O(\min(\log n, \log(1/\epsilon)))$. Note that this holds for any $0 < \epsilon < 1$, not just a constant. Therefore, our lower bound in the case of nearly linear rate and polynomial distance codes (such as the punctured toric code) matches the upper bound – up to constant factors – closing the question on the circuit complexity of the approximate ground-states of these codes.

We also highlight that the only known constructions of LDPC stabilizer codes of linear rate and polynomial distance are built from classical expander graphs and therefore cannot live on a lattice of constant dimension D. Therefore, our result in Theorem 1.1 (applied to linear rate codes) conveniently evades this counterexample.

1.5 The physics perspective

The crucial role of entanglement in the theory of quantum many-body systems is widely known with some seminal examples including topological phases of matter [40] and quantum computation with physically realistic systems [53, 54]. But entanglement also brings new challenges as the classical simulation of realistic many-body systems faces serious computational overheads.

Estimating the ground-energy of such systems is one of the major problems in condensed matter physics [58], quantum chemistry [24], and quantum annealing [12, 36]. One of the key methods to address this problem is to construct *ansatz quantum states* that achieve as low energy as possible and are also suitable for numerical simulations. A leading ansatz, used in Variational Quantum Eigensolvers [52, 43, 24] or Quantum Adiabatic Optimization Algorithm [28], is precisely the class of quantum states that can be generated by low-depth quantum circuits. Theorem 1.1 shows that there are Hamiltonians for which any constant-depth ansatz cannot estimate their ground-energies beyond a fairly large threshold. As discussed earlier, we provide examples even in the physically realistic two-dimensional setting. For example, the 2D punctured toric code Hamiltonians on n qubits with distance d (which is a free parameter) requires a circuit of depth $\Omega(\log d)$ for an approximation to ground-energy better than $O(n/d^3)$.

1.6 Prior Results

To the best of our knowledge, prior to this result, a circuit lower bound on the complexity of *all* low-energy states was only known for states of energy $O(n^{-2})$. This result follows from the QMA-completeness of the local Hamiltonian problem with a promise gap of $O(n^{-2})$ (assuming NP $\neq$ QMA); the original proof of Kitaev had a promise gap of $O(n^{-3})$ [41, 38] which was improved by [23, 15].

Robustness to perturbations Prior to our results, being robust against constant-distance perturbations was only known in the special case of CSS codes of distance $\omega(n^{0.5})$ or larger [27], as exhibited in recent codes [35, 51] . We prove as a warm-up that the robust notion of circuit complexity holds (a) for any state of a quantum code of linear-rate (Lemmas 3.1 and 3.4) or (b) any state of a quantum code of linear-distance (Lemma A.1). For commuting codes, we can further show that they are robust against perturbations in trace distance very close to 1 (Lemma 3.4).

Subclasses of low-energy states Freedman and Hastings proved a circuit lower bound for all "one-sided" low-energy states of a particular stabilizer Hamiltonian where a state is one-sided if it only violates either type X or type Z stabilizer terms but not both [30].

As mentioned earlier, a different line of work focused on the low-error states [27], which differ from a code-state on at most ϵn qubits. These papers prove a circuit lower bound of $\Omega(\log n)$ on the complexity of all low-error states of a specific local Hamiltonian [27, 50] (for some constant ϵ).

Eldar has also shown an $\Omega(\log n)$ circuit lower bound for Gibbs or thermal states of local Hamiltonians at $O(1/\log^2 \log n)$ temperature [26] which is a specific low-energy state formed by coupling the ground-state of a physical system to a "heat bath."

Article [18] gives examples of classical Hamiltonians for which all the states with $\mathbb{Z}_2$ symmetry require $\Omega(\log n)$ circuit complexity.

1.7 Future work and open questions

Our main result, Theorem 1.1, comes quite close to proving NLTS for a large class of codes. And while we are able to provide a constant depth lower bound for all states of energy $\leq n/100$ of many families of quantum codes, we have been unsuccessful, thus far, at extending this result to a super-constant depth lower bound. Below are sketches of some potential avenues at completing the proof of the NLTS result and future questions to consider.

1.7.1 Gap amplification implies circuit complexity amplification

Consider a transformation of a local Hamiltonian H into a different Hamiltonian H' such that for all low-energy states ϕ, $\operatorname{tr}(H'\phi) \geq p \cdot \operatorname{tr}(H\phi)$ for a large value p. If one could perform this transformation without increasing the locality of the Hamiltonian or the norm of the Hamiltonian for $p = \omega(1)$, we would obtain an NLTS Hamiltonian due to Theorem 1.1.

However, we do not know any construction of such a transformation. The closest result we know is a construction that amplifies the energy of all low-depth states at the cost of increasing the locality of the Hamiltonian; we state this result as Theorem C.2 in Appendix C, where we delve into this idea in greater detail. This is analogous to the amplification step in Dinur's PCP theorem [25] or the quantum gap amplification lemma [2] which performs amplification for the lowest energy eigenstate. In order to complete the transformation, we need a "locality reduction" transformation which reduces the locality of the Hamiltonian while preserving the energy of all low-depth states. The analogous transformation from Dinur's PCP theorem involves cloning of information, which is not viable in the quantum context.

1.7.2 Improving our circuit lower bound, Theorem 1.1

Our results give the strongest circuit lower bounds when we consider stabilizer codes of linear rate and polynomial distance. There are two possibilities to consider: (1) such codes are simply not necessarily NLTS and another assumption is needed to prove NLTS or (2) our proof techniques have the potential to be strengthened in order to prove NLTS. For the first possibility, recall that Eldar and Harrow [27] proved that locally testable linear distance CSS codes are NLTS; however, such codes are not known to exist. For the second possibility, let us reexamine our proof in greater details.

At a high level, we proceed via a proof by contradiction in which we assume that a low-depth state $|\psi\rangle$ of low energy exists. We then construct a related state Θ whose entropy is at least k (the rate of the code) and yet its entropy is upper bounded by $O(2^t \epsilon n)$ due to its similarity to $|\psi\rangle$ on small marginals. The ϵn term in the upper bound is a consequence of the gentle measurement lemma. The 2^t term is, we believe, an over-counting due to the naïve application of sub-additivity of entropy to the state Θ. Instead, there may be a more sophisticated analysis using conditional entropies, which would avoid the 2^t factor. If successful, this would prove NLTS for some constant $\epsilon = \Omega(k/n) = \Omega(1)$.

1.7.3 Lower bounds against other classical approximations

The NLTS statement postulates a lower bound on the approximability of local Hamiltonians by low-depth circuits. However, if the QPCP conjecture is true and $\mathsf{NP} \neq \mathsf{QMA}$, then we should be able to prove lower bounds on the approximability of local Hamiltonians by any means of classically simulation, such as stabilizer codes, tensor networks of low tree width, etc. Our result, of course, does not prove general lower bounds against classical simulation as the Hamiltonians are stabilizer codes, which can be solved classically. One interpretation of our result is a proof that stabilizer codes and low-depth circuits are not equal in simulation power (even in an approximate sense). One future avenue of research is to produce similar lower bounds against other methods of classical simulation. Furthermore, one should be able to provide lower bounds against generalized non-deterministic computation: show that there exists a family of local Hamiltonians which has no low-energy states whose energy can be verified in $\mathsf{NPTIME}[t(n)]$ for progressively larger and larger $t(n)$ up to $\mathsf{poly}(n)$.

1.8 Organization

In Section 2, we give the necessary background information. Section 3 proves the entropy-based robust lower bound for code-states of any code (Lemma 3.1). In Section 4, we prove our main result, Theorem 1.1. Appendix A contains proofs of other related techniques for lower bounding circuit complexity. Appendix B contains improved lower bound techniques based on approximate ground-state projectors. Appendix C contains the mathematics behind the gap amplification techniques suggested in Section 1.7.1.

2 Preliminaries

We will assume that the reader is familiar with the basics of quantum computing and quantum information. A standard textbook is that of Nielsen and Chuang [48].

2.1 Notation

The set of integers $\{1, 2, \dots m\}$ is abbreviated as $[m]$. Given a composite system of m qubits, we will often omit the register symbol from the states (being clear from context). For a set $A \subseteq [m]$, $-A$ will denote the set complement $[m] \setminus A$ and tr_A will denote the partial trace operation on qubits in A and $\mathrm{tr}_{-A} \overset{\text{def}}{=} \mathrm{tr}_{[m]\setminus A}$. Therefore, $\mathrm{tr}_{-\{i\}}(\cdot)$ gives the reduced marginal on the ith qubit.

Quantum states A quantum state is a positive semidefinite matrix with unit trace, acting on a finite-dimensional complex vector space (a Hilbert space) $\mathcal{H}$. In this paper we will only concern ourselves with Hilbert spaces coming from a collection of qubits, i. e., $\mathcal{H} = (\mathbb{C}^2)^{\otimes m}$. A pure quantum state is a quantum state of rank 1 (i. e., it can be expressed as $|\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle$). In this case we will refer to the state as $|\psi\rangle$ when interested in the unit vector representation and ψ when interested in the positive semidefinite matrix representation. Given two Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, their tensor product is denoted by $\mathcal{H}_A \otimes \mathcal{H}_B$. For a quantum state ρ_{AB} acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, the reduced state on $\mathcal{H}_A$ is denoted by $\rho_A \overset{\text{def}}{=} \mathrm{tr}_B(\rho_{AB})$, where tr_B is the partial trace operation on the Hilbert space $\mathcal{H}_B$. The partial trace operation is a type of quantum channel. More generally, a quantum channel $\mathcal{E}$ maps quantum states acting on some Hilbert space $\mathcal{H}_A$ to another Hilbert space $\mathcal{H}_B$. For two quantum states, ρ and σ, in the same Hilbert space, the fidelity $F(\rho, \sigma)$ is defined as $\left(\mathrm{tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right)^2$. Unless specified otherwise, we assume $\|\cdot\| = \|\cdot\|_2$, the spectral norm for a matrix, which for positive semidefinite Hermitian matrices is the largest eigenvalue.

Every quantum state ρ acting on a D-dimensional Hilbert space has a collection of eigenvalues $\{\lambda_i\}_{i=1}^D$, where $\sum_i \lambda_i = 1$ and $\lambda_i \geq 0$. The von Neumann entropy of ρ, denoted $\mathrm{S}(\rho)$, is defined as $\sum_i \lambda_i \log \frac{1}{\lambda_i}$. All logarithms are in base 2.

Unless specified otherwise, assume that we are considering a quantum code on n physical qubits and assume we are considering quantum states on an expanded Hilbert space of $m \geq n$ qubits. We will denote the n qubits corresponding to the code-space as code and the remainder $(m-n)$ qubits defining the expanded Hilbert space as anc for ancillas. Furthermore, the reduced state on code of a state ρ will be referred to as ρ_{code} and, respectively, ρ_{anc} for the ancillas. The uniformly distributed quantum state on a Hilbert space $\mathcal{H}$ will be represented by ν:

$$\nu_{\mathcal{H}} \overset{\text{def}}{=} \frac{\mathbb{I}_{\mathcal{H}}}{|\mathcal{H}|}. \tag{2.1}$$

2.2 Error-correction

We assume the reader is familiar with the basics of quantum error-correction. Here, we employ the notation of Nielsen and Chuang [48] of a quantum error-correcting code; we refer the reader to [48] for more details. We will refer to a code C as a $[[n, k, d]]$ code where n is the number of physical qubits (i. e., the states are elements of $(\mathbb{C}^2)^{\otimes n}$), k is the dimension of the code-space, and d is the distance of the code. Furthermore, we refer to k as the *rate* of the code; this is slightly non-traditional as some authors refer to the ratio k/n as the rate of the code. We can define distance precisely using the Knill–Laflamme conditions [42].

Let $\{|\overline{x}\rangle\} \subseteq C$ be an orthonormal basis for C parameterized by $x \in \{0,1\}^k$. The Knill–Laflamme conditions[3] state that the code can correct an error E iff

$$\langle\overline{x}| E |\overline{y}\rangle = \begin{cases} 0 & x \neq y \\ \eta_E & x = y \end{cases} \tag{2.2}$$

where η_E is a constant dependent on E. This is equivalent to

$$\Pi_C E \Pi_C = \eta_E \Pi_C \tag{2.3}$$

where Π_C is the projector onto the code-space. We say that the code C has distance d if it can correct all Pauli-errors of weight $< d$. By linearity, it can then correct all errors of weight $< d$. Furthermore, given a set S of fewer than d qubits, the reduced state ρ_S of any code-state ρ on the set S is an invariant of the code. Intuitively, this property can be seen as a consequence of the no-cloning theorem since ρ can be recovered exactly from ρ_{-S}; therefore, ρ_S cannot depend on ρ without violating the no-cloning theorem. The property can also be derived as a direct consequence of the Knill–Laflamme conditions and is known as *local indistinguishability*.

Fact 2.1 (Local Indistinguishability)**.** *Let C be an $[[n, k, d]]$ error correcting code and S a subset of the qubits such that $|S| < d$. Then the reduced state ρ_S of any code-state ρ on the set S is an invariant of the code.*

Proof. Let E be any operator whose support is entirely contained in S. Then for any code-state ρ,

$$\begin{aligned} \operatorname{tr}(E\rho) &= \operatorname{tr}(E\Pi_C\rho\Pi_C) && (2.4)\\ &= \operatorname{tr}(\Pi_C E \Pi_C \rho) && (2.5)\\ &= \operatorname{tr}(\eta_E \Pi_C \rho) && (2.6)\\ &= \eta_E && (2.7) \end{aligned}$$

where Equation (2.4) holds because ρ is a code-state, Equation (2.5) is due to cyclicality of trace, Equation (2.6) is an application of Equation (2.3), and Equation (2.7) holds because ρ has trace 1. Since this equality holds for any operator E and η_E is a constant independent of ρ such that $\eta_E = \operatorname{tr}(E\rho) = \operatorname{tr}(E\rho_S)$, then ρ_S is an invariant of the code C. □

Given a code C and a state σ on n qubits, we define the trace-distance between σ and C as $\inf_{\rho\in C} \|\rho - \sigma\|_1$.

We will refer to a code C as a *stabilizer* code if it can be expressed as the simultaneous eigenspace of a subgroup of Pauli operators.

[3] The Knill–Laflamme conditions are often stated for $E = E_i^\dagger E_j$ where both E_i and E_j are correctable errors. This can lead to a difference in notation for the distance by a factor of 2. This is not relevant for the asymptotic scaling we consider in this article.

Definition 2.2 (Pauli group)**.** The Pauli group on n qubits, denoted by $\mathcal{P}_n$ is the group generated by the n-fold tensor product of the Pauli matrices

$$\mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.8}$$

Definition 2.3 (Stabilizer Code)**.** Let $\{C_i\}_{i\in[N]}$ be a collection of commuting Pauli operators from $\mathcal{P}_n$ and $\mathcal{S}$ be the group generated by $\{C_i\}$ with multiplication. The stabilizer error-correcting code C is defined as the simultaneous +1 eigenspace of each element of $\mathcal{S}$:

$$C = \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : C_i |\psi\rangle = |\psi\rangle \ \forall i \in [N] \right\}. \tag{2.9}$$

More generally, for every $s \in \{0,1\}^N$, define the space D_s as

$$D_s = \left\{ |\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : C_i |\psi\rangle = (-1)^{s_i} |\psi\rangle \ \forall i \in [N] \right\}. \tag{2.10}$$

In this language, $C = D_{0^N}$. The logical operators $\mathcal{L}$ are the collection of Pauli operators that commute with every element of $\mathcal{S}$ but are not generated by $\mathcal{S}$:

$$\mathcal{L} = \{P \in \mathcal{P}_n : PC_i = C_iP \ \forall i \in [N]\} \setminus \mathcal{S}. \tag{2.11}$$

We say that the code is ℓ-local if every C_i is trivial on all but ℓ components of the tensor product and that each qubit of the code is non-trivial in at most ℓ of the checks $\{C_i\}$.

Given a stabilizer code defined by $\{C_i\}_{i\in[N]}$, the associated local Hamiltonian is defined by

$$H = \sum_{i\in[N]} H_i \overset{\text{def}}{=} \sum_{i\in[N]} \frac{\mathbb{I} - C_i}{2}. \tag{2.12}$$

This Hamiltonian is therefore commuting and furthermore it is a ℓ-local low-density parity check Hamiltonian where ℓ is the locality of the code. Since the Hamiltonian consists of commuting terms, by considering the basis in which every local term is simultaneously diagonal, one can see that the eigenspaces of H are precisely the spaces $\{D_s\}$ with corresponding eigenvalues of $|s|$, the Hamming weight of s. If the rate of the stabilizer code is k, we can identify a subset of $2k$ logical operators denoted as

$$\overline{X_1}, \overline{Z_1}, \ldots, \overline{X_k}, \overline{Z_k} \tag{2.13}$$

such that all operators square to identity and pairwise commute except $\overline{X_i}$ and $\overline{Z_i}$ which anti-commute for all $i \in [k]$.

2.3 Circuits and lightcones

We will assume that all quantum circuits in this paper consist of gates with fan-in and fan-out of 2 and that the connectivity of the circuits is all-to-all. The gate set for the circuits will be the collection of all 2 qubit unitaries. Our results will be modified only by a constant factor if we assume gates with a larger constant bound on the fan-in and fan-out.

Definition 2.4 (Circuit Complexity)**.** Let ρ be a mixed quantum state of n qubits. Then the circuit complexity[4] of ρ, $\mathsf{cc}(\rho)$, is defined as the minimum depth over all m-qubit quantum circuits U such that $U\left|0\right\rangle^{\otimes m} \in (\mathbb{C}^2)^{\otimes m}$ is a purification of ρ. Equivalently,

$$\mathsf{cc}(\rho) = \min\left\{\text{depth}(U) : \text{tr}_{[m]\setminus[n]}\left(U\left|0\middle\rangle\middle\langle 0\right|^{\otimes m} U^\dagger\right) = \rho\right\}. \tag{2.14}$$

All product states including classical pure states have circuit complexity 0 or 1. Given a state ψ of circuit complexity t, each individual qubit of ψ is entangled with at most 2^t other qubits, and therefore, states of constant circuit complexity are referred to as "trivial" or "classical" and likewise states of super-constant circuit complexity are inherently "quantum" and possess complex entanglement. Furthermore, properties of constant circuit complexity states are easy to classically verify: the energy $\text{tr}(H\psi)$ of ψ with respect to a local Hamiltonian H can be computed classically in time $\exp(\exp(t))$.

Let $U = U_t \cdots U_1$ be a depth t circuit acting on $(\mathbb{C}^2)^{\otimes m}$, where each $U_j = \bigotimes_k u_{j,k}$ is a tensor product of disjoint two-qubit unitaries $u_{j,k}$. Fix a set of qubits $A \subset [m]$. We say that a qubit i is in the lightcone of A with respect to U if the following holds. There is a sequence of successively overlapping two-qubit unitaries $\{u_{t,k_t}, u_{t-1,k_{t-1}}, \ldots u_{b,k_b}\}$ (with $1 \leq b \leq t$) such that the following holds: supports of u_{t,k_t} and A intersect, the supports of u_{j,k_j} and $u_{j-1,k_{j-1}}$ intersect for all $b < j \leq t$, and the qubit i is in the support of u_{b,k_b}. The support of the lightcone of A with respect to U is the set of qubits in the lightcone of A with respect to U. We represent as U_A the circuit obtained by removing all the two-qubit unitaries from U not in the support of the light cone of A. We will use the following facts about lightcones.

Fact 2.5. *Consider a quantum state ψ acting on $(\mathbb{C}^2)^{\otimes m}$. For any $A \in [m]$, let L_A denote the support of the lightcone of A with respect to U. It holds that*

$$\text{tr}_{-A}(U\psi U^\dagger) = \text{tr}_{-A}\left(U(\psi_{L_A} \otimes \nu_{-L_A})U^\dagger\right). \tag{2.15}$$

In other words, the reduced state on qubit A, only depends on the reduced state ψ_{L_A} on the lightcone of A.

Proof. For any operator O supported on A, consider

$$\begin{aligned} \text{tr}_A(O\,\text{tr}_{-A}(U\psi U^\dagger)) = \text{tr}\Big(U^\dagger O U\psi\Big) &= \text{tr}\Big(U^\dagger O U \psi_{L_A} \otimes \nu_{-L_A}\Big) &(2.16)\\ &= \text{tr}_A(O\,\text{tr}_{-A}(U(\psi_{L_A} \otimes \nu_{-L_A})U^\dagger)). &(2.17)\end{aligned}$$

The second equality uses $U^\dagger O U = U_A^\dagger O U_A$ where U_A is the circuit restricted to the region A. This proves the fact. □

[4] We note that while our definition for circuit complexity of ρ is given as the minimum depth of any circuit exactly generating a state ρ, we could have equivalently defined the circuit complexity of ρ as the minimum depth of any circuit generating a state ρ' within a small ball $B_\delta(\rho)$ of ρ for some $\delta > 0$. This would not have changed our results except for constant factors. This is because our results will be concerned with lower-bounding the circuit complexity of all states of energy $\leq \epsilon n$. If ρ is a state of energy $\leq \epsilon n$, then every state $\rho' \in B_\delta(\rho)$ has energy $\leq (\epsilon + \delta)n$. Therefore, by redefining $\epsilon \longleftarrow \epsilon - \delta$, we can switch to the alternate definition of circuit complexity. We use the listed definition in our proofs as it vastly simplifies legibility.

Fact 2.6. *Consider a quantum state $\left|\phi\right\rangle = U\left|0\right\rangle^{\otimes m}$. Let $A \subset [m]$ and define $\left|\phi'\right\rangle = U_A\left|0\right\rangle^{\otimes m}$. We have $\mathrm{tr}_{-A}(\phi) = \mathrm{tr}_{-A}(\phi')$.*

Proof. The proof is very similar to that of Fact 2.5. For any operator O supported on A, consider

$$\mathrm{tr}\big(O\,\mathrm{tr}_{-A}(\phi)\big) = \mathrm{tr}\Big(U^\dagger O U \left|0\middle\rangle\middle\langle 0\right|^m\Big) = \mathrm{tr}\Big(U_A^\dagger O U_A \left|0\middle\rangle\middle\langle 0\right|^m\Big) = \mathrm{tr}\big(O\,\mathrm{tr}_{-A}(\phi')\big). \tag{2.18}$$

This completes the proof. □

In our proofs, we will assume the simple upper bound of $2^t|A|$ for the size of the lightcone generated by a depth t circuit. This assumes all-to-all connectivity of the circuit. If the circuit was geometrically constrained to a lattice of a fixed constant dimension D, then the simple upper bound would be $O((tD)^D|A|)$. All our proofs can easily be translated into lower bounds for geometric circuits on a lattice using this substitution.

2.4 Quantum PCP conjecture and NLTS statement

We review the definitions of the quantum PCP conjecture and NLTS statement and their relationship.

Conjecture 2.7 (Quantum PCP [6, 3]). *There exist an integer q and a constant $c > 0$ such that it is QMA-hard to decide whether, given (H, a, b) where a, b are rational numbers, $H = H_1 + \cdots + H_m$ is a q-local Hamiltonian, and $b - a \geq cm$, is the minimum eigenvalue of H at most a or at least b.*

Since it is widely believed that NP ≠ QMA, solutions (i. e., ground-states) of QMA-complete local Hamiltonians should not have classically checkable descriptions; for one, ground-states of QMA-complete local Hamiltonians should not have constant circuit complexity.

If we assume the quantum PCP conjecture, then *no low-energy* states of the local Hamiltonians corresponding to Yes instances of quantum PCP problems should have constant circuit complexity. This is because if there exists a a state of constant circuit complexity and of energy less than the promise gap, then the circuit description of the state can serve as a *classically checkable witness* to the local Hamiltonian problem. This would place the promise gapped problem in NP. Since the quantum PCP conjecture posits that promise gapped local Hamiltonians are also QMA-complete, this would imply that NP = QMA, a contradiction. This is the inspiration for the NLTS statement.

Theorem 2.8 (NLTS [30, 9]). *There exists a fixed constant $\epsilon > 0$ and an explicit family of $O(1)$-local Hamiltonians $\{H^{(n)}\}_{n=1}^{\infty}$, where $H^{(n)}$ acts on n particles and consists of $\Theta(n)$ local terms, such that for any family of states $\{\psi_n\}$ satisfying*

$$\mathrm{tr}\Big(H^{(n)}\psi_n\Big) \leq \epsilon n + \lambda_{\min}(H^{(n)}), \tag{2.19}$$

the circuit complexity $\mathsf{cc}(\psi_n)$ grows as $\Omega(\log n)$.[5]*.*

[5] This definition is the one originally expressed by Freedman and Hastings in [30]. However, a consequence of the quantum PCP conjecture and NP ≠ QMA would be a circuit complexity lower bound of $\omega(\log\log n)$. For this

Therefore, making the widely believed assumption $\mathsf{NP} \neq \mathsf{QMA}$, the quantum PCP conjecture implies the NLTS statement, thereby identifying a necessary property of any QMA-complete promise gapped local Hamiltonian. This property is referred to as "robust entanglement" since the entanglement complexity of every low-energy state must be non-trivial. Resolution of the NLTS statement was an important first step towards proving the quantum PCP conjecture. One of the advantages of the NLTS statement is that it does not involve complexity classes such as QMA, but rather focuses solely on the entanglement complexity that is intrinsic to low-energy states of local Hamiltonians.

3 Robust entropy-based lower bounds

In this section, we subsume a folklore proof for the circuit complexity of code-states to prove that the lower bound is robust against small trace-distance perturbations.

Lemma 3.1. *Let C be a $[[n, k, d]]$ code and ψ a state on m qubits. Let ψ_{code} be the reduced state on the n code qubits. If the trace-distance between ψ_{code} and C is $0 < \delta < 1/2$ and the code is of rate at least $k > 2\delta \log(1/\delta)m$, then the circuit complexity $cc(\psi) > \log d$.*

Proof. Let ψ be a state on m qubits such that $\psi = U |0\rangle^{\otimes m}$ where U is a circuit of depth t. Suppose $2^t < d$. Further assume that ψ is δ-close to the code C in trace distance, meaning that there exists a state $\rho_{\mathsf{code}} \in C$ such that $\|\psi_{\mathsf{code}} - \rho_{\mathsf{code}}\|_1 \leq \delta$. Thus, Uhlmann's theorem [57] ensures that there is a purification $|\rho\rangle$ on m qubits such that $\||\psi\rangle\langle\psi| - |\rho\rangle\langle\rho|\|_1 \leq \delta$.

Let Enc be any encoding CPTP map from $(\mathbb{C}^2)^{\otimes k} \to (\mathbb{C}^2)^{\otimes n}$ mapping k qubits to the k qubit code-space. Define $\mathcal{E}$ as the maximally decohering channel as follows

$$\mathcal{E}(\cdot) \overset{\mathsf{def}}{=} \frac{1}{4^k} \sum_{a,b \in \{0,1\}^k} \left(X^a Z^b\right) (\cdot) \left(X^a Z^b\right)^\dagger . \tag{3.1}$$

Then let Θ be the encoding of ρ defined as

$$\Theta \overset{\mathsf{def}}{=} \mathrm{Enc} \circ \mathcal{E} \circ \mathrm{Enc}^{-1}(\rho). \tag{3.2}$$

This state is well-defined and has entropy $S(\Theta) \geq k$ since $S(\mathcal{E}(\rho)) \geq k$. We omit proof of this statement here as it is covered in greater generality by Fact 4.4.

Fact 3.2 (Extended local indistinguishability property)**.** *For any region $R_1 \cup R_2$ where R_1 is contained in the code qubits and R_2 in the ancilla qubits with $|R_1| < d$, $\rho_{R_1 \cup R_2} = \Theta_{R_1 \cup R_2}$.*

reason, we will be more interested in circuit lower bounds of $\omega(\log \log n)$. This is because calculating the energy of a state of depth $O(\log \log n)$ with respect to any local Hamiltonian can be done by a classical $\mathsf{poly}(n)$-time algorithm. Furthermore, if $\mathsf{QCMA} \neq \mathsf{QMA}$ (QCMA is another potential analog of NP like QCMA; it corresponds to proofs that are classical while their verification is quantum), then the necessary consequence of the quantum PCP conjecture is a circuit lower bound of $\omega(\mathsf{poly}(n))$. Our techniques make no obvious progress towards this strengthened conjecture as we study stabilizer codes whose circuit complexity is $O(\log n)$. Some progress towards super-polynomial NLETS was made by Nirkhe, Vazirani, and Yuen [50].

We prove this fact after the lemma. Let $R \subset [m]$ be any region of the qubits of size $< d$. Using this fact,

$$\|\psi_R - \Theta_R\|_1 \le \delta. \tag{3.3}$$

For any qubit $i \in [m]$, let $L_i \subset [m]$ be the support of the lightcone of i with respect to U. The size of L_i, $|L_i|$ is at most $2^t < d$. Applying Fact 2.5 here, we have

$$\mathrm{tr}_{-\{i\}}(U^\dagger \Theta U) = \mathrm{tr}_{-\{i\}}(U^\dagger(\Theta_{L_i} \otimes \nu_{-L_i})U). \tag{3.4}$$

Since the size of L_i is $< d$, we can combine Equations (3.3) and (3.4) to achieve

$$\left\|\mathrm{tr}_{-\{i\}}(U^\dagger(\psi_{L_i} \otimes \nu_{-L_i})U) - \mathrm{tr}_{-\{i\}}(U^\dagger(\Theta_{L_i} \otimes \nu_{-L_i})U)\right\|_1 \le \delta. \tag{3.5}$$

However, $U^\dagger \psi U = |0\rangle\langle 0|^{\otimes m}$ and so

$$\left\||0\rangle\langle 0| - \mathrm{tr}_{-\{i\}}(U^\dagger(\Theta_{L_i} \otimes \nu_{-L_i})U)\right\|_1 \le \delta. \tag{3.6}$$

Using standard entropy bounds[6], we can bound the entropy of the ith qubit of the rotated state Θ:

$$S\left(\mathrm{tr}_{-\{i\}}(U^\dagger \Theta U)\right) = S\left(\mathrm{tr}_{-\{i\}}(U^\dagger(\Theta_{L_i} \otimes \nu_{-L_i})U)\right) \le H_2(\delta) \le 2\delta\log(1/\delta). \tag{3.7}$$

Notice that $S(U^\dagger \Theta U) = S(\Theta) = k$. We can, therefore, bound k by

$$k \le S(\Theta) \le \sum_{i \in [m]} S\left(\mathrm{tr}_{-\{i\}}(U^\dagger \Theta U)\right) \le 2\delta\log(1/\delta)m. \tag{3.8}$$

This leads to a contradiction since we assumed $k > 2\delta\log(1/\delta)m$. □

If $m = n$, then this provides a circuit lower bound for linear-rate codes. Fact 2.6 ensures that we can assume $m \le 2^{\mathsf{cc}(\psi)}n$, without loss of generality. This gives us the following corollary:

Corollary 3.3. *Let C be a $[[n, k, d]]$ code and $|\psi\rangle$ a pure-state and the trace-distance between $|\psi\rangle$ and C is $0 < \delta < 1/2$ such that $k > 2\delta\log(1/\delta)n$. Then, the circuit complexity $\mathsf{cc}(|\psi\rangle)$ satisfies*

$$\mathsf{cc}(|\psi\rangle) \ge \log\left(\min\left\{d, \frac{k}{2\delta\log(1/\delta)n}\right\}\right). \tag{3.9}$$

Proof. By Lemma 3.1, either $2^{\mathsf{cc}(|\psi\rangle)} \ge d$ or $k \le 2\delta\log(1/\delta)2^{\mathsf{cc}(|\psi\rangle)}n$ since $m \le 2^{\mathsf{cc}(|\psi\rangle)}n$. Rearranging this is equivalent to the corollary. □

[6] Namely, that $H_2(x) \le x\log(1/x)$.

Proof. (of Fact 3.2) Let R_1 be a subset of the code qubits and R_2 be a subset of the ancilla qubits such that $|R_1| < d$. We can express any code-state $|\psi\rangle$ over the m qubits as

$$|\psi\rangle = \sum_{x \in \{0,1\}^k} |\overline{x}\rangle\, |\psi_x\rangle \tag{3.10}$$

where $\{|\overline{x}\rangle\}$ is a basis for the code and $|\psi_x\rangle$ are un-normalized. Let U be any logical operator (i. e., one that preserves the code-space). Then,

$$\operatorname{tr}_{-(R_1 \cup R_2)}\left(U\psi U^\dagger\right) = \sum_{x,y \in \{0,1\}^k} \operatorname{tr}_{-R_1}(U\,|\overline{x}\rangle\!\langle\overline{y}|\,U^\dagger) \otimes \operatorname{tr}_{-R_2}(|\psi_x\rangle\!\langle\psi_y|) \tag{3.11}$$

In the summation, if $x = y$, then the first component is ϕ_{R_1} for some fixed state ϕ_{R_1} by local indistinguishability. Furthermore, if $x \neq y$, then the first component is 0 by orthogonality of $U\,|\overline{x}\rangle$ and $U\,|\overline{y}\rangle$ despite the erasure of $|R_1| < d$ qubits. Therefore,

$$\operatorname{tr}_{-(R_1 \cup R_2)}\left(U\psi U^\dagger\right) = \phi_{R_1} \otimes \sum_{x \in \{0,1\}^k} \operatorname{tr}_{-R_2}(\psi_x). \tag{3.12}$$

which is an invariant of U, which means $\operatorname{tr}_{-(R_1 \cup R_2)}(\rho) = \operatorname{tr}_{-(R_1 \cup R_2)}(U\rho U^\dagger)$. Since (a) Θ is a mixture over applications of *logical* Paulis to ρ and (b) a logical operator applied to a code-state is another code-state and therefore is locally indistinguishable, then it follows that $\rho_{R_1 \cup R_2} = \Theta_{R_1 \cup R_2}$. □

3.1 Improved circuit lower bounds using AGSPs

Corollary 3.3 shows that if we are given a $[[n, k, d]]$ code with linear rate $k = \Omega(n)$, then a state generated by a depth $t \leq \gamma \log d$ circuit must be $\Omega\left(2^{-2t}\right) = \Omega\left(d^{-2\gamma}\right)$ far from the code-space in trace distance. Now we show an even stronger separation, if the code is the zero-eigenspace (ground-space) of a commuting local Hamiltonian.

Consider a $[[n, k, d]]$ QLDPC code C which is the common zero-eigenspace of commuting checks $\{\Pi_j\}_{j=1}^N$ of locality ℓ each (this includes, but is not restricted to, the stabilizer code defined earlier). Consider a state $|\psi\rangle = U\,|0\rangle^{\otimes m}$ obtained by applying a depth t circuit U on m qubits. Suppose there is a state $\rho_0 \in C$ having good fidelity with the code-space, that is, $f \overset{\text{def}}{=} F(\psi_{\mathsf{code}}, \rho_0)$. Fact 2.6 ensures that we can choose $m \leq 2^t n$. We prove the following lemma.

Lemma 3.4. *For the state $|\psi\rangle$ as defined above, it holds that*

$$2^{2t} \geq \min\left(d, \frac{1}{64\sqrt{\ell}\log^2 d\ell} \cdot \frac{k\sqrt{d}}{n \cdot \sqrt{\log\frac{1}{f}}}\right). \tag{3.13}$$

The proof of this lemma appears in the Appendix B. It uses the tool of approximate ground-space projectors (AGSP) and the principle that low min-entropy for gapped ground-states implies low entanglement entropy [32, 14, 13, 10]. The lemma shows that if the code has linear rate $k = \Omega(n)$, then any state generated by a depth $t \leq \gamma \log d$ circuit must be $1 - \exp\left(-\widetilde{\Omega}\left(d^{1-4\gamma}\right)\right)$ far from the code-space in trace distance. Here, the $\widetilde{\Omega}$ notation hides some polylog factors. This bears some resemblance with the results of [16, 46], which show that the distributions sampled from depth t (and size $\mathrm{e}^{n^{1/t}}$) classical $\mathsf{AC0}$ circuits are $1 - \mathrm{e}^{-n^{1/t}}$ far from the uniform distribution over a good classical code (linear rate and linear distance). A comparison with Lemma 3.4 is largely unclear, due to the differences between classical and quantum codes, as well as $\mathsf{AC0}$ circuits and quantum circuits.

We further prove the following lemma for codes encoding at least one qubit and having large distance. This complements Lemma 3.4 replacing the linear rate condition with linear distance condition. We note that the use of Chebyshev polynomials to improve circuit lower bounds was also used by Eldar and Harrow [27, Propositions 44,45].

Lemma 3.5. *Given $|\psi\rangle = U|0\rangle^{\otimes m}$ with U of depth t and let C be a code with distance d. Let Π be the projector onto the codespace and $f = \sqrt{\langle\psi|(\Pi \otimes \mathbb{I}_{\mathsf{anc}})|\psi\rangle}$ be the fidelity of $|\psi\rangle$ with the codespace. If $2^t \leq \frac{d}{2}$ then*

$$f^2 \leq 2\mathrm{e}^{-\frac{d^2}{2^{2t+10}m}}. \tag{3.14}$$

Proof. Let $G = \sum_{i=1}^{m} U|1\rangle\langle 1|_i U^\dagger$ be the 2^t local Hamiltonian with $|\psi\rangle$ as its unique ground state. From Fact B.2, there is a polynomial $P(G)$ of degree $\frac{d}{2^{t+1}}$ such that

$$\|P(G) - |\psi\rangle\langle\psi|\| \leq \mathrm{e}^{-\left(\frac{d}{2^{t+1}}\right)^2/2^8 m} = \mathrm{e}^{-\frac{d^2}{2^{2t+10}m}}. \tag{3.15}$$

Note that each multinomial term in $P(G)$ is supported on $\leq 2^t \cdot \frac{d}{2^{t+1}} \leq \frac{d}{2}$ terms. Let $|\phi\rangle = \Pi|\psi\rangle/f$ be the codestate having largest overlap with $|\psi\rangle$. Consider any vector $|\phi'\rangle$ with $\phi'_{\mathsf{code}} \in \Pi$ that is orthogonal to $|\phi\rangle$ (and hence orthogonal to $|\psi\rangle$). One way to construct $|\phi'\rangle$ is to expand $|\phi\rangle = \sum_x |\bar{x}\rangle|\phi_x\rangle$ (with $\{|\bar{x}\rangle\}_x$ a basis for Π and $|\phi_x\rangle$ unnormalized) and then define $|\phi'\rangle \propto \sum_x \alpha_x |\bar{x}\rangle|\phi_x\rangle$. The complex numbers $\{\alpha_x\}_x$ are chosen such that

$$\sum_x \alpha_x \langle\phi_x|\phi_x\rangle = 0 \implies \langle\phi|\phi'\rangle = 0. \tag{3.16}$$

Since $P(G)$ is a sum of $\leq \frac{d}{2}$-local terms, Equation (2.3) ensures that

$$\langle\phi'|P(G)|\phi'\rangle = \langle\phi'|\Pi P(G)\Pi|\phi'\rangle = \eta_{P(G)}\langle\phi'|\Pi|\phi'\rangle = \eta_{P(G)} = \langle\phi|P(G)|\phi\rangle. \tag{3.17}$$

Using Equation (3.15) and $\langle\phi'|\psi\rangle = 0$, we have $\langle\phi'|P(G)|\phi'\rangle \leq \mathrm{e}^{-\frac{d^2}{2^{2t+10}m}}$. Thus using Equation (3.15) again,

$$f^2 = |\langle\phi|\psi\rangle|^2 \leq \langle\phi|P(G)|\phi\rangle + \mathrm{e}^{-\frac{d^2}{2^{2t+10}m}} = \langle\phi'|P(G)|\phi'\rangle + \mathrm{e}^{-\frac{d^2}{2^{2t+10}m}} \leq 2\mathrm{e}^{-\frac{d^2}{2^{2t+10}m}}. \tag{3.18}$$

This proves the lemma. □

Even with such a wide separation between the code-space and the states generated by low-depth circuits, these results give no insights into the energy such states can achieve. This is because these results do not rule out the possibility that such low-depth circuits live in the energy 1 eigenspace of the code Hamiltonian, which is orthogonal to the code-space. In the later section, we show how to achieve this guarantee; this proves our main result.

4 Lower bounds for stabilizer codes

In this section we prove Theorem 1.1; which combines Theorems 4.6 and 4.9. For Theorem 4.6, we show how the entropy-based bounds from the previous section can be improved from handling states physically near the code-space to all low-energy states, once we assume that the code is a stabilizer code. The key property we exploit is that the local indistinguishability property of the code-space C also holds for each eigenspace D_s in the case of stabilizer codes. We make this precise in the following facts; all facts are proven after the proof of the theorems.

The following fact argues that logical operators not only preserve the code-space C but rather any eigenspace D_s.

Fact 4.1. *Fix a stabilizer code C on n qubits with generator set $\{C_i\}_{i\in[N]}$. For any string $s \in \{0,1\}^n$, a state ρ such that $\rho_{\mathsf{code}} \in D_s$, and a logical operator $P \in \mathcal{L}$, we have $(P\rho P)_{\mathsf{code}} \in D_s$.*

Each pair of Pauli operators either commute or anti-commute. The following fact imposes constraints on non-logical and non-stabilizer Pauli operators.

Fact 4.2. *Let P be a Pauli operator such that for some $i \in [N]$, $PC_i = -C_iP$. For any $s \in \{0,1\}^N$ and any quantum state ρ such that $\rho_{\mathsf{code}} \in D_s$, we have $\mathrm{tr}(P\rho) = 0$.*

The third crucial fact we will use is about the local indistinguishability of stabilizer codes. We will show that the measure of any local operator of locality $< d$, the distance of the code, is an invariant of each eigenspace D_s.

Fact 4.3. *Let ρ be a state such that $\rho_{code} \in D_s$ for a string s. For a logical pauli $P \in \mathcal{L}$, define $\rho' = P\rho P$. It holds that for any region $T \subset [m]$ of size less than d, $\rho_T = \rho'_T$. In general, let ρ, ρ' be states such that $\rho_{\mathsf{anc}} = \rho'_{\mathsf{anc}}$ and $\rho_{code}, \rho'_{code} \in D_s$ for a string s. It holds that for any region $T \subset [m]$ of size less than d, $\rho_T = \rho'_T$.*

Since logical operators act like single qubit Pauli operators within the code-space, they can be used for randomization. Define the following quantum "completely depolarizing in the logical basis" channel that acts on code qubits, analogous to the channel defined in Equation (3.2):

$$\mathcal{E}(\cdot) \overset{\mathsf{def}}{=} \frac{1}{4^k} \sum_{a,b\in\{0,1\}^k} \left(\overline{X}^a\overline{Z}^b\right)(\cdot)\left(\overline{Z}^b\overline{X}^a\right) \tag{4.1}$$

where $\overline{X}^a = \prod_i \overline{X_i}^{a_i}$ is a product of logical X operators defined by a and likewise $\overline{Z}^b$ is a product of logical Z operators defined by b. We will utilize the following two properties of this channel, analogous to Fact 3.2.

Fact 4.4. *It holds that*

1. *For any quantum state ρ, the entropy $S(\mathcal{E}(\rho)) \geq k$.*
2. *For any quantum state ρ such that $\rho_{\mathsf{code}} \in D_s$ for some s, $\mathcal{E}(\rho)_{\mathsf{code}} \in D_s$. Furthermore, for any set $T \subset [m]$ of size less than d, $\rho_T = \mathcal{E}(\rho)_T$.*

The next fact describes how all stabilizer terms of the code can be measured simultaneously using a short-depth circuit if the code has small locality. Let N be the number of checks for an ℓ-local code; recall that then $n/\ell \leq N \leq \ell n$.

Fact 4.5. *Let C be a stabilizer code of locality ℓ on n qubits with N checks $\{C_i\}_{i\in[N]}$. Then, there is a circuit V of depth $\leq 2\ell^3$ which coherently measures the value of each stabilizer term into N ancilla.*

Lastly, consider a state $\left|\phi\right\rangle = U\left|0\right\rangle^{\otimes m}$ where U is a circuit of depth t. From Fact 2.6, we can assume $m \leq n2^t$ without loss of generality. We are now ready to state and prove the following theorem for codes of large rate.

Theorem 4.6. *Let C be a $[[n,k,d]]$ stabilizer code of locality ℓ defined by checks $\{C_i\}_{i\in[N]}$. Let H be the corresponding Hamiltonian. Suppose there is a state $\left|\phi\right\rangle$ on m qubits with $\mathrm{tr}(H\phi) \leq \epsilon N$ and circuit complexity $t \overset{\mathsf{def}}{=} \mathsf{cc}(\phi) < \log(d) - 2\ell^3$. Then, for a constant c_ℓ depending only on ℓ and not the size of the code,*

$$2^{2t} > \frac{k}{c_\ell n \cdot \epsilon \log\frac{1}{\epsilon}}. \tag{4.2}$$

Proof. All stated intermediate claims are proven in the next sub-section. By assumption, $\left|\phi\right\rangle = U\left|0\right\rangle^{\otimes m}$ for a circuit of depth $t < \log(d) - 2\ell^3$. Define the energy of each local Hamiltonian term H_i as

$$\epsilon_i \overset{\mathsf{def}}{=} \mathrm{tr}(H_i\phi) = \frac{1}{2} - \frac{1}{2}\mathrm{tr}(C_i\phi). \tag{4.3}$$

Add $N \leq n$ new syndrome-measurement ancilla (SMA) qubits each with initial state $\left|0\right\rangle$ and coherently measure the entire syndrome using the depth $2\ell^3$ circuit V from Fact 4.5. Then the state

$$\left|\psi\right\rangle = V\left(\left|\phi\right\rangle \otimes \left|0\right\rangle^{\otimes N}\right) = VU\left|0\right\rangle^{\otimes(m+N)} \overset{\mathsf{def}}{=} W\left|0\right\rangle^{\otimes(m+N)} \tag{4.4}$$

with $W = VU$ a circuit of minimum circuit depth $\overset{\mathsf{def}}{=} \mathsf{cc}(W) \leq t + 2\ell^3$.

Define the state obtained by incoherently measuring all the SMA qubits of $\left|\psi\right\rangle$ as

$$\Psi = \sum_{s\in\{0,1\}^N} D_s\left|\phi\right\rangle\!\left\langle\phi\right| D_s \otimes \left|s\right\rangle\!\left\langle s\right| \tag{4.5}$$

where we abuse notation slightly and use D_s both as the eigenspace and the projector onto it. Since we assume that C is a stabilizer code, the Hamiltonian terms H_i all mutually commute and therefore so do the measurements of the SMA qubits. Therefore, the order of measurement used is irrelevant.

Define the state $\Theta = \mathcal{E}(\Psi)$ obtained by applying the logical completely depolarizing channel $\mathcal{E}$ from Equation (4.1). Then, we have

$$\Theta = \sum_s \operatorname{tr}\left(D_s \phi D_s\right) \mu_s \otimes |s\rangle\langle s| \qquad \text{for } \mu_s \overset{\text{def}}{=} \mathcal{E}\left(\frac{D_s \phi D_s}{\operatorname{tr}\left(D_s \phi D_s\right)}\right). \tag{4.6}$$

Claim 4.7. *Fix any region $R \subset [m+N]$. Let S_R be the set of all indices $i \in [N]$ such that the ith SMA qubit belongs to R. It holds that*

$$F(\psi_R, \Psi_R) \geq 1 - \sum_{i \in S_R} \epsilon_i. \tag{4.7}$$

Further, if $|R| < d$, then $\Psi_R = \Theta_R$.

For every $j \in [m+N]$, let L_j be the support of the lightcone of j with respect to the unitary $W^\dagger$. Note that $|L_j| \leq 2^{\mathsf{cc}(W)} < d$. Since $W^\dagger |\psi\rangle$ is $|0\rangle^{\otimes(m+N)}$, we have that for any qubit $j \in [m+N]$,

$$\operatorname{tr}_{-\{j\}}\left(W^\dagger \psi W\right) = |0\rangle\langle 0|\,. \tag{4.8}$$

However, Fact 2.5 allows us to equate

$$\operatorname{tr}_{-\{j\}}\left(W^\dagger \psi W\right) = \operatorname{tr}_{-\{j\}}\left(W^\dagger(\psi_{L_j} \otimes \nu_{-L_j})W\right), \tag{4.9}$$

$$\operatorname{tr}_{-\{j\}}\left(W^\dagger \Theta W\right) = \operatorname{tr}_{-\{j\}}\left(W^\dagger(\Theta_{L_j} \otimes \nu_{-L_j})W\right). \tag{4.10}$$

Using Equation (4.7), we find that for all $j \in [m+N]$,

$$\begin{aligned}
&F\left(\operatorname{tr}_{-\{j\}}\left(W^\dagger \psi W\right), \operatorname{tr}_{-\{j\}}\left(W^\dagger \Theta W\right)\right) && (4.11)\\
&= F\left(\operatorname{tr}_{-\{j\}}\left(W^\dagger(\psi_{L_j} \otimes \nu_{-L_j})W\right), \operatorname{tr}_{-\{j\}}\left(W^\dagger(\Theta_{L_j} \otimes \nu_{-L_j})W\right)\right) && (4.12)\\
&\geq F\left(\psi_{L_j}, \Theta_{L_j}\right) && (4.13)\\
&\geq 1 - \sum_{i \in S_{L_j}} \epsilon_i. && (4.14)
\end{aligned}$$

We now infer from Equations (4.8) and (4.14) that[7]

$$S\left(\operatorname{tr}_{-\{j\}}\left(W^\dagger \Theta W\right)\right) \leq 2\left(\sum_{i \in S_{L_j}} \epsilon_i\right) \log \frac{1}{\min\left(\sum_{i \in S_{L_j}} \epsilon_i, \frac{1}{4}\right)}. \tag{4.15}$$

[7] Given a binary distribution $(p, 1-p)$, we can upper bound its entropy as follows. If $p \geq \frac{1}{4}$, then an upper bound is 1. Else the upper bound is $2p \log \frac{1}{p}$. The combined upper bound is $2p \log \frac{1}{\min(p, \frac{1}{4})}$.

Using the concavity of the function $x \mapsto x \log \frac{1}{\min(x, \frac{1}{4})}$ in the interval $x \in (0, 2^{\mathsf{cc}(W)})$, we can average over all $j \in [m+N]$ to conclude

$$\begin{aligned}
&\mathop{\mathbb{E}}_{j \in [m+N]} S\left(\mathrm{tr}_{-\{j\}}\left(W^\dagger \Theta W\right)\right) && (4.16)\\
&\leq 2 \mathop{\mathbb{E}}_{j \in [m+N]} \left(\left(\sum_{i \in S_{L_j}} \epsilon_i\right) \log \frac{1}{\min\left(\sum_{i \in S_{L_j}} \epsilon_i, \frac{1}{4}\right)}\right) && (4.17)\\
&\leq 2 \cdot \left(\mathop{\mathbb{E}}_{j \in [m+N]} \sum_{i \in S_{L_j}} \epsilon_i\right) \log \frac{1}{\min\left(\mathbb{E}_{j \in [m+N]} \sum_{i \in S_{L_j}} \epsilon_i, \frac{1}{4}\right)}. && (4.18)
\end{aligned}$$

The next claim helps upper and lower bound this expression.

Claim 4.8. *It holds that*

$$\frac{\epsilon N}{m+N} \leq \mathop{\mathbb{E}}_{j \in [m+N]} \sum_{i \in S_{L_j}} \epsilon_i \leq 2^{2\mathsf{cc}(W)} \frac{\epsilon N}{m+N}. \tag{4.19}$$

Now we give an upper bound on the entropy of Θ. For this, let us assume $2^{\mathsf{cc}(W)} \leq \frac{1}{\epsilon}$, otherwise the proof is immediate.

$$\begin{aligned}
S(\Theta) = S(W^\dagger \Theta W) &\leq \sum_{j \in [m+N]} S\left(\mathrm{tr}_{-\{j\}}\left(W^\dagger \Theta W\right)\right) && (4.20)\\
&\leq 2^{1+2\mathsf{cc}(W)} \epsilon N \log \frac{1}{\min\left(\frac{\epsilon N}{m+N}, \frac{1}{4}\right)} && (4.21)\\
&\leq 2^{1+2\mathsf{cc}(W)} \epsilon \ell n \log \frac{2^{\mathsf{cc}(W)}}{\epsilon} && (4.22)\\
&\leq \left(2^{2+2\mathsf{cc}(W)} \ell n\right) \cdot \epsilon \log \frac{1}{\epsilon}. && (4.23)
\end{aligned}$$

The inequality in Equation (4.20) comes from the subadditivity of entropy; the inequality in Equation (4.21) uses Equation (4.17) and then substitutes the upper and lower bounds given in Claim 4.8; the inequality in Equation (4.22) uses $\frac{n}{\ell} \leq N \leq \ell n$ and $\frac{\epsilon N}{m+N} \geq \frac{\epsilon}{\ell 2^t + 1} \geq \frac{\epsilon}{2^{\mathsf{cc}(W)}}$; the inequality in Equation (4.23) uses $2^{\mathsf{cc}(W)} \leq \frac{1}{\epsilon}$. Furthermore, Θ is the output of $\mathcal{E}$ acting on Ψ. By Fact 4.4 (Item 2), $S(\Theta) \geq k$. Combining the lower and upper bounds on the entropy of Θ, the proof concludes. □

Next, we prove the following theorem for codes of large distance.

Theorem 4.9. *Let C be a $[[n,k,d]]$ stabilizer code of locality ℓ defined by checks $\{C_i\}_{i\in[N]}$. Let H be the corresponding Hamiltonian. Suppose there is a state $|\phi\rangle$ on m qubits with $\operatorname{tr}(H\phi) \leq \epsilon N$ and circuit complexity $t \overset{\text{def}}{=} \mathsf{cc}(\phi) < \log(d) - 1$. Then,*

$$2^{2t} \geq \frac{d}{2^6 n \sqrt{\ell\epsilon \log\frac{1}{\epsilon}}}. \tag{4.24}$$

Proof. Since $\operatorname{tr}(H\phi) \leq \epsilon N$, Markov's inequality ensures that $\operatorname{tr}(D_{\leq 2\epsilon N}\phi) \geq \frac{1}{2}$, where $D_{\leq 2\epsilon N}$ is the subspace of energy $\leq 2\epsilon N$. Since $D_{\leq 2\epsilon N} = \sum_{s\in\{0,1\}^N:|s|\leq 2\epsilon N} D_s$ and the number of s satisfying $|s| \leq 2\epsilon N$ is $\leq 2^{4\epsilon N\log\frac{1}{\epsilon}}$, there exists a $s^* \in \{0,1\}^N$ such that $\operatorname{tr}(D_{s^*}\phi) \geq 2^{-4\epsilon N\log\frac{1}{\epsilon}-1}$. Now, Fact 4.3 ensures that D_{s^*} is also an error correcting code of distance d. Applying Lemma 3.5 (assuming $2^t \leq \frac{d}{2}$) and setting $m \leq 2^t n$ (using Fact 2.6), we conclude

$$\begin{aligned} 2^{-4N\epsilon\log\frac{1}{\epsilon}-1} &\leq 2\mathrm{e}^{-\frac{d^2}{2^{3t+10}n}} && (4.25)\\ \implies 2^{4N\epsilon\log\frac{1}{\epsilon}+2} &\geq \mathrm{e}^{\frac{d^2}{2^{3t+10}n}} && (4.26)\\ \implies 2^{3t} &\geq \frac{d^2}{2^{12}nN\epsilon\log\frac{1}{\epsilon}}. && (4.27) \end{aligned}$$

Since $N \leq n\ell$ and $2^{3t} \leq 2^{4t}$, the proof concludes. □

Combining Theorems 4.6 and 4.9, the proof of Theorem 1.1 concludes.

4.1 Omitted proofs

Proof. (of Fact 4.1) For all $i \in [N]$ it suffices to verify that

$$C_i(P\rho P) = PC_i\rho P = P(-1)^{s_i}\rho P = (-1)^{s_i}(P\rho P). \tag{4.28}$$

□

Proof. (of Fact 4.2)

$$\operatorname{tr}(P\rho) = \operatorname{tr}\left(P\left((-1)^{s_i}C_i\rho\right)\right) = (-1)^{s_i+1}\operatorname{tr}(C_iP\rho) = (-1)^{s_i+1}\operatorname{tr}(\rho C_iP) = -\operatorname{tr}(P\rho). \tag{4.29}$$

where we used the cyclicality of trace twice. □

Proof. (of Fact 4.3) Consider the first part of the fact. If the region T lies entirely on the ancilla qubits, then the claim is easy since P is trivial on the ancilla qubits. Thus, consider a region $T = T_{\mathsf{code}} \cup T_{\mathsf{anc}}$ with code region T_{code} and ancilla region T_{anc}. From Fact 4.1, $\rho'_{\mathsf{code}} \in D_s$. Suppose $\rho'_T \neq \rho_T$. Then there is a Pauli operator P' of weight $\leq |T|$ distinguishing the two states:

$$\operatorname{tr}(P'\rho_T) \neq \operatorname{tr}(P'\rho'_T). \tag{4.30}$$

This can be re-written as

$$\mathrm{tr}(P'\rho) \neq \mathrm{tr}(P'\rho') = \mathrm{tr}(PP'P\rho). \tag{4.31}$$

This relation holds only if

1. $\mathrm{tr}(P'\rho) \neq 0$ or $\mathrm{tr}(P'\rho') \neq 0$, and
2. $PP' = -P'P$.

The first relation ensures that P' commutes with all C_i (Fact 4.2) and hence P'_{code} commutes with all C_i. Further, $P'_{\mathsf{code}} \notin \mathcal{S}$, else we would have $PP'_{\mathsf{code}} = P'_{\mathsf{code}}P$ which would imply $\mathrm{tr}(PP'P\rho) = \mathrm{tr}(P'\rho)$. Thus P'_{code} is a logical operator of weight $\leq |T| < d$. This suffices to establish a contradiction and prove the first part. But we can go further: the second relation implies that P'_{code} anti-commutes with P. But this is also a contradiction if $|T|$ is less than the weight of the smallest logical Pauli anti-commuting with P. This will be useful in Section A.

The second part follows similarly. Consider a region $T = T_{\mathsf{code}} \cup T_{\mathsf{anc}}$ such that $\rho_T \neq \rho'_T$. Then there is a Pauli P' of weight $< d$ such that $\mathrm{tr}(P'\rho) \neq \mathrm{tr}(P'\rho')$. Clearly, P'_{code} must be non-identity and one of $\mathrm{tr}(P\rho)$ or $\mathrm{tr}(P\rho')$ should be non-zero. Due to Fact 4.2, P must commute with all C_i. This implies that P_{code} must also commute with all C_i. But then P_{code} is a logical operator with weight less than d, a contradiction. □

Proof. (of Fact 4.4) For the first item, note that there exists an isometry V such that

$$V\overline{X_j}V^\dagger = X_j, \quad V\overline{Z_j}V^\dagger = Z_j, \forall j \in [k], \tag{4.32}$$

where $\{(X_j, Z_j)\}_{j\in[k]}$ are pairs of single qubit pauli operators on k qubits $Q_1, \ldots Q_k$. The map $V\mathcal{E}(V^\dagger(.)V)V^\dagger$ is the completely depolarizing map on these k qubits. Since the completely depolarizing map transforms any quantum state σ to $\mathrm{tr}_{Q_1,\ldots Q_k}(\sigma) \otimes \frac{\mathbb{I}_{Q,\ldots Q_k}}{2^k}$, the statement follows.

The first part of the second item is a consequence of Fact 4.1. For the second part of the second item, we use an argument similar to Fact 4.3. Since $\mathcal{E}$ only acts on code qubits, T must have support on code qubits. Suppose $\rho_T \neq \mathcal{E}(\rho)_T$ and let P be a Pauli such that $\mathrm{tr}(P\rho) \neq \mathrm{tr}(P\mathcal{E}(\rho))$. Since one of the two terms is non-zero, Fact 4.2 ensures that P commutes with all the C_i. But $P_{\mathsf{code}} \notin \mathcal{S}$, else $\mathcal{E}(P) = P$. Thus, P_{code} is a logical Pauli operator. This implies that the weight of P_{code} must be at least d, a contradiction. □

Proof. (of Fact 4.5) Since each code qubit acts non-trivially in at most ℓ checks and each check C_i is of size ℓ, then each check C_i overlaps non-trivially with at most ℓ^2 other checks. Consider a graph defined by vertices $i \in [N]$ and edges whenever checks overlap non-trivially; this graph has degree ℓ^2 and is, therefore, $\ell^2 + 1$-colorable.

The following unitary V_i coherently measures the stabilizer check C_i:

$$V_i \left|\omega\right\rangle \left|y\right\rangle \overset{\mathsf{def}}{=} \frac{\mathbb{I} + C_i}{2} \left|\omega\right\rangle \left|y\right\rangle + \frac{\mathbb{I} - C_i}{2} \left|\omega\right\rangle \left|y \oplus 1\right\rangle. \tag{4.33}$$

Furthermore, there is a depth ℓ circuit which calculates V_i. By the coloring argument, we can produce a depth $\ell(\ell^2 + 1)$ circuit V that coherently measures all the stabilizers; namely, we apply sequentially all the unitaries V_i per color. □

Proof. (of Claim 4.7) Let ψ' be the state obtained from ψ by measuring all the SMA qubits in S_R. Notice that $\psi'_R = \Psi_R$. Thus, by appealing to data-processing, we have

$$F(\Psi_R, \psi_R) = F(\psi'_R, \psi_R) \geq F(\psi', \psi). \tag{4.34}$$

Next, we lower bound $F(\psi', \psi)$. We can represent $|\psi\rangle$ by

$$|\psi\rangle = \sum_{t \in \{0,1\}^{|S_R|}} \sqrt{P(t)}\, |\psi_t\rangle\, |t\rangle_{S_R}, \quad \psi' = \sum_{t \in \{0,1\}^{|S_R|}} P(t)\, |\psi_t\rangle\!\langle\psi_t| \otimes |t\rangle\!\langle t|_{S_R}, \tag{4.35}$$

where $|\psi_t\rangle$ are normalized states. We have

$$\begin{aligned} F^2(\psi, \psi') &= \sum_{t \in \{0,1\}^{|S_R|}} \sqrt{P(t)} P(t) \sqrt{P(t)} |\langle \psi_t | \psi_t \rangle|^2 & (4.36)\\ &= \sum_{t \in \{0,1\}^{|S_R|}} P(t)^2 & (4.37)\\ &\geq P(t = (0, \ldots, 0))^2. & (4.38) \end{aligned}$$

Using a union bound, we get

$$P(t = (0, \ldots, 0)) \geq 1 - \sum_{i=1}^{|S_R|} P(t_i = 1) = 1 - \sum_{i \in S_R} \epsilon_i, \tag{4.39}$$

where the last equality uses the definition of the energy ϵ_i. Thus,

$$F(\psi, \psi') = P(t = (0, \ldots, 0)) \geq 1 - \sum_{i \in S_R} \epsilon_i. \tag{4.40}$$

This completes the first part of the Claim. For the second part, we consider for every $s \in \{0,1\}^N$:

$$\begin{aligned} (\mu_s \otimes |s\rangle\!\langle s|)_R &= (\mu_s)_{R \setminus S_R} \otimes (|s\rangle\!\langle s|)_{S_R} & (4.41)\\ &= \left(\frac{D_s \phi D_s}{\mathrm{tr}(D_s \phi D_s)} \right)_{R \setminus S_R} \otimes (|s\rangle\!\langle s|)_{S_R} & (4.42)\\ &= \left(\frac{D_s \phi D_s}{\mathrm{tr}(D_s \phi D_s)} \otimes |s\rangle\!\langle s| \right)_R . & (4.43) \end{aligned}$$

The second equality uses Fact 4.4 (Item 2) as $|R \setminus S_R| \leq |R| < d$. This establishes $\Psi_R = \Theta_R$. □

Proof. (of Claim 4.8) Consider

$$(m + N) \mathop{\mathbb{E}}_{j \in [m+N]} \sum_{i \in S_{L_j}} \epsilon_i = \sum_{j \in [m+N]} \sum_{i \in S_{L_j}} \epsilon_i = \sum_i \epsilon_i |\{j : i \in S_{L_j}\}|. \tag{4.44}$$

Let us upper bound $|\{j : i \in S_{L_j}\}|$ for any given i. Suppose $j \in [m + N]$ is such that S_{L_j} contains a particular SMA qubit i. Then i lies in the support of the lightcone of j with respect to $W^\dagger$. This puts a constraint on the set of possible j's: for some $b \in [\mathsf{cc}(W)]$, j must lie in the lightcone of i with respect to the circuit $W^{(b)}$ defined as the last b layers of W. The number of j's which satisfy this, for a given i, is at most $\sum_{b=1}^{\mathsf{cc}(W)} 2^b \leq 2^{2\mathsf{cc}(W)}$. Thus,

$$\sum_{j\in[m+N]} \sum_{i\in S_{L_j}} \epsilon_i \leq 2^{2\mathsf{cc}(W)} \sum_i \epsilon_i = 2^{2\mathsf{cc}(W)} \epsilon N. \tag{4.45}$$

The lower bound follows since $|\{j : i \in S_{L_j}\}| \geq 1$. This completes the proof. □

A Additional techniques for circuit lower bounds

In this appendix, we include other techniques for lower bounds on the circuit depth of error-correcting codes. We developed these techniques along the way, but are not necessary for our main result. However, they offer related, and yet different, techniques for circuit lower bounds and may be of independent interest.

A.1 Robust circuit lower bounds for linear-distance codes

Similar to the proof of the circuit lower bound for all states physically close to the code-space in the case of linear-rate codes, we provide a similar proof in the case of linear-distance codes. The intuition is the same: show that the distance of the $|0\rangle^{\otimes n}$ state from any code-space is dependent on d/n and argue its consequence for the original code. The bounds apply for ancilla-free circuits.

Lemma A.1. *Let C be a $[[n, k, d]]$ code for $k > 0$. Then the ancilla-free circuit complexity of any state σ on n qubits with trace distance δ from C is at least $\Omega(\log\left(\frac{d}{\delta n}\right))$.*

Proof. Let U be a depth t circuit generating the state $U|0\rangle^{\otimes n}$ and suppose it has distance δ from the $[[n, k, d]]$ code C (i. e., $\left\|\rho - |0\rangle\langle 0|^{\otimes n}\right\|_1 \leq \delta$). Then $|0\rangle\langle 0|^{\otimes n}$ has distance δ from the code $U^\dagger C U$ which is a $[[n, k, d/2^t]]$ code. Lemma A.2 shows that $\delta = \Omega\left(\frac{d}{2^t n}\right)$, completing the proof. □

Lemma A.2. *Let $k > 0$ and consider a $[[n, k, d]]$ code. The trace distance between $|0\rangle^{\otimes n}$ and the code-space is at least $\Omega(d/n)$.*

Proof. Assume that the distance between $|0\rangle\langle 0|^{\otimes n}$ and some state ρ of the $[[n, k, d]]$ code is $\delta \in (0, 1)$. Define $\Pi_R = \prod_{i\in R} |0\rangle\langle 0|_i$ for any $R \subset [n]$. Divide $[n]$ into $\frac{2n}{d}$ disjoint sets $\{R_j\}_{j=1,\ldots,\frac{2n}{d}}$, each of size at most $d - 1$. For any ρ' in the code-space, local indistinguishability implies $\forall\, i$,

$$\operatorname{tr}(\Pi_{R_i}\rho') = \operatorname{tr}(\Pi_{R_i}\rho) \geq \operatorname{tr}\left(\Pi_{R_i} |0\rangle\langle 0|^{\otimes n}\right) - \delta = 1 - \delta. \tag{A.1}$$

Using the 'union bound' inequality

$$\mathbb{I} - |0\rangle\langle 0|^{\otimes n} \leq \sum_{i=1}^{\frac{2n}{d}} (\mathbb{I} - \Pi_{R_i}), \tag{A.2}$$

we thus find

$$\operatorname{tr}\big((\mathbb{I} - |0\rangle\langle 0|^{\otimes n})\rho'\big) \leq \sum_{i=1}^{\frac{2n}{d}} \operatorname{tr}((\mathbb{I} - \Pi_{R_i})\rho') \leq \frac{2n\delta}{d}. \tag{A.3}$$

If $\delta \leq \frac{d}{6n}$, this implies that all code-states ρ' have fidelity at least $\frac{2}{3}$ with $|0\rangle\langle 0|^{\otimes n}$. But this leads to a contradiction as one can choose two orthogonal code-states; the dimension of the code being at least 2. This completes the proof. □

A.2 Best distance code lower bounds

Attempts at the CNLTS statement[8] may require circuit lower bound methods that are robust against the removal of a small fraction of code Hamiltonian checks. Unfortunately, circuit lower bounds in terms of distance do not appear to be robust: removing checks from a stabilizer code may significantly reduce the code distance. But, it is plausible that the distance associated with some pairs of logical operators does not decrease. We call this the 'best distance' of the code (formalized below and implicit in [27]) and prove lower bounds in terms of this notion. Our lower bound is inspired by the use of the uncertainty principle from [27], but provides a statement that may be incomparable to theirs.

Fix a stabilizer code and consider a logical Pauli pair $\overline{X}_i, \overline{Z}_i$. We drop the subscript i and write $\overline{X}, \overline{Z}$. Let w be the maximum of two weights, $\left|\overline{X}\right|$ and $\left|\overline{Z}\right|$. Let d' be the weight of the smallest logical operator that anti-commutes with either of $\overline{X}$ or $\overline{Z}$. The best distance of the code is the largest value of d' over all logical pairs. Note that $d' \geq d$. Eldar and Harrow [27, Section 4: Lemma 37] show that for any state $|\psi\rangle$,

$$\langle\psi|\,\overline{X}\,|\psi\rangle^2 + \langle\psi|\,\overline{Z}\,|\psi\rangle^2 \leq 1. \tag{A.4}$$

This is interpreted as an uncertainty principle. Now we show the following.

Lemma A.3. *Consider a product state $|\psi\rangle = \bigotimes_{j=1}^{n} |u_j\rangle$. Then for any code-state $|\rho\rangle$, we have $\frac{1}{2}\|\psi - \rho\|_1 \geq \frac{d'}{8w}$.*

Proof. We assume for contradiction that there is a code-state $|\rho\rangle$ with $\frac{1}{2}\|\psi - \rho\|_1 < \frac{d'}{8w}$. From Equation (A.4), we have one of the following possibilities:

$$\left|\langle\psi|\,\overline{X}\,|\psi\rangle\right| \leq \frac{1}{\sqrt{2}}, \quad \left|\langle\psi|\,\overline{Z}\,|\psi\rangle\right| \leq \frac{1}{\sqrt{2}}. \tag{A.5}$$

[8] A proof of the CNLTS statement was given in [8] and [9].

Without loss of generality, assume the first holds. Define the product state $|\theta\rangle = \overline{X}\,|\psi\rangle$. Thus, $F(\psi,\theta) \leq \frac{1}{\sqrt{2}}$. Let L be the set of qubits supporting $\overline{X}$. Divide L into distinct parts $L_1, L_2, \ldots L_{w/d'}$ such each part has size at most $d'-1$. Since ψ is a product state,

$$F(\psi_{L_1},\theta_{L_1})F(\psi_{L_2},\theta_{L_2})\ldots F(\psi_{L_{w/d'}},\theta_{L_{w/d'}}) = F(\psi,\theta) \leq \frac{1}{\sqrt{2}}. \tag{A.6}$$

Thus, for at least one of L_j (take L_1 without loss of generality), we have

$$F(\psi_{L_1},\theta_{L_1}) \leq \frac{1}{2^{d'/2w}} \implies \frac{1}{2}\|\psi_{L_1} - \theta_{L_1}\|_1 \geq \frac{d'}{4w}. \tag{A.7}$$

On the other hand, the proof assumes $\frac{1}{2}\|\psi - \rho\|_1 < \frac{d'}{8w}$ which implies $\frac{1}{2}\|\theta - \overline{X}\rho\overline{X}\|_1 < \frac{d'}{8w}$. Since ρ is a code-state and L_1 has size at most $d'-1$, first part of the Fact 4.3 (i. e., local indistinguishability) ensures that $\rho_{L_1} = (\overline{X}\rho\overline{X})_{L_1}$ (as noted in its proof, the first part of this fact applies with the distance d replaced by d'). This implies via triangle inequality that $\frac{1}{2}\|\psi_{L_1} - \theta_{L_1}\|_1 < \frac{d'}{4w}$, which is a contradiction. □

Product states have circuit complexity ≤ 1. We extend this argument to the case of low-depth circuits.

Lemma A.4. *Consider a state $|\psi\rangle = U\,|0\rangle^{\otimes m}$ on m qubits, where U has depth t and $t \leq \log \frac{d'}{2}$. Then for any state $\rho_{\mathsf{code}} \in D_s$ for some $s \in \{0,1\}^N$, we have*

$$\frac{1}{2}\|\psi_{\mathsf{code}} - \rho_{\mathsf{code}}\|_1 \geq \frac{1}{2}\left(\frac{d'}{2^{2t+6}w}\right)^2. \tag{A.8}$$

The lemma uses the following well known fact.

Fact A.5. *For any quantum state $|\psi\rangle$ on m qubits and a quantum state ρ_{code} on code qubits, there is a quantum state $|\rho\rangle$ on m qubits such that*

$$\frac{1}{2}\|\psi_{\mathsf{code}} - \rho_{\mathsf{code}}\|_1 \geq \frac{1}{8}\|\psi - \rho\|_1^2. \tag{A.9}$$

Proof. By Uhlmann's theorem [57], there is a quantum state $|\rho\rangle$ purifying ρ_{code} on $m-n$ qubits such that

$$F(\psi_{\mathsf{code}},\rho_{\mathsf{code}}) = F(\psi,\rho). \tag{A.10}$$

Thus,

$$\begin{aligned}
\frac{1}{2}\|\psi_{\mathsf{code}} - \rho_{\mathsf{code}}\|_1 &\geq 1 - \sqrt{F(\psi_{\mathsf{code}},\rho_{\mathsf{code}})} && \text{(A.11)}\\
&= 1 - \sqrt{F(\psi,\rho)} && \text{(A.12)}\\
&\geq 1 - \sqrt{1 - \frac{1}{4}\|\psi - \rho\|_1^2} && \text{(A.13)}\\
&\geq \frac{1}{8}\|\psi - \rho\|_1^2. && \text{(A.14)}
\end{aligned}$$

□

Proof. (of Lemma A.4) We assume for contradiction that there is a $\rho_{\mathsf{code}} \in D_s$ (for some s) such that $\frac{1}{2}\|\psi_{\mathsf{code}} - \rho_{\mathsf{code}}\|_1 < \frac{1}{2}\left(\frac{d'}{2^{2t+6}w}\right)^2$. Fact A.5 ensures that there is a purification $|\rho\rangle$ of ρ_{code} on m qubits such that $\frac{1}{2}\|\psi - \rho\|_1 < \frac{d'}{2^{2t+6}w}$. From Equation (A.4), we have one of the following possibilities:

$$\left|\langle\psi|\,\overline{X}\,|\psi\rangle\right| \leq \frac{1}{\sqrt{2}}, \quad \left|\langle\psi|\,\overline{Z}\,|\psi\rangle\right| \leq \frac{1}{\sqrt{2}}. \tag{A.15}$$

Without loss of generality, assume the first holds. Define the state $|\theta\rangle = \overline{X}\,|\psi\rangle$. Thus, $F(\psi, \theta) \leq \frac{1}{\sqrt{2}}$. We have the following claim, proved later.

Claim A.6. *For every integer $K < w$, there is a set T (a subset of ancillas and code qubits) of size at most $K \cdot 2^t$ such that*

$$\frac{1}{2}\|\psi_T - \theta_T\|_1 \geq \frac{K}{2^{t+4}w}. \tag{A.16}$$

Setting $K = \frac{d'}{2^{t+1}} \geq 1$ (recall $d' \leq w$ and $2^{t+1} \leq d'$), we find a set T of size $|T| \leq d'/2$ such that $\frac{1}{2}\|\psi_T - \theta_T\|_1 \geq \frac{d'}{2^{2t+5}w}$. On the other hand, by assumption $\frac{1}{2}\|\psi - \rho\|_1 < \frac{d'}{2^{2t+6}w}$ which implies $\frac{1}{2}\|\theta - \overline{X}\rho\overline{X}\|_1 < \frac{d'}{2^{2t+6}w}$. Since $\rho_{\mathsf{code}} \in D_s$, first part of the Fact 4.3 ensures that $\rho_T = (\overline{X}\rho\overline{X})_T$. This implies, via triangle inequality, that $\frac{1}{2}\|\psi_T - \theta_T\|_1 < \frac{d'}{2^{2t+5}w}$, which is a contradiction. This completes the proof. □

Proof. (of Claim A.6) The main idea is that low-depth states are uniquely determined by their marginals on 2^t qubits. We are given a state $|\psi\rangle = U\,|0\rangle^{\otimes m}$ and $|\theta\rangle = \overline{X}\,|\psi\rangle$. Consider the Hamiltonian

$$H = \sum_{S \subset [m]} P_S \overset{\mathsf{def}}{=} U\left(\sum_{j=1}^{m} |1\rangle\langle 1|_j\right)U^\dagger \tag{A.17}$$

which is a sum of commuting projectors and each $|S| \leq 2^t$. The unique ground-state is $|\psi\rangle$ and the spectral gap is 1. This is because each local term has eigenvalues 0 adn 1 and they commute. Define $\overline{P}_S = \mathbb{I} - P_S$. Let $\mathcal{U}$ be set of P_S that overlap the support of $\overline{X}$. Number of such P_S is u where $w \leq u \leq 2^t w$. For any $P_S \notin U$ we have $[P_S, \overline{X}] = 0$ which implies $\langle\theta|\,P_S\,|\theta\rangle = \langle\psi|\,P_S\,|\psi\rangle = 0$. Consider the operator

$$W_K \overset{\mathsf{def}}{=} \mathbb{I} + \left(\frac{\sum_{S \in U} P_S}{u} - \mathbb{I}\right)^K, \tag{A.18}$$

where $K < s$ is odd. It holds that[9]

$$\langle\theta|\,W_K\,|\theta\rangle \geq \frac{K}{2u}\,\langle\theta|\,(\mathbb{I} - |\psi\rangle\langle\psi|)\,|\theta\rangle\,. \tag{A.20}$$

[9] To show this, consider $\Pi_U^\perp$ (the excited space of $\sum_{S\in U} P_S$) and $\Pi^\perp = \mathbb{I} - |\psi\rangle\langle\psi|$ (the excited space of H). Since $P_S\,|\theta\rangle = 0$ for all $S \notin U$, we have $\langle\theta|\,\Pi_U^\perp\,|\theta\rangle = \langle\theta|\,\Pi^\perp\,|\theta\rangle$. Next, we show that $W_k \geq \frac{k}{2u}\Pi_U^\perp$. For this, we need to

Since $F(\psi, \theta) \leq \frac{1}{\sqrt{2}}$, we have $\langle\theta| (\mathbb{I} - |\psi\rangle\langle\psi|) |\theta\rangle \geq 1 - \frac{1}{2} = \frac{1}{2}$. Thus,

$$\langle\theta| W |\theta\rangle \geq \frac{K}{2u} \langle\theta| (\mathbb{I} - |\psi\rangle\langle\psi|) |\theta\rangle \geq \frac{K}{4u}. \tag{A.21}$$

On the other hand (using $P_S |\theta\rangle = 0$ for $S \notin \mathcal{U}$),

$$\langle\theta| W |\theta\rangle = 1 + \langle\theta| \left(\frac{\sum_{S\in U} P_S}{u} - \mathbb{I}\right)^K |\theta\rangle \tag{A.22}$$

$$= 1 - \langle\theta| \left(\frac{\sum_{S\in U} \overline{P}_S}{u}\right)^K |\theta\rangle \tag{A.23}$$

$$= \frac{1}{u^K} \sum_{S_1,\ldots S_K \in U} \langle\theta| \left(\mathbb{I} - \overline{P}_{S_1}\overline{P}_{S_2}\ldots\overline{P}_{S_K}\right) |\theta\rangle . \tag{A.24}$$

We conclude that there exist $S_1, S_2, \ldots S_K \in \mathcal{U}$ such that for $S' = S_1 \cup S_2 \cup \ldots \cup S_K$,

$$\operatorname{tr}\left(\left(\mathbb{I} - \overline{P}_{S_1}\overline{P}_{S_2}\ldots\overline{P}_{S_K}\right) \theta_{S'}\right) \geq \frac{K}{4u} \geq \frac{K}{2^{t+4}w}. \tag{A.25}$$

The size of S' is at most $K \cdot 2^t$. Using

$$\operatorname{tr}\left(\left(\mathbb{I} - \overline{P}_{S_1}\overline{P}_{S_2}\ldots\overline{P}_{S_K}\right) \psi_{S'}\right) = 0, \tag{A.26}$$

we get $\frac{1}{2}\|\theta_{S'} - \psi_{S'}\|_1 \geq \frac{K}{2^{t+4}w}$. □

B Proof of improved circuit lower bounds using AGSPs

Proof of Lemma 3.4. If $2^t \geq d$, then the proof is immediate. Thus, assume $2^t < d$. Using Uhlmann's theorem [57], we find that there is a purification $|\rho_0\rangle$ of ρ_0 such that

$$F(|\psi\rangle\langle\psi| , |\rho_0\rangle\langle\rho_0|) = F(\psi_{\mathsf{code}}, \rho_0) = f. \tag{B.1}$$

Since $|\psi\rangle$ has the maximum fidelity (over all code-states) with the projected vector

$$|\rho\rangle \overset{\mathsf{def}}{=} \frac{1}{\sqrt{\langle\psi| \Pi_C |\psi\rangle}} \Pi_C |\psi\rangle , \tag{B.2}$$

argue that $1 + \left(\frac{v}{u} - 1\right)^k \geq \frac{k}{2u}$ for all $v \geq 1$. This is trivial when $v \geq u$. For $1 \leq v < u$, consider

$$(1 - \frac{v}{u})^K \leq (1 - \frac{1}{u})^K \leq \mathrm{e}^{-\frac{K}{u}} \leq 1 - \frac{K}{2u}. \tag{A.19}$$

Here we used $K < w \leq u$.

we conclude $F(|\psi\rangle\langle\psi|, |\rho\rangle\langle\rho|) \geq f$. Defining the rotated vector $|\rho'\rangle = U^\dagger |\rho\rangle$, we further find that $F(|0\rangle\langle 0|^{\otimes m}, \rho') \geq f$.

Since the vector $|\rho'\rangle$ is the projection of $|0\rangle^{\otimes m}$ on the rotated code-space $C' \overset{\text{def}}{=} U^\dagger(\mathbb{I} \otimes C)U$, it is expected to have low entanglement. This is formalized below, adapted from [32, 14, 13] and proven later.

Claim B.1. *For any region $R \subset [m]$, it holds that*

$$S(\rho'_R) \leq 32\left(\sqrt{2^{t+1}\ell|R|\log\frac{1}{f}}\right)\log^2(2^{t+1}\ell|R|). \tag{B.3}$$

Define the state Θ from $|\rho\rangle$ as in Equation (3.2) and let $\Theta' = U^\dagger \Theta U$. It holds that for any region R of size $< d$, $\Theta_R = \rho_R$. Fact 2.5 now implies that for any region R' of size at most $\frac{d}{2^{t+1}}$, $\Theta'_R = \rho'_R$. Thus, dividing $[m]$ into $\frac{2^{t+1}m}{d}$ regions $R_1, R_2, \ldots R_{\frac{2^{t+1}m}{d}}$, each of size at most $\frac{d}{2^{t+1}}$, we find that

$$k \leq S(\Theta') \leq \sum_{j=1}^{\frac{2^{t+1}m}{d}} S(\Theta'_{R_j}) = \sum_{j=1}^{\frac{2^{t+1}m}{d}} S(\rho'_{R_j}) \leq \frac{2^{t+1}m}{d} \cdot \left(8\sqrt{d\ell\log\frac{1}{f}}\right)\log^2 d\ell. \tag{B.4}$$

We used Claim B.1 above. Since $m \leq 2^t n$, we can re-write this as

$$k \leq \frac{2^{2t+6}n\log^2 d\ell}{\sqrt{d}} \cdot \sqrt{\ell\log\frac{1}{f}}. \tag{B.5}$$

Thus, we conclude that

$$2^{2t} \geq \frac{k\sqrt{d}}{64n\log^2 d\ell \cdot \sqrt{\ell\log\frac{1}{f}}}. \tag{B.6}$$

This completes the proof. □

Now, we prove Claim B.1. It is a simple application of the Approximate Ground-State Projector (AGSP) framework based on polynomial approximations to local Hamiltonian [13]. We will use the following well known polynomials that improve upon the Chebyshev approximation to AND function.

Fact B.2 ([37, 22])**.** *Let n be an integer and $h : \{0, 1, \ldots n\} \to \{0, 1\}$ be the function defined as $h(0) = 1$ and $h(j) = 0$ for $j \in [n]$. For every $\sqrt{n} \leq \mathsf{deg} \leq n$, there is a polynomial K_{deg} of degree deg such that for every $j \in \{0, 1, \ldots n\}$, $|h(j) - K_{\mathsf{deg}}(j)| \leq \exp\left(-\frac{\mathsf{deg}^2}{2^8 n}\right)$.*

Proof. *(of Claim B.1)* Let $\Pi'_j \overset{\text{def}}{=} U^\dagger \Pi_j U$ be the rotated commuting checks. Each Π'_j has locality $\leq \ell 2^t$ and each qubit participates in at most $\ell 2^t$ rotated checks. Let R_1 be the extended region defined as the set of all qubits that share a rotated check with a qubit in R. Let $\Pi_c = \times_{j:\mathrm{supp}(\Pi'_j)\notin R_1} \Pi_j$ be the common eigenspace of all the checks not in R_1 and define the "truncated Hamiltonian"

$$H_{\mathsf{trunc}} = \left(\sum_{j:\mathrm{supp}(\Pi'_j)\subset R_1} (\mathbb{I} - \Pi'_j) \right) + (\mathbb{I} - \Pi_c). \tag{B.7}$$

Note that $\Pi_{C'}$ is the ground-space of H_{trunc} and the spectral gap of H_{trunc} is 1. The advantage is that the norm of H_{trunc} is now $\leq 2^t \ell |R| + 1 \leq 2^{t+1}\ell|R|$. For an integer deg to be chosen later, consider the degree deg polynomial of H_{trunc} obtained from Fact B.2: $K_{\mathsf{deg}}(H_{\mathsf{trunc}})$. It satisfies

$$\|K_{\mathsf{deg}}(H_{\mathsf{trunc}}) - \Pi_{C'}\|_\infty \leq \exp\left(-\frac{\mathsf{deg}^2}{2^{t+9}\ell|R|}\right). \tag{B.8}$$

This ensures that the state

$$|\omega\rangle \overset{\text{def}}{=} \frac{K_{\mathsf{deg}}(H_{\mathsf{trunc}})\,|0\rangle^{\otimes m}}{\|K_{\mathsf{deg}}(H_{\mathsf{trunc}})\,|0\rangle^{\otimes m}\|_1} \tag{B.9}$$

satisfies

$$\||\omega\rangle - |\rho'\rangle\|_1 \leq \frac{2}{f}\cdot\exp\left(-\frac{\mathsf{deg}^2}{2^{t+9}\ell|R|}\right). \tag{B.10}$$

Letting $\mathsf{deg} = \sqrt{2^{t+9}\ell|R|\log\frac{2|R|}{f}}$, we conclude that $\|\,|\omega\rangle - |\rho'\rangle\,\|_1 \leq \frac{1}{|R|}$. Claim B.3, below, shows that the Schmidt rank of $K_{\mathsf{deg}}(H_{\mathsf{trunc}})$ across R and $[m]\setminus R$ is at most $(2^{2t+1}\ell^2|R|)^{\mathsf{deg}}$. Thus,

$$S(\omega_R) \leq \mathsf{deg}\cdot\log\left(2^{2t+1}\ell^2|R|\right) \leq 2\mathsf{deg}\cdot\log\left(2^{t+1}\ell|R|\right). \tag{B.11}$$

Using the Alicki-Fannes inequality [7], we thus find that

$$\begin{aligned}
S(\rho'_R) &\leq 2|R|\cdot\frac{1}{|R|} + S(\omega_R) && \text{(B.12)}\\
&\leq 2\mathsf{deg}\cdot\log\left(2^{t+1}\ell|R|\right) + 2 && \text{(B.13)}\\
&\leq 2\left(\sqrt{2^{t+9}\ell|R|\log\frac{2|R|}{f}}\right)\log\left(2^{t+1}\ell|R|\right) + 2 && \text{(B.14)}\\
&\leq 32\left(\sqrt{2^{t+1}\ell|R|\log\frac{1}{f}}\right)\log^2(2^{t+1}\ell|R|). && \text{(B.15)}
\end{aligned}$$

This completes the proof. □

Claim B.3. *Schmidt rank of any degree* deg *polynomial* $K_{\mathsf{deg}}(H_{\mathsf{trunc}})$ *across* R *and* $[m] \setminus R$ *is at most*

$$\mathsf{deg}^3 \cdot (2^{2t}\ell^2|R|)^{\mathsf{deg}} \le (2^{2t+1}\ell^2|R|)^{\mathsf{deg}}. \tag{B.16}$$

Proof. Let us provide an upper bound on the Schmidt rank of $(H_{\mathsf{trunc}})^q$, for any $0 \le q \le \mathsf{deg}$. Let $H_{\mathsf{trunc}} = H_\partial + H_{\mathsf{in}} + H_{\mathsf{out}}$, where H_∂ is the set of all rotated checks supported on both R and $[m] \setminus R$, H_{in} is the set of rotated checks strictly within R and H_{out} is the set of rotated checks (including the truncated part Π_c) within $[m] \setminus R$. Note that all these terms commute and the number of H_∂ is at most $2^t\ell|R|$ (since each qubit in R participates in at most $2^t\ell$ rotated checks). Then $(H_{\mathsf{trunc}})^q = \sum_{a+b+c=q} H_{\mathsf{in}}^a H_{\mathsf{out}}^b H_\partial^c$. The operators H_{in}^a and H_{out}^b do not increase the Schmidt rank across R and $[m] \setminus R$. The Schmidt rank of H_∂ is $\le 2^t\ell|R| \cdot 2^t\ell = 2^{2t}\ell^2|R|$, since each of the $2^t\ell|R|$ rotated checks has Schmidt rank $2^t\ell$. Thus, $(H_{\mathsf{trunc}})^q$ has Schmidt rank

$$\le q^2 \cdot (2^{2t}\ell^2|R|)^q \le \mathsf{deg}^2 \cdot (2^{2t}\ell^2|R|)^{\mathsf{deg}}. \tag{B.17}$$

Finally, $K_{\mathsf{deg}}(H_{\mathsf{trunc}})$ has Schmidt rank at most deg times this number. This completes the proof. □

C Amplification of circuit lower bounds

In the previous sections, we considered local Hamiltonians H which were the sum $\sum_{i=1}^N H_i$ of local terms H_i of norm ≤ 1. In this framework, we were interested in the circuit complexity of states of energy $\le \epsilon N$. In this section, we will shift to an equivalent framework and let $H = \mathbb{E}_i H_i$ and consider states of energy $\le \epsilon$. This is because we will be considering Hamiltonians of super-constant locality and it is notationally simpler to consider normalized Hamiltonians. We define the locality of a Hamiltonian as follows.

Definition C.1. We say a local Hamiltonian is (ℓ, D)-local if each Hamiltonian term acts non-trivially on at most ℓ qubits and each qubit is acted on non-trivially by at most D Hamiltonian terms. We will also refer to a Hamiltonian as simply ℓ-local if it is (ℓ, ℓ)-local.

The main result of this section is a simple transformation one can apply to a local Hamiltonian instance to improve circuit depth lower bounds at the cost of worsening the locality of the Hamiltonian. The principal idea is to transform the Hamiltonian H into a Hamiltonian H' such that for any low-depth state ϕ,

$$\operatorname{tr}(H'\phi) \ge p \cdot \operatorname{tr}(H\phi) \tag{C.1}$$

for some choice of $p > 1$. If we can construct such an energy amplification, then any depth lower bound we had for *very* low-energy states of H can be translated to a depth lower bound for low-energy states of H. For example, in the case of the lower bounds proven in the prior section which scale roughly as $\log(1/\epsilon)$ for states of energy $\le \epsilon$, applying such a transformation would give us a lower bound of $\log(p/\epsilon)$ for states of energy $\le \epsilon$. The following theorem shows how to achieve this result for low depth states at a cost of increasing the locality of the Hamiltonian by a factor of p.

Theorem C.2. *Let H be a ℓ-local Hamiltonian on n qubits such that $H \geq 0$. Define the Hamiltonian $H^{(p)}$ as*

$$H^{(p)} \overset{\mathsf{def}}{=} \mathbb{I} - (\mathbb{I} - H)^p \,. \tag{C.2}$$

Then for any mixed state ϕ of $\mathsf{cc}(\phi) \leq t$, we have

$$\operatorname{tr}\left(H^{(p)}\phi\right) \geq \frac{1}{2}\min\left\{1, p\operatorname{tr}(H\phi)\right\} - \frac{2^t p^2 \ell^2}{n}. \tag{C.3}$$

We prove this theorem at the end of the section. We now apply this theorem to our previous lower bounds to generate a super-constant locality Hamiltonian with super-constant circuit lower bounds for all states of energy $\leq 1/100$ with respect to the new Hamiltonian. The following is a reformulation of Theorem 1.1 (Theorem 4.6) applied to stabilizer codes of linear rate and polynomial distance such as the Tillich-Zémor code [55].

Corollary C.3. *For fixed constants $\ell > 2, c > 0$, there exists a family of ℓ-local Hamiltonians H on n qubits such that for any state ϕ of energy $\operatorname{tr}(H\phi) \leq \epsilon$, the circuit complexity of ϕ is at least*

$$\mathsf{cc}(\phi) \geq c \cdot \min\left\{\log n, \log\frac{1}{\epsilon}\right\}. \tag{C.4}$$

To apply Theorem C.2, let us consider a state ϕ of circuit complexity $\mathsf{cc}(\phi) \leq t < \frac{1}{3}\log n - \log 100\ell^3$ (otherwise, the lower bound is trivial) and an amplification factor of $p \leq n^{1/3}$. Let us also assume that $\operatorname{tr}\left(H^{(p)}\phi\right) \leq \frac{1}{100}$. If $\operatorname{tr}(H\phi) \geq \ell/p$, then we reach a contradiction as

$$\frac{1}{100} \geq \operatorname{tr}\left(H^{(p)}\phi\right) \geq \frac{\ell}{2} - \frac{p^2 n^{1/3}}{100n} \geq \frac{\ell}{2} - \frac{1}{100} \geq 1 - \frac{1}{100}. \tag{C.5}$$

Therefore, we may assume $\operatorname{tr}(H\phi) < \ell/p$. Then,

$$\frac{1}{100} \geq \frac{p}{2}\operatorname{tr}(H\phi) - \frac{p^2 n^{1/3}}{100n} \geq \frac{p}{2}\operatorname{tr}(H\phi) - \frac{1}{100}, \tag{C.6}$$

or equivalently,

$$\operatorname{tr}(H\phi) \leq \frac{1}{25p}. \tag{C.7}$$

Therefore, the circuit complexity of ϕ is at least

$$\mathsf{cc}(\phi) \geq c \cdot \min\left\{\log n, \log\frac{p}{25}\right\}, \tag{C.8}$$

thus proving a circuit lower bound for all states of energy $\leq 1/100$ with respect to $H^{(p)}$. The locality of the Hamiltonian $H^{(p)}$ can be calculated as follows: Each term of $H^{(p)}$ is a product of p terms of H and therefore acts on $p\ell$ qubits. Likewise, each qubit of $H^{(p)}$ is acted on by $\leq p\ell^{p+1}n^{p-1} \overset{\text{def}}{=} D$ terms since there are $\leq (\ell n)^p$ Hamiltonian terms in $H^{(p)}$.

Assuming we are content with each Hamiltonian term acting on $p\ell$ qubits, we can apply the operator Chernoff bound to sparsify the Hamiltonian such that each qubit does not act in too many terms. To sparsify the Hamiltonian $H^{(p)}$, we select a uniformly random subset of k terms from the Hamiltonian $H^{(p)}$ and consider the Hamiltonian H' defined as the expectation over these k terms. The following lemma demonstrates that with high probability over this sparsification procedure, the spectra of $H^{(p)}$ and H' are close.

Lemma C.4. *Fix $\delta > 0$ and consider a normalized Hamiltonian (ℓ, D)-local Hamiltonian G on n qubits. For a choice of*

$$k = n \cdot \max\left\{\frac{32}{\delta^2}, \frac{\log n}{\ell}\right\} \tag{C.9}$$

the sparsified Hamiltonian G' constructed by choosing k random terms of G satisfies the following: With probability $\geq \frac{1}{3}$ over the sparsification,

$$\|G - G'\| \leq \delta \tag{C.10}$$

and each term of G' participates in at most $O(\ell/\delta^2)$ Hamiltonian terms.

The proof of this lemma is given at the end of this section. Directly applying the lemma on $H^{(p)}$ for $\log n < p < n^{1/3}$ using $\delta = 1/200$, we get that there exists a local Hamiltonian H' consisting of $\Theta(n)$ local terms with each term of H' participates in $O(p)$ Hamiltonian terms. Furthermore, H' is $1/200$-close to $H^{(p)}$ in spectral norm, so any state of energy $\leq 1/200$ with respect to H' has energy $\leq 1/100$ with respect to $H^{(p)}$ and the previously proven circuit lower bound applies. Restated, we achieve the following.

Theorem C.5 (Super-constant locality NLTS)**.** *For $p(n)$ a function such that $\log n < p(n) < n^{1/3}$, there exists a $O(p(n))$-local family of local Hamiltonians acting on n qubits and consisting of $N = \Theta(n)$ local terms such that every state ϕ of energy $\leq N/200$ has a circuit complexity lower bound of*

$$\mathsf{cc}(\phi) \geq \Omega(\log p(n)). \tag{C.11}$$

C.1 Developing locality reduction

By itself, Theorem C.5, is not a surprising result since the lower bound we get is the logarithm of the locality of the Hamiltonian. Consider the Hamiltonian

$$H = \frac{p}{n}\left(\Pi_1 + \Pi_2 + \ldots + \Pi_{n/p}\right) \tag{C.12}$$

where each Π_i is the projector onto the state $|\mathsf{cat}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes p} + |1\rangle^{\otimes p})$ for a disjoint set of p qubits. [50] show how to prove a circuit lower bound of $\Omega(\log p)$ for all states of energy $\leq 1/200$ with respect to Π_i. Using a simple Markov inequality, one can extend it to a circuit lower bound for the low-energy states of H from Equation (C.12). Furthermore, a small variation of this Hamiltonian can be constructed with $\Theta(n)$ local terms.

What Theorem C.5 provides, however, is a technique for amplifying the circuit complexity of a Hamiltonian at the cost of increasing locality. Consider then a hypothetical locality reducing transformation which takes as input a Hamiltonian H and outputs a ℓ-local Hamiltonian H', for a fixed constant ℓ, such that for any low-depth state ϕ, $\mathrm{tr}(H'\phi) \geq c \cdot \mathrm{tr}(H\phi)$ for some fixed constant $c > 0$. Then one could sequentially apply amplification and locality reduction transformations until an NLTS Hamiltonian was constructed. This is analogous to Dinur's construction of the PCP theorem [25].

Unfortunately, the locality reduction step of Dinur's proof relies heavily on copying information, a luxury unavailable in the quantum setting. In fact, it is unclear if we should even believe that a locality reduction transformation exists. For one, a Hamiltonian term testing a global property cannot be replicated by any family of local Hamiltonians. For example, the $|\mathsf{cat}\rangle$ state is not the ground-state of any local Hamiltonian and therefore the projector $|\mathsf{cat}\rangle\langle\mathsf{cat}|$ cannot be approximated by local terms[10].

C.2 Omitted Proofs

Proof. (of Theorem C.2) Let $H = \mathbb{E}_i\, h_i$ being the decomposition into local terms, $g_i = \mathbb{I} - h_i$, and $G = \mathbb{E}_i\, g_i$ so $G = \mathbb{I} - H$ and $H^{(p)} = \mathbb{I} - G^p$. Let ϕ be a state of depth $\mathsf{cc}(\phi) \leq t$. Then, we can express the energy of ϕ with respect to H_p as

$$\mathrm{tr}\left(H^{(p)}\phi\right) = 1 - \mathrm{tr}\left(G^p\phi\right) \tag{C.13}$$

$$= 1 - \left(1 - \mathrm{tr}(H\phi)\right)^p - \left[\mathrm{tr}(G\phi)^p - \mathrm{tr}(G^p\phi)\right]. \tag{C.14}$$

To bound this difference of terms, we will use the property that ϕ has a low-depth circuit. We can write

$$\mathrm{tr}(G\phi)^p - \mathrm{tr}(G^p\phi) = \mathop{\mathbb{E}}_{i_1,\ldots,i_t}\left(\mathrm{tr}(g_{i_1}\ldots g_{i_t}\phi) - \mathrm{tr}(g_{i_1}\phi)\ldots\mathrm{tr}(g_{i_t}\phi)\right) \tag{C.15}$$

$$\leq \Pr_{i_1,\ldots,i_t}\left(\mathrm{tr}(g_{i_1}\ldots g_{i_t}\phi) \neq \mathrm{tr}(g_{i_1}\phi)\ldots\mathrm{tr}(g_{i_t}\phi)\right) \tag{C.16}$$

since each Hamiltonian term g_i is normalized. We claim that the only sequences $(i_1, \ldots, i_t)$ for which $\mathrm{tr}(g_{i_1}\ldots g_{i_t}\phi)$ may not equal $\mathrm{tr}(g_{i_1}\phi)\ldots\mathrm{tr}(\phi g_{i_t})$ are those for which g_{i_k} falls in the light cone of a previous $g_{i_1}, \ldots, g_{i_{k-1}}$. This is because the value of an observable only depends on the

[10] However, a state near the $|\mathsf{cat}\rangle$ state is the unique ground-state of a local Hamiltonian as shown by Nirkhe, Vazirani and Yuen [50] .

reduced state in its light cone. Assume $g_{i_1}, \dots, g_{i_t}$ have disjoint light cones $L_1, \dots, L_t$. Then

$$\begin{aligned}\operatorname{tr}(g_{i_1} \dots g_{i_t} \phi) &= \operatorname{tr}\left(g_{i_1} \dots g_{i_t} \phi_{L_1 \cup \dots \cup L_t}\right) && \text{(C.17)}\\ &= \operatorname{tr}\left(g_{i_1} \dots g_{i_t} \phi_{L_1} \otimes \dots \otimes \phi_{L_t}\right) && \text{(C.18)}\\ &= \operatorname{tr}(g_{i_1}\phi_{L_1}) \dots \operatorname{tr}(g_{i_t}\phi_{L_t}) && \text{(C.19)}\\ &= \operatorname{tr}(g_{i_1}\phi) \dots \operatorname{tr}(g_{i_t}\phi). && \text{(C.20)}\end{aligned}$$

Therefore, we can upper bound the probability of this event by the probability that g_{i_k} does not fall in the light cone of any previous $g_{i_1}, \dots, g_{i_{k-1}}$ for all k. We use the fact each light cone has size at most $\ell 2^t$ and that g_{i_k} has size ℓ and apply a union bound:

$$\left(1 - \frac{2^d \ell^2}{n}\right) \cdot \left(1 - 2\frac{2^d \ell^2}{n}\right) \cdot \dots \left(1 - (t-1)\frac{2^d \ell^2}{n}\right) \geq 1 - \frac{2^d t^2 \ell^2}{n}. \tag{C.21}$$

Lastly, we combine this bound with trivial bound for $1 - (1-x)^p$ of $\min\{1, px\}/2$ to achieve

$$\operatorname{tr}\left(H^{(p)}\phi\right) \geq \frac{\min\{1, p \operatorname{tr}(H\phi)\}}{2} - \frac{2^d t^2 \ell^2}{n}. \tag{C.22}$$

□

Proof. (of Lemma C.4) Let G be a (ℓ, D)-local Hamiltonian where $G = \frac{1}{m}\sum_{i=1}^m g_i$. Pick $i_1, \dots, i_k$ uniformly randomly from $[m]$ and let $G' = \frac{1}{k}\sum_{j=1}^k g_{i_j}$. Let X be the operator-valued random variable which takes on the value g_i with probability $\frac{1}{m}$. Then G' is generated by k samples from X. Applying the operator Chernoff bound [56, Lemma 2.8],

$$\Pr\left[\|H' - H\| \geq \epsilon\right] \leq 2^n \mathrm{e}^{-k\delta^2/32} \leq \frac{1}{3} \tag{C.23}$$

using that $k \geq 32n/\delta^2$. Letting Y_a be the random variable that equals 1 if the random term chosen by X acts non-trivially on the qubit a and 0 otherwise. Then $\mathbb{E}\, Y_a = \frac{D}{m} = \Theta(\frac{\ell}{n})$. Then for k independent draws of Y_a: $\{Y_a^1, \dots, Y_a^k\}$, the standard Chernoff bound states that

$$\Pr\left[Y_a^1 + \dots + Y_a^k \geq \Theta\left(\frac{k\ell}{n}\right)\right] \leq \mathrm{e}^{-\Theta(k\ell/n)}. \tag{C.24}$$

Applying a union bound gives the probability that any qubit a is acted on by more than $\Theta(k\ell/n)$ terms is at most $n\mathrm{e}^{-\Theta(k\ell/n)}$. Since $k \geq (n \log n)/\ell$, this is at most $1/3$. □

Acknowledgments

We thank Lior Eldar, Zeph Landau, Umesh Vazirani, and many anonymous reviewers for detailed comments on the manuscript that greatly improved the presentation. Additional thanks to Dorit Aharanov, Matt Hastings, Aleksander Kubica, Rishabh Pipada, Elizabeth Yang, and Henry Yuen for helpful discussions.

References

[1] SCOTT AARONSON AND DANIEL GOTTESMAN: Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70(5):052328, 2004. [doi:10.1103/PhysRevA.70.052328] 6

[2] DORIT AHARONOV, ITAI ARAD, ZEPH LANDAU, AND UMESH VAZIRANI: The detectability lemma and quantum gap amplification. In *Proc. 41st STOC*, pp. 417–426. ACM Press, 2009. [doi:10.1145/1536414.1536472] 2, 7

[3] DORIT AHARONOV, ITAI ARAD, AND THOMAS VIDICK: Guest column: The quantum PCP conjecture. *SIGACT News*, 44(2):47–79, 2013. [doi:10.1145/2491533.2491549] 5, 13

[4] DORIT AHARONOV AND LIOR ELDAR: The commuting local Hamiltonian problem on locally expanding graphs is approximable in NP. *Quantum Info. Processing*, 14(1):83–101, 2015. [doi:10.1007/s11128-014-0877-9] 2

[5] DORIT AHARONOV AND LIOR ELDAR: Quantum locally testable codes. *SIAM J. Comput.*, 44(5):1230–1262, 2015. [doi:10.1137/140975498] 5

[6] DORIT AHARONOV AND TOMER NAVEH: Quantum NP – A survey, 2002. [arXiv:quant-ph/0210077] 13

[7] ROBERT ALICKI AND MARK FANNES: Continuity of quantum conditional information. *J. Phys. A: Math. Gen.*, 37(5):L55, 2004. [doi:10.1088/0305-4470/37/5/L01] 31

[8] ANURAG ANSHU AND NIKOLAS P. BREUCKMANN: A construction of combinatorial NLTS. *J. Math. Phys.*, 63(122201):1–12, 2022. [doi:10.1063/5.0113731, arXiv:2206.02741] 2, 26

[9] ANURAG ANSHU, NIKOLAS P. BREUCKMANN, AND CHINMAY NIRKHE: NLTS Hamiltonians from good quantum codes. In *Proc. 55th STOC*, pp. 1090–1096. ACM Press, 2023. [doi:10.1145/3564246.3585114, arXiv:2206.13228] 2, 5, 13, 26

[10] ANURAG ANSHU, ARAM W. HARROW, AND MEHDI SOLEIMANIFAR: Entanglement spread area law in gapped ground states. *Nature Physics*, 18(11):1362–1366, 2022. [doi:10.1038/s41567-022-01740-7, arXiv:2004.15009] 17

[11] ANURAG ANSHU AND CHINMAY NIRKHE: Circuit lower bounds for low-energy states of quantum code Hamiltonians. In *Proc. 13th Innovations in Theoret. Comp. Sci. Conf. (ITCS'22)*, pp. 6:1–22. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2022. [doi:10.4230/LIPIcs.ITCS.2022.6] 1, 2

[12] BRUNO APOLLONI, MARIA C. CARVALHO, AND DIEGO DE FALCO: Quantum stochastic optimization. *Stoch. Proc. Appl.*, 33(2):233–244, 1989. [doi:10.1016/0304-4149(89)90040-9] 6

[13] ITAI ARAD, ALEXEI YURIEVICH KITAEV, ZEPH LANDAU, AND UMESH VAZIRANI: An area law and sub-exponential algorithm for 1D systems, 2013. [arXiv:1301.1162] 17, 30

[14] ITAI ARAD, ZEPH LANDAU, AND UMESH VAZIRANI: Improved one-dimensional area law for frustration-free systems. *Phys. Rev. B*, 85(19):195145, 2012. [doi:10.1103/PhysRevB.85.195145] 17, 30

[15] JOHANNES BAUSCH AND ELIZABETH CROSSON: Analysis and limitations of modified circuit-to-Hamiltonian constructions. *Quantum*, 2(94):1–36, 2018. [doi:10.22331/q-2018-09-19-94] 6

[16] CHRIS BECK, RUSSELL IMPAGLIAZZO, AND SHACHAR LOVETT: Large deviation bounds for decision trees and sampling lower bounds for AC0-circuits. In *Proc. 53rd FOCS*, pp. 101–110. IEEE Comp. Soc., 2012. [doi:10.1109/FOCS.2012.82] 17

[17] FERNANDO G. S. L. BRANDAÕ AND ARAM W. HARROW: Product-state approximations to quantum states. *Comm. Math. Phys.*, 342:47–80, 2016. Preliminary version in STOC'13. [doi:10.1007/s00220-016-2575-1] 2

[18] SERGEY BRAVYI, ALEXANDER KLIESCH, ROBERT KOENIG, AND EUGENE TANG: Obstacles to variational quantum optimization from symmetry protection. *Phys. Rev. Lett.*, 125(26):260505, 2020. [doi:10.1103/PhysRevLett.125.260505, arXiv:1910.08980] 7

[19] SERGEY BRAVYI, DAVID POULIN, AND BARBARA TERHAL: Tradeoffs for reliable quantum information storage in 2D systems. *Phys. Rev. Lett.*, 104(5):050503, 2010. [doi:10.1103/PhysRevLett.104.050503] 3, 4

[20] SERGEY BRAVYI AND MIKHAIL VYALYI: Commutative version of the local Hamiltonian problem and common eigenspace problem. *Quantum Inf. Comput.*, 5(3):187–215, 2005. ACM DL. 2

[21] NIKOLAS P. BREUCKMANN AND JENS N. EBERHARDT: Balanced product quantum codes. *IEEE Trans. Inform. Theory*, 67(10):6653–6674, 2021. [doi:10.1109/TIT.2021.3097347, arXiv:2012.09271] 3

[22] HARRY BUHRMAN, RICHARD CLEVE, RONALD DE WOLF, AND CHRISTOF ZALKA: Bounds for small-error and zero-error quantum algorithms. In *Proc. 40th FOCS*, pp. 358–368. IEEE Comp. Soc., 1999. [doi:10.1109/SFFCS.1999.814607, arXiv:cs/9904019] 30

[23] LIBOR CAHA, ZEPH LANDAU, AND DANIEL NAGAJ: Clocks in Feynman's computer and Kitaev's local Hamiltonian: Bias, gaps, idling, and pulse tuning. *Phys. Rev. A*, 97(6):062306, 2018. [doi:10.1103/PhysRevA.97.062306] 6

[24] YUDONG CAO, JONATHAN ROMERO, JONATHAN P. OLSON, MATTHIAS DEGROOTE, PETER D. JOHNSON, MÁRIA KIEFEROVÁ, IAN D. KIVLICHAN, TIM MENKE, BORJA PEROPADRE, NICOLAS P. D. SAWAYA, SUKIN SIM, LIBOR VEIS, AND ALÁN ASPURU-GUZIK: Quantum chemistry in the age of quantum computing. *Chemical Reviews*, 119(19):10856–10915, 2019. [doi:10.1021/acs.chemrev.8b00803] 6

[25] IRIT DINUR: The PCP Theorem by gap amplification. *J. ACM*, 54(3):12–55, 2007. [doi:10.1145/1236457.1236459] 7, 35

[26] LIOR ELDAR: Robust quantum entanglement at (nearly) room temperature. In *Proc. 12th Innovations in Theoret. Comp. Sci. Conf. (ITCS'21)*, pp. 49:1–20. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2021. [doi:10.4230/LIPIcs.ITCS.2021.49, arXiv:1911.04461] 2, 4, 7

[27] LIOR ELDAR AND ARAM W. HARROW: Local Hamiltonians whose ground states are hard to approximate. In *Proc. 58th FOCS*, pp. 427–438. IEEE Comp. Soc., 2017. [doi:10.1109/FOCS.2017.46] 2, 4, 5, 6, 7, 8, 17, 26

[28] EDWARD FARHI, JEFFREY GOLDSTONE, AND SAM GUTMANN: A quantum approximate optimization algorithm, 2014. [arXiv:1411.4028] 6

[29] AUSTIN G. FOWLER, MATTEO MARIANTONI, JOHN M. MARTINIS, AND ANDREW N. CLELAND: Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86(3):032324, 2012. [doi:10.1103/PhysRevA.86.032324] 3

[30] MICHAEL H. FREEDMAN AND MATTHEW B. HASTINGS: Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *Quantum Inf. Comput.*, 14(1–2):144–180, 2014. ACM DL. [arXiv:1301.1363] 2, 5, 7, 13

[31] LARRY GUTH AND ALEXANDER LUBOTZKY: Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds. *J. Math. Phys.*, 55(8):082202, 2014. [doi:10.1063/1.4891487] 3

[32] MATTHEW B. HASTINGS: An area law for one-dimensional quantum systems. *J. Stat. Mech.: Theory and Experiment*, 2007(08):P08024, 2007. [doi:10.1088/1742-5468/2007/08/P08024] 17, 30

[33] MATTHEW B. HASTINGS: Topological order at nonzero temperature. *Phys. Rev. Lett.*, 107(21):210501, 2011. [doi:10.1103/PhysRevLett.107.210501] 3

[34] MATTHEW B. HASTINGS: Quantum codes from high-dimensional manifolds. In *Proc. 8th Innovations in Theoret. Comp. Sci. Conf. (ITCS'17)*, volume 67, pp. 25:1–26. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017. [doi:10.4230/LIPIcs.ITCS.2017.25] 5

[35] MATTHEW B. HASTINGS, JEONGWAN HAAH, AND RYAN O'DONNELL: Fiber bundle codes: Breaking the $N^{1/2}\mathrm{polylog}(N)$ barrier for quantum LDPC codes. In *Proc. 53rd STOC*, pp. 1276–1288. ACM Press, 2021. [doi:10.1145/3406325.3451005, arXiv:2009.03921] 3, 6

[36] TADASHI KADOWAKI AND HIDETOSHI NISHIMORI: Quantum annealing in the transverse ising model. *Phys. Rev. E*, 58(5):5355–5363, 1998. [doi:10.1103/PhysRevE.58.5355] 6

[37] JEFF KAHN, NATHAN LINIAL, AND ALEX SAMORODNITSKY: Inclusion-exclusion: Exact and approximate. *Combinatorica*, 16(4):465–477, 1996. [doi:10.1007/BF01271266] 30

[38] JULIA KEMPE, ALEXEI YURIEVICH KITAEV, AND ODED REGEV: The complexity of the local Hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, 2006. [doi:10.1137/S0097539704445226] 6

[39] ALEXEI YURIEVICH KITAEV: Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003. [doi:10.1016/S0003-4916(02)00018-0] 3

[40] ALEXEI YURIEVICH KITAEV AND JOHN PRESKILL: Topological entanglement entropy. *Phys. Rev. Lett.*, 96(11):110404, 2006. [doi:10.1103/PhysRevLett.96.110404] 6

[41] ALEXEI YURIEVICH KITAEV, ALEXANDER H. SHEN, AND MIKHAIL N. VYALYI: *Classical and Quantum Computation*. Amer. Math. Soc., 2002. ACM DL. 6

[42] EMANUEL KNILL AND RAYMOND LAFLAMME: Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, 1997. [doi:10.1103/PhysRevA.55.900] 10

[43] RYAN LAROSE, ARKIN TIKKU, ÉTUDE O'NEEL-JUDY, LUKASZ CINCIO, AND PATRICK J. COLES: Variational quantum state diagonalization. *npj Quantum Information*, 5(1):57, 2019. [doi:10.1038/s41534-019-0167-6] 6

[44] ANTHONY LEVERRIER, VIVIEN LONDE, AND GILLES ZÉMOR: Towards local testability for quantum coding. *Quantum*, 6(661):1–43, 2022. [doi:10.22331/q-2022-02-24-661, arXiv:1911.03069] 5

[45] VIVIEN LONDE AND ANTHONY LEVERRIER: Golden codes: Quantum LDPC codes built from regular tessellations of hyperbolic 4-manifolds. *Quantum Inf. Comput.*, 19(5 & 6):361–391, 2019. [doi:10.26421/QIC19.5-6] 3

[46] SHACHAR LOVETT AND EMANUELE VIOLA: Bounded-depth circuits cannot sample good codes. *Comput. Complexity*, 21(2):245–266, 2012. [doi:10.1007/s00037-012-0039-3, ECCC:TR10-115] 3, 17

[47] ANAND NATARAJAN AND THOMAS VIDICK: Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *Proc. 59th FOCS*, pp. 731–742. IEEE Comp. Soc., 2018. [doi:10.1109/FOCS.2018.00075] 2

[48] MICHAEL A. NIELSEN AND ISAAC L. CHUANG: *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge Univ. Press, 2010. [doi:10.1017/CBO9780511976667] 9, 10

[49] CHINMAY NIRKHE: *Lower bounds on the complexity of quantum proofs*. Ph. D. thesis, EECS Dept., UC Berkeley, 2022. Available as Tech Report UCB/EECS-2022-236. 4

[50] CHINMAY NIRKHE, UMESH VAZIRANI, AND HENRY YUEN: Approximate low-weight check codes and circuit lower bounds for noisy ground states. In *Proc. 45th Internat. Colloq. on Automata, Languages, and Programming (ICALP'18)*, volume 107, pp. 91:1–11. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018. [doi:10.4230/LIPIcs.ICALP.2018.91] 2, 4, 5, 7, 14, 35

[51] PAVEL PANTELEEV AND GLEB KALACHEV: Quantum LDPC codes with almost linear minimum distance. *IEEE Trans. Inform. Theory*, 68(1):213–229, 2021. [doi:10.1109/tit.2021.3119384, arXiv:2012.04068] 3, 6

[52] ALBERTO PERUZZO, JARROD MCCLEAN, PETER SHADBOLT, MAN-HONG YUNG, XIAO-QI ZHOU, PETER J. LOVE, ALÁN ASPURU-GUZIK, AND JEREMY L. O'BRIEN: A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5(4213):1–7, 2014. [doi:10.1038/ncomms5213] 6

[53] ROBERT RAUSSENDORF AND HANS J. BRIEGEL: A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, 2001. [doi:10.1103/PhysRevLett.86.5188] 6

[54] ROBERT RAUSSENDORF, DANIEL E. BROWNE, AND HANS J. BRIEGEL: Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68(2):022312, 2003. [doi:10.1103/PhysRevA.68.022312] 6

[55] JEAN-PIERRE TILLICH AND GILLES ZÉMOR: Quantum LDPC codes with positive rate and minimum distance proportional to the square root of blocklength. *IEEE Trans. Inform. Theory*, 60(2):1193–1202, 2014. Preliminary version in Internat. Symp. Info. Thy (ISIT'09). [doi:10.1109/TIT.2013.2292061] 3, 5, 33

[56] JOEL A. TROPP: User-friendly tail bounds for sums of random matrices. *Found. Computational Math.*, 12(4):389–434, 2012. [doi:10.1007/s10208-011-9099-z] 36

[57] ARMIN UHLMANN: The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9(2):273–279, 1976. [doi:10.1016/0034-4877(76)90060-4] 14, 27, 29

[58] STEVEN R. WHITE: Density matrix formulation for quantum renormalization groups. *Phys. Rev. Lett.*, 69(19):2863–2866, 1992. [doi:10.1103/PhysRevLett.69.2863] 6

AUTHORS

Anurag Anshu
Assistant Professor of Computer Science
School of Engineering and Applied Sciences
Harvard University
Cambridge, Massachusetts, USA
anuraganshu@seas.harvard.edu
https://anuraganshu.seas.harvard.edu/

Chinmay Nirkhe
Assistant Professor of Computer Science
Paul G. Allen School of Computer Science & Engineering
University of Washington
Seattle, Washington, USA
nirkhe@cs.washington.edu
https://homes.cs.washington.edu/~nirkhe

ABOUT THE AUTHORS

ANURAG ANSHU is currently an assistant professor at the School of Engineering and Applied Sciences, Harvard University. Previously, he was a postdoctoral researcher at UC Berkeley and the Simons Institute for the Theory of Computing. This work was completed and initially published while he was at UC Berkeley. Before that, he was a joint postdoctoral researcher at the Institute for Quantum Computing (IQC) and the Perimeter Institute for Theoretical Physics. He completed his Ph. D. at the Centre for Quantum Technologies, National University of Singapore, advised by Rahul Jain. He enjoys thinking about quantum complexity theory, quantum many-body systems, quantum Shannon theory and quantum learning theory.

CHINMAY NIRKHE is currently an assistant professor at the Paul G. Allen School of Computer Science & Engineering at the University of Washington. Previously, he was a research staff member at IBM Quantum. Prior to that appointment, he completed his Ph. D. at UC Berkeley, advised by Umesh Vazirani. This work was completed and initially published while he was at UC Berkeley. His research interests lie at the intersection of quantum information theory and complexity theory.