

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

Anurag Anshu   

Simons Institute for the Theory of Computing, Berkeley, California, USA

Challenge Institute for Quantum Computation, University of California, Berkeley, CA, USA

Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA

Chinmay Nirkhe   

Challenge Institute for Quantum Computation, University of California, Berkeley, CA, USA

Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA

Abstract

The No Low-energy Trivial States (NLTS) conjecture of Freedman and Hastings [27] – 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 work, 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 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.

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases quantum pcps, local hamiltonians, error-correcting codes

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.6

Related Version *Full Version:* <https://arxiv.org/abs/2011.02044>

Funding *Anurag Anshu:* was 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*.

Chinmay Nirkhe: was 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*. He also acknowledges support from an IBM Quantum PhD Internship.

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

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



© Anurag Anshu and Chinmay Nirkhe;

licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 6; pp. 6:1–6:22

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

spectrum is embodied in the quantum PCP conjecture, which is arguably the most important open question 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, 27, 23, 45, 44, 24] and against [17, 14, 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) conjecture* [27]. The NLTS conjecture posits that there exists a fixed constant $\varepsilon > 0$ and a family of n qubit local Hamiltonians such that every state of energy $\leq \varepsilon n$ requires a quantum circuit of super-constant depth to generate. The NLTS conjecture is a necessary consequence of the quantum PCP conjecture because QMA-complete problems likely do not have NP solutions and a constant-depth quantum circuit generating a low-energy state would serve as a NP witness. Thus, this conjecture addresses the inapproximability of local Hamiltonians by classical means. Proving the NLTS conjecture remains a fundamental obstacle to the resolution of the quantum PCP conjecture.

In this work, we show that for local Hamiltonians corresponding to LDPC stabilizer quantum error-correcting codes of linear rate and polynomial distance, every state of energy $\leq \varepsilon n$ requires a quantum circuit of depth $\Omega(\log 1/\varepsilon)$ to generate. We also show similar results for linear distance LDPC codes. Thus, any reasonable improvement to our result would resolve the NLTS conjecture.

1.1 Our results

We restrict our attention to quantum error-correcting codes and the low-energy states of the associated code Hamiltonians¹. 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 [38, 30]. Call an error-correcting code an $[[n, k, d]]$ code with locality ℓ if it has n physical qubits, k 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.** *Let \mathcal{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 $\varepsilon > 0$ and any state ψ on n -qubits with energy $\leq \varepsilon n$, the circuit depth of ψ is at least*

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

In the case of linear-rate and polynomial-distance codes such as the hypergraph product code of Tillich and Zémor [50], 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

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 [43].

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 $O(n/\text{poly} \log n)$ and a super-constant circuit lower bound for any state of energy $o(n)$. Recent developments [46, 32, 18] 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 $1/\text{poly}(n)$.

Furthermore, for any stabilizer code of nearly-linear-rate (i.e. $n^{1-\delta}$ rate) 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 code² with $O(n^{1-\delta})$ punctures [16, 26]. 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 [28] or golden codes [42], for which our main result will also prove a super-constant circuit lower bound for all states of energy $o(n)$.

1.2 Challenges and an overview of proof techniques

Code-states of an error correcting code are well known to have a large circuit complexity $\sim \log d$, where d is the distance of the code. This lower bound arises from the local indistinguishability property (see Fact 2), which means that for any size $< d$ subset S of the qubits, the reduced density matrix 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 works [23, 45], 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 [45], low-error is a strictly weaker notion than low-energy. Without invoking highly non-trivial properties such as local testability [23], it seems unclear if the low-energy states can be viewed as low-error. This leads to the central challenge towards the NLTS conjecture: capturing the circuit complexity of the low-energy states. The prior arguments, all of which rely on local indistinguishability (captured 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 [16], 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-space³.

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 works [23, 24] was to build a low-depth decoding circuit to bring

² The punctured 2D toric code is known to saturate the information-distance tradeoff bound of [16].

³ This is proved using an information theory argument. Consider a state ψ with small trace distance to the code. Then, the reduced density matrices $\{\psi_S\}$ approximate the reduced density matrices of the closest state of \mathcal{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

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 ideal parameter regime. We instead appeal to the observation that every eigenspace of a stabilizer code Hamiltonian possesses the local indistinguishability property (Fact 2). 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 conjecture 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 has been previously suspected that a QLDPC property would be necessary for NLTS Hamiltonians [27, 5, 31, 23, 45]. Our result 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 is believed that the QLDPC codes also need to be locally-testable [5] for NLTS. This fact is formalized by Eldar and Harrow [23] 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 $O(1/\text{poly log } n)$ with a distance of $\Omega(\sqrt{n})$ [31, 41]. Our construction does not require local-testability; in fact, the hypergraph product code [50] 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 [41, page 4].

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

output of a low-depth circuit W , then for any qubit i ,

$$\text{tr}_{-\{i\}}(W^\dagger \psi W) \approx \text{tr}_{-\{i\}}(W^\dagger \Theta W). \quad (2)$$

This is because (a) $\text{tr}_{-L_i}(\psi) \approx \text{tr}_{-L_i}(\Theta)$ where L_i is the support of the lightcone of qubit i with respect to W and (b) the value of the i th qubit of a W -rotated state only depends on the lightcone of the i th qubit. However, the left-hand side of (2) equals the pure state $|0\rangle\langle 0|$ and so the entropy of $\text{tr}_{-\{i\}}(W^\dagger \Theta W)$, the i th 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.

chunk is $O((D\varepsilon)^{-1/D})$. 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 $\exp(((D\varepsilon)^{-1/D})^D) = O(\exp(1/D\varepsilon)) = O(1)$; 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 $O(1/\varepsilon^{1/D})$, the aforementioned quantum state ρ can actually be prepared by a circuit of depth $O(\min(\log n, \log(1/\varepsilon)))$. Note that this holds for any $0 < \varepsilon < 1$, 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 (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 [37] and quantum computation with physically realistic systems [48, 49]. 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 [52], quantum chemistry [21], and quantum annealing [9, 33]. 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 [47, 40, 21] or Quantum Adiabatic Optimization Algorithm [25], is precisely the class of quantum states that can be generated by low-depth quantum circuits.

Theorem 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 $\text{NP} \neq \text{QMA}$); the original proof of Kitaev had a promise gap of $O(n^{-3})$ [36, 35] which was improved by [20, 12].

Robustness to perturbations

Prior to our results, being robust to constant-distance perturbations was only known in the special case of CSS codes of distance $\omega(n^{0.5})$ or larger [23], as exhibited in recent codes [32, 46]. 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 10 and 13) or (b) any state of a quantum code of linear-distance (see full version [8]). For commuting codes, we can further show that they are robust to perturbations in trace distance very close to 1 (Lemma 13).

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 [27].

As mentioned earlier, a different line of work focused on the low-error states [23], which differ from a code-state on at most εn qubits. These works prove a circuit lower bound of $\Omega(\log n)$ on the complexity of all low-error states of a specific local Hamiltonian [23, 45] (for some constant ε).

Eldar has also shown an $\Omega(\log n)$ circuit lower bounds for Gibbs or thermal states of local Hamiltonians at $O(1/\log^2 \log n)$ temperature [24] which is a specific low-energy state formed by coupling the ground-state of a physical system to a “heat bath.”

Bravyi *et. al.* [15] give 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, comes quite close to proving the NLTS conjecture and, therefore, provides a positive result for the QPCP conjecture. And while we are able to provide a constant depth lower bound for all states of energy $\leq n/100$, 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 , $\text{tr}(H'\phi) \geq p \cdot \text{tr}(H\phi)$ 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.

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 34 in the full version [8] Appendix C, where we delve into this idea in greater detail. This is analogous to the amplification step in Dinur’s PCP theorem [22] 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

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 [23] 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 $O(2^t \varepsilon n)$ 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 using linear rate codes for some constant $\varepsilon = \Omega(k/n) = \Omega(1)$.

1.7.3 Lower bounds against other classical approximations

The NLTS conjecture postulates a lower bound on the approximability of local Hamiltonians by low-depth circuits. However, if the QPCP conjecture is true and $\text{NP} \neq \text{QMA}$, then we should be able to prove lower bounds on the approximability of local Hamiltonians by any means of classical 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 $\text{NPTIME}[t(n)]$ for progressively larger and larger $t(n)$ up to $\text{poly}(n)$.

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 10). In Section 4, we prove our main result, Theorem 1. Additional appendix, available in the full version [8], contain (1) proofs of other related techniques for lower bounding circuit complexity, (2) improved lower bound techniques based on approximate ground-state projectors, and (3) 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.

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 $\text{tr}_{-A} \stackrel{\text{def}}{=} \text{tr}_{[m] \setminus A}$. Therefore, $\text{tr}_{-i}(\cdot)$ gives the reduced marginal on the i th qubit.

Quantum states

A quantum state is a positive semi-definite 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 with rank 1 (i.e. it can be expressed as $|\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle$). In which case we will refer to the state as $|\psi\rangle$ when interested in the unit vector representation and ψ when interested in the positive semi-definite 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 $\rho_A \stackrel{\text{def}}{=} \text{tr}_B(\rho_{AB})$, 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 .

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 $S(\rho)$, 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 density matrix 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 $\nu_{\mathcal{H}} \stackrel{\text{def}}{=} \frac{\mathbb{1}_{\mathcal{H}}}{|\mathcal{H}|}$.

2.2 Error-correction

Here we recall the definitions of a quantum error-correcting code. We will refer to a code \mathcal{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. We can define distance precisely using the Knill-Laflamme conditions [39].

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

$$\langle \bar{x} | E | \bar{y} \rangle = \begin{cases} 0 & x \neq y \\ \eta_E & x = y \end{cases} \quad (3)$$

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

$$\Pi_{\mathcal{C}} E \Pi_{\mathcal{C}} = \eta_E \Pi_{\mathcal{C}} \quad (4)$$

where $\Pi_{\mathcal{C}}$ is the projector onto the code-space. We say that the code \mathcal{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 density matrix 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 (Local Indistinguishability).** *Let \mathcal{C} be a $[[n, k, d]]$ error correcting code and S a subset of the qubits such that $|S| < d$. Then the reduced density matrix ρ_S of any code-state ρ on the set S is an invariant of the code.*

Proof. See full version [8]. ◀

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

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

► **Definition 3 (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*

$$\mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (5)$$

► **Definition 4 (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 \mathcal{C} is defined as the simultaneous $+1$ eigenspace of each element of \mathcal{S} :*

$$\mathcal{C} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : C_i |\psi\rangle = |\psi\rangle \quad \forall i \in [N]\}. \quad (6)$$

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

$$D_s = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : C_i |\psi\rangle = (-1)^{s_i} |\psi\rangle \quad \forall i \in [N]\}. \quad (7)$$

In this language, $\mathcal{C} = D_{0^N}$. 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} :

$$\mathcal{L} = \{P \in \mathcal{P}_n : PC_i = C_i P \quad \forall i \in [N]\} \setminus \mathcal{S}. \quad (8)$$

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

$$H = \sum_{i \in [N]} H_i \stackrel{\text{def}}{=} \sum_{i \in [N]} \frac{\mathbb{I} - C_i}{2}. \quad (9)$$

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. Furthermore, 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

$$\overline{X}_1, \overline{Z}_1, \dots, \overline{X}_k, \overline{Z}_k \quad (10)$$

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 work consist of gates with fan-in and fan-out of 2 and that the connectivity of the circuits is all-to-all⁴. 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.

⁴ 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.

► **Definition 5** (Circuit Complexity). *Let ρ be a mixed quantum state of n qubits. Then the circuit complexity⁵ of ρ , $\text{cc}(\rho)$, is defined as the minimum depth over all m -qubit quantum circuits U such that $U|0\rangle^{\otimes m} \in (\mathbb{C}^2)^{\otimes m}$ is a purification of ρ . Equivalently,*

$$\text{cc}(\rho) = \min \left\{ \text{depth}(U) : \text{tr}_{[m] \setminus [n]} \left(U|0\rangle\langle 0|^{\otimes m} U^\dagger \right) = \rho \right\}. \quad (11)$$

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 $\{u_{t,k_t}, u_{t-1,k_{t-1}}, \dots, u_{b,k_b}\}$ (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, proven in the full version [8].

► **Fact 6.** *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*

$$\text{tr}_{-A}(U\psi U^\dagger) = \text{tr}_{-A}(U(\psi_{L_A} \otimes \nu_{-L_A})U^\dagger). \quad (12)$$

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

► **Fact 7.** *Consider a quantum state $|\phi\rangle = U|0\rangle^{\otimes m}$. Let $A \subset [m]$ and define $|\phi'\rangle = U_A|0\rangle^{\otimes m}$. We have $\text{tr}_{-A}(\phi) = \text{tr}_{-A}(\phi')$.*

2.4 Quantum PCP and NLTS conjectures

► **Conjecture 8** (Quantum PCP [6, 3]). *It is QMA-hard to decide whether a given $O(1)$ -local Hamiltonian $H = H_1 + \cdots + H_m$ (where each $\|H_i\| \leq 1$) has minimum eigenvalue at most a or at least b when $b - a \geq c\|H\|$ for some universal constant $c > 0$.*

Since, it is widely believed that $\text{NP} \neq \text{QMA}$, 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.

⁵ 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 $\leq \varepsilon n$. If ρ is a state of energy $\leq \varepsilon n$, then every state $\rho' \in B_\delta(\rho)$ has energy $\leq (\varepsilon + \delta)n$. Therefore, by redefining $\varepsilon \leftarrow \varepsilon - \delta$, we can switch to the alternate definition of circuit complexity. We use the listed definition in our proofs as it vastly simplifies legibility.

If we assume the quantum PCP conjecture, then *all low-energy* states of the local Hamiltonian should not have constant circuit complexity. This is because if there exists a constant circuit complexity state 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 $\text{NP} \neq \text{QMA}$, a contradiction. This is the inspiration for the NLTS conjecture.

► **Conjecture 9** (NLTS [27]). *There exists a fixed constant $\varepsilon > 0$ 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*

$$\text{tr}\left(H^{(n)}\psi_n\right) \leq \varepsilon\|H^{(n)}\| + \lambda_{\min}(H^{(n)}), \quad (13)$$

the circuit complexity $\text{cc}(\psi_n)$ grows faster than any constant⁶.

Therefore, making the widely believed assumption $\text{NP} \neq \text{QMA}$, the quantum PCP conjecture implies the NLTS conjecture, 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 conjecture is an important first step towards proving the quantum PCP conjecture. One of the advantages of the NLTS conjecture 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 to small trace-distance perturbations.

► **Lemma 10.** *Let \mathcal{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 \mathcal{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 $\text{cc}(\psi) > \log d$.*

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 \mathcal{C} in trace distance, meaning that there exists a state $\rho_{\text{code}} \in \mathcal{C}$ such that $\|\psi_{\text{code}} - \rho_{\text{code}}\|_1 \leq \delta$. Thus, Uhlmann’s theorem [51] 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 $(\mathbb{C}^2)^{\otimes k} \rightarrow (\mathbb{C}^2)^{\otimes n}$ mapping k qubits to the k qubit code-space. Define \mathcal{E} as the maximally decohering channel as follows

$$\mathcal{E}(\cdot) \stackrel{\text{def}}{=} \frac{1}{4^k} \sum_{a,b \in \{0,1\}^k} (X^a Z^b) (\cdot) (X^a Z^b)^\dagger. \quad (14)$$

⁶ This definition is the one originally expressed by Freedman and Hastings in [27]. However, a consequence of the quantum PCP conjecture and $\text{NP} \neq \text{QMA}$ would be a circuit complexity lower bound of $\omega(\log \log n)$. For this reason, we will be more interested in circuit lower bounds of $\omega(\log \log n)$. Furthermore, if $\text{QCMA} \neq \text{QMA}$, then the necessary consequence of the quantum PCP conjecture is a circuit lower bound of $\omega(\text{poly}(n))$. 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 NLTS was made by Nirkhe, Vazirani, and Yuen [45].

6:12 Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians

Then let Θ be the encoding of ρ defined as

$$\Theta \stackrel{\text{def}}{=} \text{Enc} \circ \mathcal{E} \circ \text{Enc}^{-1}(\rho). \quad (15)$$

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 18.

► **Fact 11** (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 $|R_1| < d$, $\rho_{R_1 \cup R_2} = \Theta_{R_1 \cup R_2}$.*

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

$$\|\psi_R - \Theta_R\|_1 \leq \delta. \quad (16)$$

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 6 here, we have

$$\text{tr}_{-\{i\}}(U^\dagger \Theta U) = \text{tr}_{-\{i\}}(U^\dagger (\Theta_{L_i} \otimes \nu_{-L_i}) U). \quad (17)$$

Since the size of L_i is $< d$, we can combine (16) and (17) to achieve

$$\|\text{tr}_{-\{i\}}(U^\dagger (\psi_{L_i} \otimes \nu_{-L_i}) U) - \text{tr}_{-\{i\}}(U^\dagger (\Theta_{L_i} \otimes \nu_{-L_i}) U)\|_1 \leq \delta. \quad (18)$$

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

$$\|\text{tr}_{-\{i\}}(|0\rangle\langle 0|_i - \text{tr}_{-\{i\}}(U^\dagger (\Theta_{L_i} \otimes \nu_{-L_i}) U)\|_1 \leq \delta. \quad (19)$$

Using standard entropy bounds, we can bound the entropy of the i th qubit of the rotated state Θ :

$$S(\text{tr}_{-\{i\}}(U^\dagger \Theta U)) = S(\text{tr}_{-\{i\}}(U^\dagger (\Theta_{L_i} \otimes \nu_{-L_i}) U)) \leq H_2(\delta) \leq 2\delta \log(1/\delta). \quad (20)$$

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

$$k \leq S(\Theta) \leq \sum_{i \in [m]} S(\text{tr}_{-\{i\}}(U^\dagger \Theta U)) \leq 2\delta \log(1/\delta) m. \quad (21)$$

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 7 ensures that we can assume $m \leq 2^{\text{cc}(\psi)} n$, without loss of generality. This gives us the following corollary:

► **Corollary 12.** *Let \mathcal{C} be a $[[n, k, d]]$ code and $|\psi\rangle$ a pure-state and the trace-distance between $|\psi\rangle$ and \mathcal{C} is $0 < \delta < 1/2$ such that $k > 2\delta \log(1/\delta) n$. Then, the circuit complexity $\text{cc}(|\psi\rangle)$ satisfies*

$$\text{cc}(|\psi\rangle) \geq \log \left(\min \left\{ d, \frac{k}{2\delta \log(1/\delta) n} \right\} \right). \quad (22)$$

Proof. By Lemma 10, either $2^{\text{cc}(|\psi\rangle)} \geq d$ or $k \leq 2\delta \log(1/\delta) 2^{\text{cc}(|\psi\rangle)} n$ since $m \leq 2^{\text{cc}(|\psi\rangle)} n$. Rearranging this is equivalent to the corollary. ◀

Proof of Fact 11. 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

$$|\psi\rangle = \sum_{x \in \{0,1\}^k} |\bar{x}\rangle |\psi_x\rangle \quad (23)$$

where $\{|\bar{x}\rangle\}$ 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,

$$\text{tr}_{-(R_1 \cup R_2)} (U\psi U^\dagger) = \sum_{x,y \in \{0,1\}^k} \text{tr}_{-R_1} (U |\bar{x}\rangle \langle \bar{y}| U^\dagger) \otimes \text{tr}_{-R_2} (|\psi_x\rangle \langle \psi_y|) \quad (24)$$

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 $U |\bar{x}\rangle$ and $U |\bar{y}\rangle$ despite the erasure of $|R_1| < d$ qubits. Therefore,

$$\text{tr}_{-(R_1 \cup R_2)} (U\psi U^\dagger) = \phi_{R_1} \otimes \sum_{x \in \{0,1\}^k} \text{tr}_{-R_2} (\psi_x). \quad (25)$$

which is an invariant of U , which means $\text{tr}_{-(R_1 \cup R_2)} (\rho) = \text{tr}_{-(R_1 \cup R_2)} (U\rho U^\dagger)$. 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 12 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 $\Omega(2^{-2t}) = \Omega(d^{-2\gamma})$ 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 \mathcal{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 $\rho_0 \in \mathcal{C}$ having good fidelity with the code-space, that is, $f \stackrel{\text{def}}{=} F(\psi_{\text{code}}, \rho_0)$. Fact 7 ensures that we can choose $m \leq 2^t n$. We prove the following lemma.

▶ **Lemma 13.** *For the state $|\psi\rangle$ as defined above, it holds that*

$$2^{2t} \geq \min \left(d, \frac{1}{64\sqrt{\ell} \log^2 d \ell} \cdot \frac{k\sqrt{d}}{n \cdot \sqrt{\log \frac{1}{f}}} \right). \quad (26)$$

The proof of this lemma appears in Appendix B of the full version [8]. 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 [29, 11, 10, 7]. 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 $1 - \exp(-\tilde{\Omega}(d^{1-4\gamma}))$ far from the code-space in trace distance. Here, the $\tilde{\Omega}$ notation hides some polylog factors. This bears some resemblance with the results of [13, 43], which show that the distributions sampled from depth t (and size $e^{n^{1/t}}$) classical AC0 circuits are $1 - e^{-n^{1/t}}$ far from the uniform distribution over a good classical code (linear rate and linear distance). A comparison with Lemma 13 is largely unclear, due to the differences between classical and quantum codes, as well as AC0 circuits and quantum circuits.

6:14 Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians

We further prove the following lemma for codes encoding at least one qubit and having large distance. This complements Lemma 13 replacing the linear rate condition with linear distance condition.

► **Lemma 14.** *Given $|\psi\rangle = U|0\rangle^{\otimes m}$ with U of depth t and let \mathcal{C} be a code with distance d . Let Π be the projector onto the codespace and $f = \sqrt{\langle\psi|(\Pi \otimes \mathbb{I}_{\text{anc}})|\psi\rangle}$ be the fidelity of $|\psi\rangle$ with the codespace. If $2^t \leq \frac{d}{2}$ then*

$$f^2 \leq 2e^{-\frac{d^2}{2^{2t+10}m}}. \quad (27)$$

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 [34, 19], it is known that there exists a polynomial $P(G)$ of degree $\frac{d}{2^{t+1}}$ such that

$$\|P(G) - |\psi\rangle\langle\psi|\| \leq e^{-(\frac{d}{2^{t+1}})^2/2^8 m} = e^{-\frac{d^2}{2^{2t+10}m}}. \quad (28)$$

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 $\phi'_{\text{code}} \in \Pi$ 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

$$\sum_x \alpha_x \langle\phi_x|\phi_x\rangle = 0 \implies \langle\phi|\phi'\rangle = 0. \quad (29)$$

Since $P(G)$ is a sum of $\leq \frac{d}{2}$ -local terms, (4) ensures that

$$\langle\phi'|P(G)|\phi'\rangle = \langle\phi'|\Pi P(G)\Pi|\phi'\rangle = \eta_{P(G)} \langle\phi'|\Pi|\phi'\rangle = \eta_{P(G)} = \langle\phi|P(G)|\phi\rangle. \quad (30)$$

Using Equation 28 and $\langle\phi'|\psi\rangle = 0$, we have $\langle\phi'|P(G)|\phi'\rangle \leq e^{-\frac{d^2}{2^{2t+10}m}}$. Thus using Equation 28 again,

$$f^2 = |\langle\phi|\psi\rangle|^2 \leq \langle\phi|P(G)|\phi\rangle + e^{-\frac{d^2}{2^{2t+10}m}} = \langle\phi'|P(G)|\phi'\rangle + e^{-\frac{d^2}{2^{2t+10}m}} \leq 2e^{-\frac{d^2}{2^{2t+10}m}}. \quad (31)$$

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; which combines Theorems 20 and 23. For Theorem 20, 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 \mathcal{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 in the full version [8].

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

► **Fact 15.** Fix a stabilizer code \mathcal{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 $\rho_{\text{code}} \in D_s$, and a logical operator $P \in \mathcal{L}$, we have $(P\rho P)_{\text{code}} \in D_s$.

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

► **Fact 16.** 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 $\rho_{\text{code}} \in D_s$, we have $\text{tr}(P\rho) = 0$.

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 17.** Let ρ be a state such that $\rho_{\text{code}} \in D_s$ 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 $\rho_{\text{anc}} = \rho'_{\text{anc}}$ and $\rho_{\text{code}}, \rho'_{\text{code}} \in D_s$ 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 (15):

$$\mathcal{E}(\cdot) \stackrel{\text{def}}{=} \frac{1}{4^k} \sum_{a, b \in \{0, 1\}^k} \left(\overline{X}^a \overline{Z}^b \right) (\cdot) \left(\overline{Z}^b \overline{X}^a \right) \quad (32)$$

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 11.

► **Fact 18.** 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 $\rho_{\text{code}} \in D_s$ for some s , $\mathcal{E}(\rho)_{\text{code}} \in D_s$. 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 19.** Let \mathcal{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 $|\phi\rangle = U|0\rangle^{\otimes m}$ where U is a circuit of depth t . From Fact 7, 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 20.** Let \mathcal{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 $\text{tr}(H\phi) \leq \varepsilon N$ and circuit complexity $t \stackrel{\text{def}}{=}} \text{cc}(\phi) < \log(d) - 2\ell^3$. Then, for a constant c_ℓ depending only on ℓ and not the size of the code,

$$2^{2t} > \frac{k}{c_\ell n \cdot \varepsilon \log \frac{1}{\varepsilon}}. \quad (33)$$

6:16 Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians

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

$$\varepsilon_i \stackrel{\text{def}}{=} \text{tr}(H_i\phi) = \frac{1}{2} - \frac{1}{2} \text{tr}(C_i\phi). \quad (34)$$

Add $N \leq n$ new syndrome-measurement ancilla (SMA) qubits each with initial state $|0\rangle$ and coherently measure the entire syndrome using the depth $2\ell^3$ circuit V from Fact 19. Then the state

$$|\psi\rangle = V\left(|\phi\rangle \otimes |0\rangle^{\otimes N}\right) = VU|0\rangle^{\otimes(m+N)} \stackrel{\text{def}}{=} W|0\rangle^{\otimes(m+N)} \quad (35)$$

with $W = VU$ a circuit of minimum circuit depth $\stackrel{\text{def}}{=} \text{cc}(W) \leq t + 2\ell^3$. Define the state obtained by incoherently measuring all the SMA qubits of $|\psi\rangle$ as

$$\Psi = \sum_{s \in \{0,1\}^N} D_s |\phi\rangle\langle\phi| D_s \otimes |s\rangle\langle s| \quad (36)$$

where we abuse notation slightly and use D_s both as the eigenspace and the projector onto it. Since we assume that \mathcal{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 (32). Then, we have

$$\Theta = \sum_s \text{tr}(D_s\phi D_s) \mu_s \otimes |s\rangle\langle s| \quad \text{for } \mu_s \stackrel{\text{def}}{=} \mathcal{E}\left(\frac{D_s\phi D_s}{\text{tr}(D_s\phi D_s)}\right). \quad (37)$$

▷ **Claim 21.** Fix any region $R \subset [m+N]$. Let S_R be the set of all indices $i \in [N]$ such that the i th SMA qubit belongs to R . Note that $S_R \subset R$. It holds that

$$F(\psi_R, \Psi_R) \geq 1 - \sum_{i \in S_R} \varepsilon_i. \quad (38)$$

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 $|L_j| \leq 2^{\text{cc}(W)} < d$. Since $W^\dagger|\psi\rangle$ is $|0\rangle^{\otimes(m+N)}$, we have that for any qubit $j \in [m+N]$,

$$\text{tr}_{-\{j\}}(W^\dagger\psi W) = |0\rangle\langle 0|. \quad (39)$$

However, Fact 6 allows us to equate

$$\text{tr}_{-\{j\}}(W^\dagger\psi W) = \text{tr}_{-\{j\}}(W^\dagger(\psi_{L_j} \otimes \nu_{-L_j})W), \quad (40)$$

$$\text{tr}_{-\{j\}}(W^\dagger\Theta W) = \text{tr}_{-\{j\}}(W^\dagger(\Theta_{L_j} \otimes \nu_{-L_j})W). \quad (41)$$

Using (38), we find that for all $j \in [m+N]$,

$$F(\text{tr}_{-\{j\}}(W^\dagger\psi W), \text{tr}_{-\{j\}}(W^\dagger\Theta W)) \quad (42)$$

$$= F(\text{tr}_{-\{j\}}(W^\dagger(\psi_{L_j} \otimes \nu_{-L_j})W), \text{tr}_{-\{j\}}(W^\dagger(\Theta_{L_j} \otimes \nu_{-L_j})W)) \quad (43)$$

$$\geq F(\psi_{L_j}, \Theta_{L_j}) \quad (44)$$

$$\geq 1 - \sum_{i \in S_{L_j}} \varepsilon_i. \quad (45)$$

We now infer from (39) and (45) that⁷

$$S(\text{tr}_{-\{j\}}(W^\dagger \Theta W)) \leq 2 \left(\sum_{i \in S_{L_j}} \varepsilon_i \right) \log \frac{1}{\min \left(\sum_{i \in S_{L_j}} \varepsilon_i, \frac{1}{4} \right)}. \quad (46)$$

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

$$\mathbb{E}_{j \in [m+N]} S(\text{tr}_{-\{j\}}(W^\dagger \Theta W)) \quad (47)$$

$$\leq 2 \mathbb{E}_{j \in [m+N]} \left(\left(\sum_{i \in S_{L_j}} \varepsilon_i \right) \log \frac{1}{\min \left(\sum_{i \in S_{L_j}} \varepsilon_i, \frac{1}{4} \right)} \right) \quad (48)$$

$$\leq 2 \cdot \left(\mathbb{E}_{j \in [m+N]} \sum_{i \in S_{L_j}} \varepsilon_i \right) \log \frac{1}{\min \left(\mathbb{E}_{j \in [m+N]} \sum_{i \in S_{L_j}} \varepsilon_i, \frac{1}{4} \right)}. \quad (49)$$

The next claim helps upper and lower bound this expression.

▷ **Claim 22.** It holds that

$$\frac{\varepsilon N}{m+N} \leq \mathbb{E}_{j \in [m+N]} \sum_{i \in S_{L_j}} \varepsilon_i \leq 2^{2\text{cc}(W)} \frac{\varepsilon N}{m+N}. \quad (50)$$

We now upper bound the entropy of Θ . For this, let us assume $2^{\text{cc}(W)} \leq \frac{1}{\varepsilon}$, else the proof is immediate.

$$S(\Theta) = S(W^\dagger \Theta W) \leq \sum_{j \in [m+N]} S(\text{tr}_{-\{j\}}(W^\dagger \Theta W)) \quad (51)$$

$$\leq 2^{1+2\text{cc}(W)} \varepsilon N \log \frac{1}{\min \left(\frac{\varepsilon N}{m+N}, \frac{1}{4} \right)} \quad (52)$$

$$\leq 2^{1+2\text{cc}(W)} \varepsilon \ell n \log \frac{2^{\text{cc}(W)}}{\varepsilon} \quad (53)$$

$$\leq \left(2^{2+2\text{cc}(W)} \ell n \right) \cdot \varepsilon \log \frac{1}{\varepsilon}. \quad (54)$$

The inequality in (51) comes from the subadditivity of entropy; the inequality in (52) uses (48) and then substitutes the upper and lower bounds given in Claim 22; the inequality in (53) uses $\frac{n}{\ell} \leq N \leq \ell n$ and $\frac{\varepsilon N}{m+N} \geq \frac{\varepsilon}{\ell 2^t + 1} \geq \frac{\varepsilon}{2^{\text{cc}(W)}}$; the inequality in (54) uses $2^{\text{cc}(W)} \leq \frac{1}{\varepsilon}$. Furthermore, Θ is the output of \mathcal{E} acting on Ψ . By Fact 18 (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 23.** Let \mathcal{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 $\text{tr}(H\phi) \leq \varepsilon N$ and circuit complexity $t \stackrel{\text{def}}{=} \text{cc}(\phi) < \log(d) - 1$. Then,

$$2^{2t} \geq \frac{d}{2^6 n \sqrt{\ell \varepsilon \log \frac{1}{\varepsilon}}}. \quad (55)$$

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 $2p \log \frac{1}{\min(p, \frac{1}{4})}$.

Proof. Since $\text{tr}(H\phi) \leq \varepsilon N$, Markov's inequality ensures that $\text{tr}(D_{\leq 2\varepsilon N}\phi) \geq \frac{1}{2}$, where $D_{\leq 2\varepsilon N}$ is the subspace of energy $\leq 2\varepsilon N$. Since $D_{\leq 2\varepsilon N} = \sum_{s \in \{0,1\}^N: |s| \leq 2\varepsilon N} D_s$ and the number of s satisfying $|s| \leq 2\varepsilon N$ is $\leq 2^{4\varepsilon N \log \frac{1}{\varepsilon}}$, there exists a $s^* \in \{0,1\}^N$ such that $\text{tr}(D_{s^*}\phi) \geq 2^{-4\varepsilon N \log \frac{1}{\varepsilon} - 1}$. Now, Fact 17 ensures that D_{s^*} is also an error correcting code of distance d . Applying Lemma 14 (assuming $2^t \leq \frac{d}{2}$) and setting $m \leq 2^t n$ (using Fact 7), we conclude

$$2^{-4N\varepsilon \log \frac{1}{\varepsilon} - 1} \leq 2e^{-\frac{d^2}{2^{3t+10}n}} \quad (56)$$

$$\implies 2^{4N\varepsilon \log \frac{1}{\varepsilon} + 2} \geq e^{\frac{d^2}{2^{3t+10}n}} \quad (57)$$

$$\implies 2^{3t} \geq \frac{d^2}{2^{12}nN\varepsilon \log \frac{1}{\varepsilon}}. \quad (58)$$

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

Combining Theorems 20 and 23, the proof of Theorem 1 concludes.

4.1 Omitted claims

Proof. (of Claim 21) 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

$$F(\Psi_R, \psi_R) = F(\psi'_R, \psi_R) \geq F(\psi', \psi). \quad (59)$$

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

$$|\psi\rangle = \sum_{t \in \{0,1\}^{|S_R|}} \sqrt{P(t)} |\psi_t\rangle |t\rangle_{S_R}, \quad \psi' = \sum_{t \in \{0,1\}^{|S_R|}} P(t) |\psi_t\rangle\langle\psi_t| \otimes |t\rangle\langle t|_{S_R}, \quad (60)$$

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

$$F^2(\psi, \psi') = \sum_{t \in \{0,1\}^{|S_R|}} \sqrt{P(t)} P(t) \sqrt{P(t)} |\langle\psi_t|\psi_t\rangle|^2 \quad (61)$$

$$= \sum_{t \in \{0,1\}^{|S_R|}} P(t)^2 \quad (62)$$

$$\geq P(t = (0, \dots, 0))^2. \quad (63)$$

Using a union bound, we get

$$P(t = (0, \dots, 0)) \geq 1 - \sum_{i=1}^{|S_R|} P(t_i = 1) = 1 - \sum_{i \in S_R} \varepsilon_i, \quad (64)$$

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

$$F(\psi, \psi') = P(t = (0, \dots, 0)) \geq 1 - \sum_{i \in S_R} \varepsilon_i. \quad (65)$$

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

$$(\mu_s \otimes |s\rangle\langle s|)_R = (\mu_s)_{R \setminus S_R} \otimes (|s\rangle\langle s|)_{S_R} \quad (66)$$

$$= \left(\frac{D_s \phi D_s}{\text{Tr}(D_s \phi D_s)} \right)_{R \setminus S_R} \otimes (|s\rangle\langle s|)_{S_R} \quad (67)$$

$$= \left(\frac{D_s \phi D_s}{\text{Tr}(D_s \phi D_s)} \otimes |s\rangle\langle s| \right)_R. \quad (68)$$

The second equality uses Fact 18 (Item 2) as $|R \setminus S_R| \leq |R| < d$. This establishes $\Psi_R = \Theta_R$. \triangleleft

Proof. (of Claim 22) Consider

$$(m + N) \mathbb{E}_{j \in [m+N]} \sum_{i \in S_{L_j}} \varepsilon_i = \sum_{j \in [m+N]} \sum_{i \in S_{L_j}} \varepsilon_i = \sum_i \varepsilon_i |\{j : i \in S_{L_j}\}|. \quad (69)$$

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 $b \in [\text{cc}(W)]$, 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 $\sum_{b=1}^{\text{cc}(W)} 2^b \leq 2^{2\text{cc}(W)}$. Thus,

$$\sum_{j \in [m+N]} \sum_{i \in S_{L_j}} \varepsilon_i \leq 2^{2\text{cc}(W)} \sum_i \varepsilon_i = 2^{2\text{cc}(W)} \varepsilon_N. \quad (70)$$

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

References

- 1 Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, November 2004. doi:10.1103/PhysRevA.70.052328.
- 2 Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, pages 417–426, New York, NY, USA, 2009. Association for Computing Machinery. doi:10.1145/1536414.1536472.
- 3 Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: The quantum pcg conjecture. *SIGACT News*, 44(2):47–79, June 2013. doi:10.1145/2491533.2491549.
- 4 Dorit Aharonov and Lior Eldar. The commuting local hamiltonian problem on locally expanding graphs is approximable in np. *Quantum Information Processing*, 14(1):83–101, January 2015. doi:10.1007/s11128-014-0877-9.
- 5 Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM Journal on Computing*, 44(5):1230–1262, 2015. doi:10.1137/140975498.
- 6 Dorit Aharonov and Tomer Naveh. Quantum np - a survey, 2002. arXiv:quant-ph/0210077.
- 7 Anurag Anshu, Aram W. Harrow, and Mehdi Soleimanifar. From communication complexity to an entanglement spread area law in the ground state of gapped local hamiltonians. arXiv:2004.15009, 2020. arXiv:2004.15009.
- 8 Anurag Anshu and Chinmay Nirkhe. Circuit lower bounds for low-energy states of quantum code hamiltonians, 2020. arXiv:2011.02044.
- 9 B. Apolloni, C. Carvalho, and D. de Falco. Quantum stochastic optimization. *Stochastic Processes and their Applications*, 33(2):233–244, 1989. doi:10.1016/0304-4149(89)90040-9.
- 10 Itai Arad, Alexei Kitaev, Zeph Landau, and Umesh Vazirani. An area law and sub-exponential algorithm for 1D systems, 2013. arXiv:1301.1162.
- 11 Itai Arad, Zeph Landau, and Umesh Vazirani. Improved one-dimensional area law for frustration-free systems. *Physical Review B*, 85:195145, May 2012. doi:10.1103/PhysRevB.85.195145.
- 12 Johannes Bausch and Elizabeth Crosson. Analysis and limitations of modified circuit-to-Hamiltonian constructions. *Quantum*, 2:94, September 2018. doi:10.22331/q-2018-09-19-94.
- 13 Chris Beck, Russell Impagliazzo, and Shachar Lovett. Large deviation bounds for decision trees and sampling lower bounds for ac0-circuits. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 101–110, 2012. doi:10.1109/FOCS.2012.82.

- 14 Fernando G.S.L. Brandao and Aram W. Harrow. Product-state approximations to quantum ground states. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 871–880, New York, NY, USA, 2013. Association for Computing Machinery. doi:10.1145/2488608.2488719.
- 15 Sergey Bravyi, Alexander Kliesch, Robert Koenig, and Eugene Tang. Obstacles to state preparation and variational optimization from symmetry protection. *arXiv*, 2019. arXiv:1910.08980.
- 16 Sergey Bravyi, David Poulin, and Barbara Terhal. Tradeoffs for reliable quantum information storage in 2d systems. *Phys. Rev. Lett.*, 104:050503, February 2010. doi:10.1103/PhysRevLett.104.050503.
- 17 Sergey Bravyi and Mikhail Vyalyi. Commutative version of the local hamiltonian problem and common eigenspace problem. *Quantum Info. Comput.*, 5(3):187–215, May 2005.
- 18 N. P. Breuckmann and J. Eberhardt. Balanced product quantum codes. *arXiv: Quantum Physics*, 2020.
- 19 Harry Buhrman, Richard Cleve, Ronald de Wolf, and Christof Zalka. Bounds for small-error and zero-error quantum algorithms. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, FOCS '99, page 358, USA, 1999. IEEE Computer Society.
- 20 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*, 97:062306, June 2018. doi:10.1103/PhysRevA.97.062306.
- 21 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, October 2019. doi:10.1021/acs.chemrev.8b00803.
- 22 Irit Dinur. The pcg theorem by gap amplification. *J. ACM*, 54(3):12–es, June 2007. doi:10.1145/1236457.1236459.
- 23 L. Eldar and A. W. Harrow. Local hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 427–438, 2017. doi:10.1109/FOCS.2017.46.
- 24 Lior Eldar. Robust quantum entanglement at (nearly) room temperature. *arXiv: Quantum Physics (to appear in ITCS 2021)*, 2019.
- 25 Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm. *arXiv preprint*, 2014. arXiv:1411.4028.
- 26 Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86:032324, September 2012. doi:10.1103/PhysRevA.86.032324.
- 27 Michael H. Freedman and Matthew B. Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *Quantum Info. Comput.*, 14(1–2):144–180, January 2014.
- 28 Larry Guth and Alexander Lubotzky. Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds. *Journal of Mathematical Physics*, 55(8):082202, 2014. doi:10.1063/1.4891487.
- 29 Matthew B Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2007(08):P08024, 2007.
- 30 Matthew B. Hastings. Topological order at nonzero temperature. *Phys. Rev. Lett.*, 107:210501, November 2011. doi:10.1103/PhysRevLett.107.210501.
- 31 Matthew B. Hastings. Quantum Codes from High-Dimensional Manifolds. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, volume 67 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 25:1–25:26, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ITCS.2017.25.

- 32 Matthew B. Hastings, Jeongwan Haah, and Ryan O'Donnell. Fiber bundle codes: Breaking the $n^{1/2}$ polylog(n) barrier for quantum ldpc codes, 2020. [arXiv:2009.03921](#).
- 33 Tadashi Kadowaki and Hidetoshi Nishimori. Quantum annealing in the transverse ising model. *Phys. Rev. E*, 58:5355–5363, November 1998. doi:10.1103/PhysRevE.58.5355.
- 34 Jeff Kahn, Nathan Linial, and Alex Samorodnitsky. Inclusion-exclusion: Exact and approximate. *Combinatorica*, 16(4):465–477, December 1996. doi:10.1007/BF01271266.
- 35 Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006. doi:10.1137/S0097539704445226.
- 36 A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, USA, 2002.
- 37 Alexei Kitaev and John Preskill. Topological entanglement entropy. *Phys. Rev. Lett.*, 96:110404, March 2006. doi:10.1103/PhysRevLett.96.110404.
- 38 A.Yu. Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303(1):2–30, 2003. doi:10.1016/S0003-4916(02)00018-0.
- 39 Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55:900–911, February 1997. doi:10.1103/PhysRevA.55.900.
- 40 Ryan LaRose, Arkin Tikku, Étude O'Neel-Judy, Lukasz Cincio, and Patrick J. Coles. Variational quantum state diagonalization. *npj Quantum Information*, 5(1):57, June 2019. doi:10.1038/s41534-019-0167-6.
- 41 Anthony Leverrier, Vivien Londe, and Gilles Zémor. Towards local testability for quantum coding, 2019. [arXiv:1911.03069](#).
- 42 Vivien Londe and Anthony Leverrier. Golden codes: Quantum ldpc codes built from regular tessellations of hyperbolic 4-manifolds. *Quantum Info. Comput.*, 19(5–6):361–391, May 2019.
- 43 Shachar Lovett and Emanuele Viola. Bounded-depth circuits cannot sample good codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 17:115, October 2010. doi:10.1007/s00037-012-0039-3.
- 44 Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 731–742. IEEE Computer Society, 2018. doi:10.1109/FOCS.2018.00075.
- 45 Chinmay Nirkhe, Umesh Vazirani, and Henry Yuen. Approximate Low-Weight Check Codes and Circuit Lower Bounds for Noisy Ground States. In Ioannis Chatzigiannakis, Christos Kaklamani, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, volume 107 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 91:1–91:11, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.ICALP.2018.91.
- 46 Pavel Panteleev and Gleb Kalachev. Quantum ldpc codes with almost linear minimum distance, 2020. [arXiv:2012.04068](#).
- 47 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(1):4213, July 2014. doi:10.1038/ncomms5213.
- 48 Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, May 2001. doi:10.1103/PhysRevLett.86.5188.
- 49 Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, August 2003. doi:10.1103/PhysRevA.68.022312.
- 50 J. Tillich and G. Zemor. Quantum ldpc codes with positive rate and minimum distance proportional to sqrt(n). In *2009 IEEE International Symposium on Information Theory*, pages 799–803, 2009. doi:10.1109/ISIT.2009.5205648.
- 51 A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

6:22 Circuit Lower Bounds for Low-Energy States of Quantum Code Hamiltonians

- 52 Steven R. White. Density matrix formulation for quantum renormalization groups. *Phys. Rev. Lett.*, 69:2863–2866, November 1992. doi:10.1103/PhysRevLett.69.2863.