58th Annual IEEE Symposium on Foundations of Computer Science

Local Hamiltonians Whose Ground States are Hard to Approximate

Lior Eldar
Center for Theoretical Physics
MIT
Cambridge, USA
leldar@mit.edu

Aram W. Harrow
Center for Theoretical Physics
MIT
Cambridge, USA
aram@mit.edu

***Abstract*—Ground states of local Hamiltonians can be generally highly entangled: any quantum circuit that generates them, even approximately, must be sufficiently deep to allow coupling (entanglement) between any pair of qubits. Until now this property was not known to be "robust" - the marginals of such states to a subset of the qubits containing all but a small constant fraction of them may be only locally entangled, and hence approximable by shallow quantum circuits. In this work we construct a family of 16-local Hamiltonians for which any marginal of a ground state to a fraction at least $1-10^{-8}$ of the qubits must be globally entangled.**

This provides evidence that quantum entanglement is not very fragile, and perhaps our intuition about its instability is an artifact of considering local Hamiltonians which are not only local but *spatially local*. Formally, it provides positive evidence for two wide-open conjectures in condensed-matter physics and quantum complexity theory which are the qLDPC conjecture, positing the existence of "good" quantum LDPC codes, and the NLTS conjecture [1] positing the existence of local Hamiltonians in which any low-energy state is highly entangled.

Our Hamiltonian is based on applying the hypergraph product by Tillich-Zémor [2] to the repetition code with checks from an expander graph. A key tool in our proof is a new lower bound on the vertex expansion of the output of low-depth quantum circuits, which may be of independent interest.

***Keywords*-NLTS, PCP, robust codes, high-dimensional expander**

I. Introduction

Quantum entanglement is the phenomenon by which distant particles are correlated in a way that cannot be replicated by correlated classical probability distributions. Despite nearly 70 years of research into this phenomenon it is far from understood. That said, quantum entanglement is considered to be the source of the possible speed-up compared with classical problems. Hence, in the context of building a quantum computer, its "supremacy" is achievable only if we can maintain and control entanglement. However, in practice, scalable quantum computers have been hard to build because large entangled states are often fragile and hard to maintain.

One way of quantifying entanglement which relates to standard notions of complexity classes is circuit depth:

Definition 1 (Depth-d Trivial States)**.** *We say that an n-qubit state ρ is depth-d trivial if it can be prepared by applying a depth-d quantum circuit comprised of d layers of tensor-products of 2-local quantum gates, to $|0\rangle^{\otimes N}$ (for some $N \geq n$) and tracing out $N-n$ qubits.*

(Variants of this definition state that ρ cannot even be approximated in this way.) We say that a family of states on n qubits is *non-trivial* or (*highly entangled*) if they are not d-trivial for any $d = O(1)$ - i.e. to generate this family of states, the circuit depths must diverge with the number of qubits. An important threshold is $d \sim \log(n)$ as a depth of $d \geq \log(n)$ allows potentially each qubit to be entangled with any other qubit.

The characterization of the amount of entanglement in a quantum state via the depth of the circuit required to (approximately) generate it has been used extensively in literature in the context of quantum complexity theory [1], [3] and to classify quantum phases of matter in condensed matter theory [4]. In particular, a pair of quantum states is said to belong to the same quantum phase of matter if one can transform one to the other using a quantum circuit of bounded depth [4].

In all of these studies the quantum states under consideration are 0-eigenstates, or ground states, of local Hamiltonians:

Definition 2 (k-Local Hamiltonians)**.** *A local Hamiltonian is a positive-semidefinite (PSD) matrix $0 \preceq H \preceq I$ that can be written as a sum $H = \sum_i H_i$ where*

0272-5428/17 $31.00 © 2017 IEEE
DOI 10.1109/FOCS.2017.46

$H_i \succeq 0$, and $H_i = h_i \otimes I$, where $h_i \succeq 0$ is a PSD operator on $\mathbb{C}^{2^{\otimes k}}$.

For simplicity we mostly consider Hamiltonians that are frustration-free, meaning that there its minimum eigenvalue is 0, corresponding to a 0-eigenstate of H (the "ground state") that is a simultaneous 0-eigenstate of each H_i. Ground states are physically relevant because at low temperatures the system will naturally reach a state which is close to the ground state. One can also think of local Hamiltonians as the quantum analog of classical constraint satisfaction problems, where quantum states play the role of assignments to the variables. Under this analogy, ground states are *satisfying* assignments of the quantum CSP's (e.g. local Hamiltonians).

Inspired by the NLTS conjecture due to Freedman and Hastings [1] and quantum error correction we introduce a notion of robustness that measures the robustness of the circuit depth of a ground state according to its similarity of states to ground states:

Definition 3. ***Ground-state impostors*** *Let H be a k-local Hamiltonian. A quantum state ρ is said to be an ε-impostor for H, if there exists a set $S \subseteq [n], |S| \geq (1-\varepsilon)n$ and a ground state σ (i.e. satisfying $\mathrm{tr}[H\sigma] = \lambda_{\min}(H)$) such that $\rho_S = \sigma_S$.*

One can then relate to an infinite family of local Hamiltonians $H = \{H_n\}_{n\in\mathbb{N}}$ and an infinite family of states $\mathcal{F} = \{\rho_n\}_{n\in N}$, and say that $\mathcal{F}$ is an ε-impostor for H if ρ_n is an ε-impostor for H_n for all sufficiently large n.

Using this definition, we say that a local Hamiltonian has no low-error trivial states (NLETS) if it is hard to generate not just the ground-state, but all states that "look" as ground-states:

Definition 4. ***No Low-Error Trivial States (NLETS)*** *Let $k > 1$ be some integer and $\{H_n\}_{n\in\mathbb{N}}$ be a family of k-local Hamiltonians. $\{H_n\}_{n\in\mathbb{N}}$ is NLETS if there exists a constant $\varepsilon > 0$ such that any ε-impostor family $\mathcal{F} = \{\rho_n\}_{n\in\mathbb{N}}$ of $\{H_n\}_{n\in\mathbb{N}}$ is non-trivial.*

In the context of classical constraint satisfaction an implication of the PCP theorem is that there exists a constant $\varepsilon > 0$ and a family of instances of CSP such that any ε-impostor of these CSP's is NP-hard to find (though generating it is very easy, as it is just a bit string). Previously known local quantum Hamiltonians are not NLETS for any constant $\varepsilon > 0$. This is partly because most physically-realizable local Hamiltonians are defined with respect to a d-regular grid for small values of d, and hence cannot be NLETS, almost trivially. [1]

It is easy to check that even quantum codes embedded in low-dimensions, such as the well-known toric code [5] have a circuit lower bound for "typical" impostor states sampled by applying uniformly random error with some constant probability $\varepsilon > 0$ to each qubit. However, this property is crucially different than NLETS as it amounts to an *average-case* robustness and not *worst-case* robustness.

Hence, to date, there are no known constructions of local Hamiltonians that are NLETS, i.e. require that any state that appears like a ground-state, must be highly entangled. In fact, the existence of such Hamiltonians is a necessary condition for a number of important conjectures in quantum complexity theory, namely the quantum PCP conjecture [6], the quantum LDPC conjecture, NLTS conjecture [1], and the qLTC conjecture [7], since the multitude of these conjectures hinge essentially on the ability to maintain *global* entanglement using a set of local constraints, in a way that is robust against a constant-fraction violation of these local constraints.

Our main contribution in this work is to establish the existence of NLETS Hamiltonians by providing an explicit construction of an infinite family of such Hamiltonians:

Theorem 5. ***Explicit NLETS*** *There exists constants $\varepsilon = 10^{-8}, a, b > 0$ and an explicit infinite family of Hamiltonians $\{H_n\}_n$, each of the form:*

$$H_n = \frac{1}{m}\sum_{i=1}^{m} \frac{I + P_i}{2}, \tag{1}$$

for P_i equal to ± 1 times a tensor product of Pauli matrices on 16 qubits and identity elsewhere. These Hamiltonians have the property that

- *There exists a state $|\phi_n\rangle$ such that $H_n|\phi_n\rangle = 0$.*

[1] This, by choosing states that are tensor-product of states, that each satisfy a small disjoint box from the grid. Analogously, a CSP defined on a d-regular grid can be approximated in P for any $\varepsilon > 0$.

- *For any ε-impostor ρ_n for H_n and any quantum circuit U_n of depth at most $d = b \cdot \log(n)$, we have*

$$\|\rho_n - U_n \left|0^{\otimes n}\right\rangle \left\langle 0^{\otimes n}\right| U_n^\dagger\|_1 > n^{-a}. \tag{2}$$

A. Outline of the Construction

Our construction is a local Hamiltonian on n qubits for which any ε-impostor, for some constant $\varepsilon > 0$ must be highly entangled - indeed it must entangle a number of qubits that is $n^{\Omega(1)}$. Since local Hamiltonians such as the toric code embedded on low-dimensional grids are not NLETS, a key to this construction is to use an expanding geometry. This approach was taken also recently in the construction of quantum codes from high-dimensional manifolds [8]. Our local Hamiltonian can be seen as a "toric code" which instead of being a certain (hyper-)graph product of two 1-dimensional cycles, is the product of two expander graphs. The graph product we refer to is a variant of the Homological product [9] which was elegantly characterized by Tillich and Zémor [2], leading to improved quantum error-correcting codes.

By specifying a toric-code type quantum error-correcting code whose underlying topology is a *robust* local topology (albeit not spatially local) we are able to show the existence of *robust* entanglement. This implies that our intuition that quantum entanglement is fragile may be no more than an artifact of considering local Hamiltonian systems that are spatially local.

B. Proof outline

To show a robust circuit lower bound for impostors of our expander-based toric code we define a "complexity witness", i.e. a simple-to-verify property that can prove a state is nontrivial. Suppose we measure a trivial state in a product basis and thereby obtain some probability distribution p over $\mathbb{F}_2^n$. Our complexity witness is the fact that p should have high vertex expansion, meaning that any $S \subset \mathbb{F}_2^n$ with $p(S) \leq 1/2$ should have an $\Omega(1)$ fraction of its mass on points near its boundary. In particular, let $\delta_\ell(S) \subseteq \mathbb{F}_2^n$ denote the points within Hamming distance ℓ of the boundary of S (see Section V for precise definition). Then the p-weighted vertex expansion is defined to be

$$h_\ell(p) := \min_{S, 0 < p(S) \leq \frac{1}{2}} \frac{p(\delta_\ell(S))}{p(S)}. \tag{3}$$

It is well known that the uniform measure on $\mathbb{F}_2^n$, or indeed any product measure, has good expansion properties (as we will quantify in Section V). It is not hard to see this is also true for the output of low-depth classical circuits. We extend this to quantum circuits, by using Chebyshev polynomials in a way inspired by [10], [11].

Theorem 6. *Let $N \geq n > 0$ be some integers, and $|\psi\rangle = U|0^N\rangle$ for U a circuit of depth d. Let p be the probability distribution that results from measuring the first n qubits in the computational basis; i.e.*

$$p(x) = \sum_{y \in \{0,1\}^{N-n}} |\langle x, y|\psi\rangle|^2. \tag{4}$$

Then for any $\ell \geq \alpha\sqrt{n}2^{1.5d} \geq 1$ with $\alpha \leq 1$, we have:

$$h_\ell(p) \geq \alpha^2/8 \tag{5}$$

We refer to non-expanding distributions as "approximately partitioned"; meaning that we can identify two well separated subsets S_0, S_1 each with large probability measure. A prototypical example of a state giving rise to an approximately partitioned distribution is the so-called "cat-state" $(|0^n\rangle + |1^n\rangle)/\sqrt{2}$. However, the cat state is not the unique ground state of any local Hamiltonian [12], so it is not a good candidate for an NLETS system. Another possibility is the uniform distribution of any (classical) code with large minimal distance, since it is also approximately partitioned. However, simply using the check operators of a classical code is insufficient since any product string state corresponding to a single code-word would pass this test, but is obviously a trivial state.

An example of a state which is both approximately partitioned *and* locally checkable is a state of a quantum error correcting code (QECC) with low-weight generators. QECCs protect quantum information by encoding a given Hilbert space into a larger Hilbert space in a non-local fashion, so they are natural candidates for creating robust forms of entanglement. We will show in Section VI the "warm-up" result that Hamiltonians corresponding to a special subclass of QECCs (namely CSS codes) have no *zero*-energy trivial states. (This claim was previously shown in [13], [14] but we present the proof using similar tools to the later proof of our main result.) Since we consider only local Hamiltonians then it is necessary to restrict to codes with low-weight check operators, also known as LPDC (low-density parity-check) codes.

Finally, in section VIII we show that for the hypergraph product of two expander graphs, the resulting code has the property that such complexity witnesses can be produced not only for the ground state but for any ε-impostor, even for constant $\varepsilon > 0$. Essentially, we leverage the robust connectivity of the expander graph under taking sub-graphs to prove that any such impostor is approximately partitioned as a distribution when measured in some tensor-product basis.

C. Discussion and Open Questions

We have established a first example where a locally defined, though not spatially local, quantum system gives rise to a robust form of quantum entanglement. Not only is its ground state highly entangled in a rigorous sense of the circuit lower bound, but this lower bound carries over for any quantum state that resembles a ground state on most qubits.

As stated above, this condition is necessary, for example for the quantum LDPC (qLDPC) conjecture. This conjecture posits the existence of quantum codes with local checks, linear minimal distance and non-zero rate. To see why NLETS is necessary for qLDPC suppose that C is such a qLDPC on n qubits, and it has minimal distance $\delta_{\min} n$. Thus if we remove an arbitrary $\delta_{\min} n/2$ qubits then we are left with a code with distance $\geq \delta_{\min} n/2$. By Proposition 24 the resulting states are nontrivial.

In addition, NLETS is a necessary condition for the NLTS conjecture [1]. This conjecture posits the existence of local Hamiltonians for which any low-energy state is non-trivial - i.e. any $|\psi\rangle$ such that $\mathrm{tr}(H|\psi\rangle\langle\psi|) < \varepsilon m$ (where m is the number of local terms) is not d-trivial for all $d = O(1)$. To see why NLETS is necessary for NLTS it is sufficient to observe that under a very mild regularity condition on the Hamiltonian, a quantum state that is an ε impostor of a local Hamiltonian H is in particular a low-energy state of H, with energy at most $K\varepsilon$ for some constant K.

Thus, in this respect, our work makes progress on these two important conjectures, and hence also establishes a new necessary condition for the qPCP conjecture. That said, our robustness results imply that quantum entanglement is robust, but does not show that *useful* quantum entanglement is robust. Showing a robust version of entanglement that is computationally useful is analogous to proving an adversarial version of the fault-tolerant threshold theorem for BQP.

Beyond quantum complexity, we believe that our idea of using vertex expansion as an entanglement witness could have further applications.

II. Preliminary facts and definitions

A. Quantum codes and local Hamiltonians

Definition 7. ***Pauli operators***

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{6}$$

For $e \in \mathbb{F}_2^n$, define $X^e = X^{e_1} \otimes X^{e_2} \otimes \cdots \otimes X^{e_n}$, i.e. the tensor product of X operators in each position where $e_i = 1$; similarly define $Z^e = \bigotimes_i Z^{e_i}$.

Definition 8. ***CSS code***
A $[[n,k,d]]$ quantum CSS (Calderbank-Shor-Steane) code on n qubits is a subspace $\mathcal{C} \subseteq \mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ of n qubits. It is defined by a pair of linear subspaces of $S_x, S_z \subseteq \mathbb{F}_2^n$ such that $S_x \perp S_z$. It is thus denoted $\mathcal{C} = \mathcal{C}(S_x, S_z)$. Explicitly the subspace is given by

$$\mathcal{C}(S_x, S_z) = \mathrm{Span}\left\{ \frac{1}{\sqrt{|S_x|}} \sum_{x \in S_x} |z + x\rangle : z \in S_z^{\perp} \right\}. \tag{7}$$

The code has $k = \log(|S_x^{\perp}/S_z|)$ logical qubits and distance $d = \min_{w \in S_x^{\perp} - S_z, S_z^{\perp} - S_x} |w|$.

The spaces of logical X, Z operators are respectively defined by the quotient spaces $S_z^{\perp}/S_x, S_x^{\perp}/S_z$. The logical X, Z operators that perform non-identity operations (also known as non-trivial logical operators) are given by $S_z^{\perp} - S_x$,$S_x^{\perp} - S_z$, respectively.

Definition 9. ***The Hamiltonian of a CSS code***
Suppose $\mathcal{C} = \mathcal{C}(S_x, S_z)$ is a CSS code and H_x, H_z are subsets of $\mathbb{F}_2^n$ that generate S_x, S_z. Then we can define a Hamiltonian $H(\mathcal{C})$, whose terms correspond to the generators of the CSS code in the following way.

$$H(\mathcal{C}) = \frac{1}{2|H_x|} \sum_{e \in H_x} \frac{I + X^e}{2} + \frac{1}{2|H_z|} \sum_{e \in H_z} \frac{I + Z^e}{2}. \tag{8}$$

Observe that the CSS condition $S_x \perp S_z$ implies that the terms of $H(\mathcal{C})$ all commute. Thus the ground subspace of $H(\mathcal{C})$ is precisely the codespace $\mathcal{C}$. Moreover, if the generating sets H_x, H_z contain only terms with weight $\leq k$ then the corresponding Hamiltonian $H(\mathcal{C})$ is a k-local Hamiltonian.

B. Locally Testable Codes

Definition 10. ***Classical locally testable code***
A code $C \subseteq \mathbb{F}_2^n$ is said to be locally testable with soundness ρ and query q, if there exists a set of q-local check terms $\{C_1, \ldots, C_m\}$, such that

$$\mathrm{Prob}_{i \sim U[m]}\left[C_i(w) = 1\right] \geq \rho \cdot \frac{\mathrm{dist}(w, C)}{n}.$$

In particular $w \in C$ iff $C_i(w) = 0$ for all i.

We now present a slight re-wording of the definition of LTC which would be useful later on:

Fact 11. ***The words of a residual LTC cluster around the original code***
Let C be a locally testable code with parameter ρ. Any word w that violates a fraction at most ε of the checks of C is at fractional distance at most ε/ρ from C.

C. Expander Graphs

The term "expander" (or more precisely "edge expander") refers to the fact that for a not-too-large subsets S of vertices a large fraction of the edges incident upon S leave S. (Later we also discuss *vertex* expansion.) Define the Cheeger constant of a graph G to be

$$h(G) = \min_{S \subseteq [n], 0 < |S| \leq n/2} \frac{|\partial(S)|}{|S|}, \qquad (9)$$

where $\partial(S)$ is the set of edges with one point in S and one in $V - S$.

Definition 12. ***Expander Graphs*** *A family of d-regular graphs $\{G_n\}_n$ is said to be expanding, if there exists a number $h > 0$ such that $h(G_n) \geq h$ for all sufficiently large n.*

In the full paper [15] we explain the standard fact that for any constant $c > 0$ infinite families $\{G_n\}$ of expander graphs exist with $h(G_n) \geq c$ and with degree upper-bounded by a constant depending only on c. We will specifically need $h(G_n) \geq 3$ which can be achieved by 14-regular graphs, as we explain in [15] using standard arguments.

Expander graphs of bounded-degree give rise naturally to *locally testable codes* (LTCs) as follows. Given an expander graph $G = (V, E)$ we define the following code $C(G)$. It is the repetition code on $|V|$ bits, with equality constraints of the form $x_i \oplus x_j = 0$ for all $(i, j) \in E$. One can easily check that this code $C(G)$ is locally testable with query size $q = 2$ and soundness $\rho = 2h(G)/d$.

In this paper we require a slightly more robust version of this fact where we allow the adversarial removal of a small fraction of the vertices and edges.

Definition 13. ***Maximal-connected residual graph*** *Let $G = (V, E)$, and subsets $V_\varepsilon \subseteq V, E_\varepsilon \subseteq E$. A connected residual graph of G w.r.t. these sets is a graph $G' = (V', E')$ where $V' \subseteq V_\varepsilon, E' \subseteq E_\varepsilon$ such that $G' = (V', E')$ is connected. A maximal-connected residual graph G_ε is a connected residual graph of maximal size $|V'|$.*

In the full paper [15, Cor 17] we prove

Proposition 14. *Consider the maximal connected residual graph G_ε above. For all $d \geq 14$, and $w \in \mathbb{F}_2^{V'}$ we have the following holds:*

$$620\varepsilon \leq \frac{|w|}{|V'|} \leq \frac{1}{2} \quad \Rightarrow \quad |\partial_{G_\varepsilon} w| \geq 3|w|. \qquad (10)$$

III. Local Hamiltonians with Approximation-Robust Entanglement

Our main result will be stated in terms of hard-to-approximate classical probability distributions as follows. Recall that QNC^1 is the set of languages computable in quantum bounded-error log depth. We will use the term to describe classical distributions that can be approximately simulated with a quantum log-depth circuit.

Definition 15. QNC^1***-hard distribution***
A family of distributions $\{\mathcal{D}_n\}$ on n bits is said to be QNC^1-hard if there exist constants $a, c > 0$ such that for sufficiently large n any n-qubit depth-$c \cdot \log(n)$ trivial state ρ_n satisfies

$$\|\mathcal{D}_n - \mathrm{diag}(\rho_n)\|_1 = \Omega(n^{-a}). \qquad (11)$$

Here $\mathrm{diag}(\rho)$ can be thought of as the probability distribution resulting from measuring ρ in the computational basis. Next, we define quantum states as QNC^1-hard if the classical distribution induced by their measurement is hard to simulate quantumly:

Definition 16. QNC^1***-hard quantum states***
A family of n-qubit quantum states $\mathcal{F} = \{\rho_n\}_n$ is said to be QNC^1-hard if for some tensor product measurement the output distribution is QNC^1-hard.

Now, we can define local Hamiltonians as QNC^1-hard if their ground states are QNC^1-hard:

Definition 17. QNC^1***-hard local Hamiltonian***
A family of local Hamiltonians $\{H_n\}_n$ is said to be QNC^1-hard if any family of states $\mathcal{F} = \{\rho_n\}_n$, with $\rho_n \in \ker(H_n)$ is QNC^1-hard.

As the final step we define a robust version thereof where we ask that even ground-state *impostors* are hard:

Definition 18. QNC^1***-robust local Hamiltonian***
A family of local Hamiltonians $\{H_n\}$ is QNC^1-robust if there exists $\varepsilon > 0$ such that any family $\mathcal{F} = \{\rho_n\}_n$,

where ρ_n is an ε-impostor of H_n for all sufficiently large n, is QNC^1*-hard.*

Using these definitions our main result (Theorem 5) states that there exists a family of $O(1)$-local Hamiltonians that is QNC^1-robust. Most of the remainder of the paper is devoted to the proof of this result (Theorem 5). In Section V we will prove that the probability distributions resulting from low-depth circuits cannot be approximately partitioned.

Then we will show that the distribution resulting from measuring quantum code-states *can* be approximately partitioned. The canonical example of such a partition is the cat state, as we mentioned in the introduction, and indeed it is well known that the cat state cannot be prepared in sub-logarithmic depth. In Section VI we will prove a "warm-up" result showing that any Hamiltonian corresponding to a CSS code with $n^{\frac{1}{2}+\Omega(1)}$ distance is QNC^1-hard, although they may generally not be QNC^1-robust.

IV. The Uncertainty Lemma and Noisy Quantum Code-States

We next present a version of the classic uncertainty principle [16] that implies that if two logical operators of a CSS codes anti-commute any state must have a high uncertainty (i.e. variance) in at least one of these operators. This "sum" version is due to Hoffman and Takeuchi [17].

Lemma 19. *Let $|\psi\rangle$ be a quantum state, and A, B Hermitian observables satisfying $AB + BA = 0$ and $A^2 = B^2 = I$. Define*

$$\Delta A^2 = \langle\psi|A^2|\psi\rangle - \langle\psi|A|\psi\rangle^2.$$

Then

$$\Delta A^2 + \Delta B^2 \geq 1. \tag{12}$$

See [15] for the proof.

Next, we require a simple fact that any CSS code has a pair of bases, one for each of the kernels $S_x^\perp, S_z^\perp$. The proof can be found for example in [18].

Fact 20. ***Anti-commuting logical operators***
Let $\mathcal{C}$ be a $[[n, k, d]]$-CSS code: $\mathcal{C} = \mathcal{C}(S_x, S_z)$. There exist sets

$$\mathcal{B}_x = \{b_1^x, \ldots, b_k^x\} \subset S_z^\perp \tag{13a}$$

$$\mathcal{B}_z = \{b_1^z, \ldots, b_k^z\} \subset S_x^\perp \tag{13b}$$

such that $\{b_i^x + S_x\}_{i\in[k]}$ and $\{b_i^z + S_z\}_{i\in[k]}$ are bases for $S_z^\perp$ and $S_x^\perp$ respectively and

$$\langle b_i^x, b_j^z\rangle = \delta_{i,j}. \tag{14}$$

Readers acquainted with quantum codes should think of $\{X^{b_i^x}\}$ and $\{Z^{b_i^z}\}$ as logical X and Z operators.

One useful property of CSS codes is that the value of the logical operators can be read off from measuring each qubit individually. If we measure a code state of $\mathcal{C}(S_x, S_z)$ in the Z (resp. X) basis then the outcomes will always lie in $S_z^\perp$ (resp. $S_x^\perp$). The $+1/-1$ eigenvalues of the first logical Z operator $Z^{b_1^z}$ correspond to the outcomes $S_z^\perp \cap (b_1^z)^\perp$ and $b_1^x + S_z^\perp \cap (b_1^z)^\perp$ when measuring each qubit in the Z basis. Observe also that $S_z^\perp \cap (b_1^z)^\perp = (S_z \cup b_1^z)^\perp = S_x + \mathrm{Span}(\mathcal{B}_x - b_1^x)$. Let us define accordingly the sets

$$C_0^Z = (S_z \cup b_1^z)^\perp \qquad C_1^Z = b_1^x + C_0^Z \tag{15a}$$

$$C_0^X = (S_x \cup b_1^x)^\perp \qquad C_1^X = b_1^z + C_0^X \tag{15b}$$

The sets C_0^Z, C_1^Z (resp. C_0^X, C_1^X) partition $S_z^\perp$ (resp. $S_x^\perp$). Let $\mathcal{D}_\psi^Z$ (resp. $\mathcal{D}_\psi^X$) denote the distribution on $\mathbb{F}_2^n$ induced by measuring $|\psi\rangle$ in the tensor Z basis (resp. the tensor X basis), and define $\langle M\rangle := \langle\psi|M|\psi\rangle$ for any operator M. The above discussion implies that if $|\psi\rangle \in \mathcal{C}$ then

$$\left\langle Z^{b_1^z}\right\rangle = \mathcal{D}_\psi^Z(C_0^Z) - \mathcal{D}_\psi^Z(C_1^Z) \tag{16a}$$

$$\left\langle X^{b_1^x}\right\rangle = \mathcal{D}_\psi^X(C_0^X) - \mathcal{D}_\psi^X(C_1^X) \tag{16b}$$

Next we argue that uncertainty in the logical operators translates into uncertainty of measurement outcomes in either the X or Z product basis.

Proposition 21. ***Uncertainty for code-states in at least one basis***
Let (S_x, S_z) be a CSS code with $\mathcal{B}_x, \mathcal{B}_z$ as in Fact 20. Let $|\psi\rangle$ be a quantum code-state, and D_ψ^X, D_ψ^Z be the distribution of the measurement of $|\psi\rangle$ in the Pauli-X or Pauli-Z basis, respectively. Then at least one of the following equations must hold:

$$D_\psi^Z(C_0^Z) \in \left[\frac{1}{2} - \frac{1}{2\sqrt{2}}, \frac{1}{2} + \frac{1}{2\sqrt{2}}\right] \tag{17a}$$

$$D_\psi^X(C_0^X) \in \left[\frac{1}{2} - \frac{1}{2\sqrt{2}}, \frac{1}{2} + \frac{1}{2\sqrt{2}}\right] \tag{17b}$$

Since $D_\psi^P(C_0^P) + D_\psi^P(C_1^P) = 1$ for $P = X, Z$ we could equivalently state (17) in terms of C_1^Z and C_1^X.

Proof: According to Lemma 19 any state $|\psi\rangle$ will have

$$1 \leq (\Delta X^{b_1^x})^2 + (\Delta Z^{b_1^z})^2 = 2 - \left\langle X^{b_1^x} \right\rangle^2 - \left\langle Z^{b_1^z} \right\rangle^2 .$$

and therefore either $|\left\langle X^{b_1^x} \right\rangle|$ or $|\left\langle Z^{b_1^z} \right\rangle|$ must be $\leq 1/\sqrt{2}$. Assume w.l.o.g. (since the other case is similar) that

$$\left|\left\langle Z^{b_1^z} \right\rangle\right| \leq 1/\sqrt{2}. \tag{18}$$

The result now follows from (16).

■

In this paper, we will mostly consider noisy code-states, and not actual code-states. We will want to argue that even noisy code-states have an uncertainty property w.r.t. the original logical operators. To do we will define partitions (analogous to Voronoi cells in geometry) which correspond to maximum-likelihood decoding of measurement outcomes in the X and Z bases.

Proposition 22. ***Generalized uncertainty for unitary decoding***
Let $\mathcal{C} = (S_x, S_z)$ be a $[[n,k,d]]$-CSS code and $C_0^Z, C_1^Z, C_0^X, C_1^X$ are defined as in (15). Let E_x, E_z be some set of errors that satisfies:

$$\tilde{C}_0^Z := C_0^Z + E_z \tag{19a}$$

$$\tilde{C}_1^Z := C_1^Z + E_z \tag{19b}$$

$$\tilde{C}_0^Z \cap \tilde{C}_1^Z = \emptyset \tag{19c}$$

and similarly this holds for the sets $\tilde{C}_0^X, \tilde{C}_1^X$, defined in the same way w.r.t. E_x. Suppose further that

$$\operatorname{supp}(D_\psi^Z) \subseteq \tilde{C}_0^Z \cup \tilde{C}_1^Z \text{ and } \operatorname{supp}(D_\psi^X) \subseteq \tilde{C}_0^X \cup \tilde{C}_1^X$$

Then there exists a constant $c_0 > 0.07$ such that

$$\begin{aligned}(D_\psi^Z(\tilde{C}_0^Z) \geq c_0 \quad &\text{and} \quad D_\psi^Z(\tilde{C}_1^Z) \geq c_0) \text{ or} \\ (D_\psi^X(\tilde{C}_0^X) \geq c_0 \quad &\text{and} \quad D_\psi^X(\tilde{C}_1^X) \geq c_0).\end{aligned} \tag{20}$$

V. Vertex expansion bounds for low-depth circuits

As stated above, a central notion of this paper (following Lovett and Viola [19]) is that distributions over codewords of good codes look very different from the outputs of low-depth circuits. We will see in this section that these can be distinguished by comparing the different values of vertex expansion that they induce on a particular graph.

Consider $\mathbb{F}_2^n$ to be the vertices of a graph with an edge between all pairs x, y with $\operatorname{dist}(x,y) \leq \ell$. If $\ell = 1$ then this is the usual hypercube, but we will be interested in $\ell \approx \sqrt{n}$. For a set $S \subseteq \mathbb{F}_2^n$ define $\delta_\ell(S)$ to be the boundary of S , meaning points in S connected by an edge to a point in $S^c := \mathbb{F}_2^n - S$, along with points in S^c connected to a point in S. In other words

$$\begin{aligned}\delta_\ell(S) = \{x \in S : \exists y \in S^c, |x-y| \leq \ell\} \\ \cup \{x \in S^c : \exists y \in S, |x-y| \leq \ell\}.\end{aligned} \tag{21}$$

Let p be a probability distribution over $\mathbb{F}_2^n$. The p-weighted vertex expansion is defined to be

$$h_\ell(p) := \min_{S, 0 < p(S) \leq \frac{1}{2}} \frac{p(\delta_\ell(S))}{p(S)}. \tag{22}$$

In this section we argue that the outputs of low-depth circuits have high vertex expansion for $\ell = \Omega(\sqrt{n})$. To get intuition for this, we consider first the case of the uniform distribution over $\mathbb{F}_2^n$. Here Harper's Theorem [20] implies that $h_\ell(U[\mathbb{F}_2^n])$ is $\Omega(1)$ when $\ell = \Omega(\sqrt{n})$.

This can be extended to the case when p is the output of a classical depth-d circuit $C : \{0,1\}^m \mapsto \mathbb{F}_2^n$ which accepts m uniformly random input bits and has fan-in, fan-out both ≤ 2. In this case each output bit depends on at most 2^d bits. Let $S \subset \mathbb{F}_2^n$, $T = C^{-1}(S) \subseteq \{0,1\}^m$, and $p = U[\mathbb{F}_2^m]$. Since the output can depend on at most $n2^d$ bits of the input, we can assume without loss of generality that $n \leq m \leq n2^d$, or if d is constant then $m = \Theta(n)$. By Harper's Theorem, since $p(T) \leq 1/2$, and by assumption$x$ is drawn uniformly from T, then with probability $\Omega(1)$ there exists a z with $|z| \leq \sqrt{m}$ and $x + z \in T^c$. Now we can use the assumption that the circuit is low depth to argue that

$$\operatorname{dist}(C(x), C(x+z)) \leq |z| 2^d \leq \sqrt{m} 2^d \leq \sqrt{n} 2^{1.5d}. \tag{23}$$

Since $C(x) \in S$ and $C(x+z) \in S^c$ this implies that $C(x) \in \delta_\ell(S)$ with $\ell = \sqrt{n}2^{1.5d}$. We conclude that $h_\ell(p) = \Omega(1)$.

The main result of this section is that a similar bound also holds for the output of low-depth *quantum* circuits, as we have stated earlier in Theorem 6.

Our proof is inspired by the use of Chebyshev polynomials by Friedman and Tillich [10] to relate the diameter of a graph to the spectral gap of its adjacency matrix, as well as by [11] to show that ground states of 1-d gapped Hamiltonians have bounded entanglement.

The idea of the proof is that the output of a depth-d quantum circuit is also the ground state of a 2^d-local Hamiltonian with minimal non-zero eigenvalue at least $1/n2^d$. Using a Chebyshev polynomial of degree $\alpha\sqrt{n2^d}$ (for $0 < \alpha \leq 1$) this minimal non-zero eigenvalue can be amplified to $\Omega(\alpha^2)$ while blowing up the locality to at most $\alpha\sqrt{2}2^{1.5d}$. If the ground state had low expansion at this Hamming distance, then we could construct an orthogonal state with only slightly higher energy, contradicting our known lower bound on the gap. Details of this argument are in [15].

An easy corollary implies that outputs of low depth circuits cannot have $\Omega(1)$ probability mass in two sets with distance significantly larger than $O(\sqrt{n}2^{1.5d})$.

Corollary 23. *Suppose p is a probability distribution on $\{0,1\}^n$ resulting from the output of a depth-d quantum circuit and $S_1, S_2 \subset \{0,1\}^n$ such that $p(S_1), p(S_2) \geq \mu$. Then*

$$d \geq \frac{2}{3}\log\left(\frac{\mu \cdot dist(S_1, S_2)}{4\sqrt{n}}\right). \tag{24}$$

VI. Warm-up: Quantum CSS Code-States are QNC^1-hard

Circuit lower bounds for generating quantum code states *exactly* can be readily derived from the local indistinguishability property. In this section, we show that our techniques can be used to derive a robust version of this property, which is that quantum CSS codes cannot be approximated by bounded-depth quantum circuits, even up to constant l_2 error. This result was previously proven by Bravyi, Hastings and Verstraete [21], but we redo it with our methods since they will be used in similar ways in the proof of our main result.

The claims in this section demonstrate our techniques by improving the approximation bounds on perfect code-states from 0 error to constant l_2 error. Notably, even such a hardness-of-approximation claim is by no means robust, because we still consider approximation of *perfect* ground states of the code Hamiltonian. In other words, while a code-state is QNC$_1$-hard, not every ε-impostor of a code-state is QNC$_1$-hard (we return to ε-impostors later). In fact, many constructions of quantum CSS codes are known to be *not* QNC$_1$-robust: i.e. one can find ε-impostors of such codes that are trivial - like in the case where the code is defined on a regular d-dimensional grid for $d = O(1)$.

Proposition 24. ***Code-states of quantum CSS codes with large distance are* QNC^1*-hard***
Let $\mathcal{C} = [[n, k, \Delta_{\min}]]$ be a quantum CSS code. Preparing any $|\psi\rangle \in \mathcal{C}$ up to l_2 error at most 0.14 requires depth $\Omega(\log(\Delta_{\min}/\sqrt{n}))$. In particular, if $\Delta_{\min} \geq n^{1/2+\Omega(1)}$ then $|\psi\rangle$ is QNC^1*-hard.*

Proof of Proposition 24: Let $|\psi\rangle$ be some code-state of $\mathcal{C}$. By Fact 20 above, one can find bases $\mathcal{B}_x, \mathcal{B}_z$ satisfying (14). Choose, say, the first pair $b^x := b_1^x \in \mathcal{B}_x$, $b^z := b_1^z \in \mathcal{B}_z$.

Let C_0 denote the linear space $C_0 = S_z^\perp \cap (b^z)^\perp \subset \mathbf{F}_2^n$, and define the affine space $C_1 = C_0 + b^x$. If $s_0 \in C_0, s_1 \in C_1$ then $s_0 + s_1 \in C_1 \subseteq S_z^\perp - S_x$, implying that $|s_0 + s_1| \geq \Delta_{\min}$, and so

$$\mathrm{dist}(C_0, C_1) \geq \Delta_{\min}. \tag{25}$$

Let $\mathcal{D}_\psi^Z$ denote the distribution on $\mathbb{F}_2^n$ induced by measuring $|\psi\rangle$ in the tensor Z basis. Then by Proposition 21 we either have

$$\mathcal{D}_\psi^Z(C_0) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} \text{ and } \mathcal{D}_\psi^Z(C_1) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}}, \tag{26}$$

or a similar statement holds for measuring in the X basis. WLOG assume that (26) holds. Thus $\mathcal{D}_\psi^Z$ is approximately partitioned with measure at least $\mu = \frac{1}{2} - \frac{1}{2\sqrt{2}}$ and distance $\Delta_{\min}$. Hence, any distribution p that is ε-close to $\mathcal{D}_\psi^Z$ for $\varepsilon < \mu$ is $(\mu - \varepsilon, \Delta_{\min})$-approximately partitioned. Therefore, by Corollary 23 (and specifically (24)) producing $|\psi\rangle$ to error ε requires depth

$$\geq \frac{2}{3}\log\left(\frac{(\mu - \varepsilon)\Delta_{\min}}{4\sqrt{n}}\right). \tag{27}$$

Since $\mu \geq 0.142\ldots$, if we take $\varepsilon = 0.14$ then this implies a depth lower bound of $\frac{2}{3}\log\frac{\Delta_{\min}}{\sqrt{n}} - O(1)$. If $\Delta_{\min} = n^{1/2+\Omega(1)}$ then this bound is $\Omega(\log n)$ and so $|\psi\rangle$ is QNC^1-hard. ∎

Implications for known quantum codes: Proposition 24 provides a nontrivial quantum circuit lower bound on the quantum LDPC codes due to [22]. These codes are CSS codes and have distance $\Omega(\sqrt{n\log(n)})$ which corresponds to a circuit depth lower bound of $\Omega(\log\log(n))$. Notably, our result applies also for codes with just inverse polynomial distance like the toric code:

Proposition 25. *Let $\mathcal{C} = [[n, k, \Delta_{\min}]]$ be a quantum CSS code with $\Delta_{\min} \geq n^\alpha$ for $\alpha > 0$ and $k \geq 1$. If $|\psi\rangle \in \mathcal{C}$ and $\|\rho - |\psi\rangle\langle\psi|\| \leq n^{-1-\beta}$ for $\beta > 0$ then preparing ρ requires depth $\Omega(\log(n))$.*

The proof can be found in [15].

We note that other methods are known [13], [14], [23] for showing that QECC ground states, and even low-temperature thermal states of the 4-d toric code [24], are nontrivial. Indeed our proof can be viewed as a certain way of generalizing the argument of [13].

VII. The Hypergraph Product

A. General

In this section, we survey the hypergraph product due to Tillich-Zémor [2]. We provide here only the very basic definitions that are required to prove our main theorem, and refer the reader to the original paper [2] for an in-depth view. The hypergraph-product code takes in two classical codes defined by their Tanner constraint graphs and generates a product of these codes as hypergraphs. Then it attaches a CSS code to the product graph. Formally stated:

Definition 26. ***The Hypergraph Product***
Let $(V_1, E_1), (V_2, E_2)$ be two constraint hypergraphs with corresponding edge-vertex incidence operators ∂_1, ∂_2 and codes $\mathcal{C}_1 = \ker \partial_1, \mathcal{C}_2 = \ker \partial_2$. Then the Tillich-Zémor hypergraph product of these codes, denoted by

$$\mathcal{C}_\times = \mathcal{C}_1 \times_{TZ} \mathcal{C}_2, \tag{28}$$

is defined by the hypergraph product of the corresponding graphs. Specifically, its Hilbert space is comprised of qubits corresponding to

$$(V_1 \times V_2) \cup (E_1 \times E_2),$$

and check matrices are

$$H_x = \left(\partial_1 \otimes I_{V_2} \middle| I_{E_1} \otimes \partial_2^T\right) \qquad H_z = \left(I_{V_1} \otimes \partial_2 \middle| \partial_1^T \otimes I_{E_2}\right) \tag{29}$$

These matrices have rows indexed by qubits and columns indexed by checks. The X constraints, for example, are labeled by elements of $E_1 \times V_2$, with constraint (e_1, v_2) is connected to all elements $(u, v_2) \in V_1 \times V_2$ for $u \in \partial^T e_1$ and also to all elements $(e_1, f) \in E_1 \times E_2$ for $f \in \partial v_2$. (Here we view $\partial^T e_1, \partial v_2$ equivalently both as vectors in $\mathbb{F}_2^{V_1}, \mathbb{F}_2^{E_2}$ respectively and as subsets of V_1, E_2.) It follows from this definition that $\mathcal{C}_\times$ is a CSS code $\mathcal{C}_\times(S_x, S_z)$, where as usual $S_x = \operatorname{Im} H_x$ and $S_z = \operatorname{Im} H_z$. For $|V_1| = n_1, |V_2| = n_2, |E_1| = m_1, |E_2| = m_2$, the code $\mathcal{C}_\times$ is a quantum CSS code on $n_1 n_2 + m_1 m_2$ qubits, with $n_1 m_2 + n_2 m_1$ local checks. One can check that $\mathcal{C}_\times$ is determined only by $\mathcal{C}_1, \mathcal{C}_2$ and not the specific choices of ∂_1, ∂_2, so (28) is well defined.

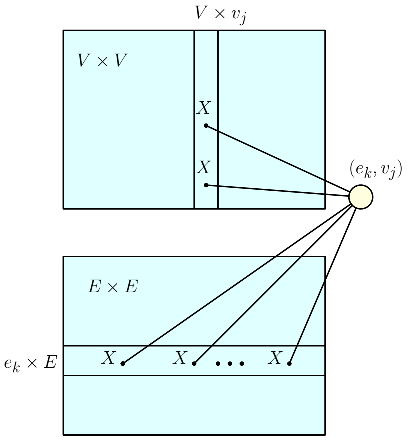

Figure 1. An example of a check term (e_k, v_j) of H_x. It is a parity check on all bits (v_m, v_j) in the j-th column of $V \times V$ such that v_m is examined by e_k in the original code $\mathcal{C}$, and on all bits in the k-th row of $E \times E$ that corresponds to checks incident on v_j in $\mathcal{C}$. If we specialize to the case when $\mathcal{C}$ is the repetition code with checks corresponding to a d-local graph (as in Section VII-C) then each check examines two bits in the $V \times V$ block and d bits in the $E \times E$ block.

We now state several useful facts on this construction, which can all be found in [2]:

Fact 27. ***Basic Properties of the hypergraph product*** *[2]*

1) *If C_1, C_2 have locality parameters l_1, l_2, l_1^T, l_2^T, respectively, (l_i^T is the maximum number of checks incident upon any bit in code C_i) then $\mathcal{C}_\times$ has locality parameter $l_1 + l_2^T$ for H_x, and $l_2 + l_1^T$ for H_z.*
2) $\delta_{\min}(\mathcal{C}_\times) \geq \min\left\{\delta_{\min}(\mathcal{C}_1), \delta_{\min}(\mathcal{C}_2), \delta_{\min}(\mathcal{C}_1^T), \delta_{\min}(\mathcal{C}_2^T)\right\}$
3) *Let $r(\mathcal{C})$ denote the number of qubits in a code $\mathcal{C}$. Then $r(\mathcal{C}_\times) = r(\mathcal{C}_1) \cdot r(\mathcal{C}_2) + r(\mathcal{C}_1^T) \cdot r(\mathcal{C}_2^T)$.*

These logical operators of $\mathcal{C}_\times$ can assume very complex forms, due in part, to the fact that the rate of the code scales like $r(\mathcal{C}_1) \cdot r(\mathcal{C}_2)$. Hence, the hypergraph product of codes with linear rate is linear itself, i.e. scales like $\Omega(|V|^2)$.

B. Column-wise logical operators

A particularly interesting subset of the logical operators, which is a subgroup w.r.t. addition modulo $\mathbb{F}_2$, has a very succinct and useful form. We exploit the structure of this group to inherit, in some sense, the classical property of local testability.

Fact 28. ***Group of logical operators isomorphic to the original code***

For any $x \in \mathcal{C}_1$, and $y \notin \mathcal{C}_2^{\perp}$, the word

$$\left((x \otimes y)_{V_1 \times V_2}, \mathbf{0}_{E_1 \times E_2}\right) \in S_x^{\perp} - S_z \tag{30}$$

Similarly, for $x \notin \mathcal{C}_1^{\perp}, y \in \mathcal{C}_2$,

$$\left((x \otimes y)_{V_1 \times V_2}, \mathbf{0}_{E_1 \times E_2}\right) \in S_z^{\perp} - S_x. \tag{31}$$

One can also show that

$$(\mathbf{0}_{V_1 \times V_2}, \mathcal{C}_2^T \otimes (\mathcal{C}_1^{T\perp})^c) \subset S_x^{\perp} - S_z \tag{32a}$$

$$(\mathbf{0}_{V_1 \times V_2}, (\mathcal{C}_2^{T\perp})^c \otimes \mathcal{C}_1^T) \subset S_z^{\perp} - S_x \tag{32b}$$

In particular, if $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_1^T, \mathcal{C}_2^T$ are linear codes in which each bit appears at least once as 0 and once as 1 in some non-zero word, then

$$\left((\mathcal{C}_1 \otimes \mathbb{F}_2^{V_2})_{V_1 \times V_2}, \mathbf{0}_{E_1 \times E_2}\right) \subset S_x^{\perp} - S_z \tag{33a}$$

$$\left((\mathbb{F}_2^{V_1} \otimes \mathcal{C}_2)_{V_1 \times V_2}, \mathbf{0}_{E_1 \times E_2}\right) \subset S_z^{\perp} - S_x \tag{33b}$$

The proof of this fact is straightforward and can be found in [2].

C. The Hypergraph Product of a Connected Graph

Proposition 29. ***The hypergraph product of a connected graph***
Let $G = (V, E)$ denote a d-regular connected graph on n vertices. Let $\mathcal{C} = \mathcal{C}(G)$ denote the repetition code on n bits defined by treating the edges of G as equality constraints. Let $\mathcal{C}_{\times}(G)$ denote the hypergraph product of $\mathcal{C} \times_{TZ} \mathcal{C}$. Then:

1) *Denote $|V| = n$, $|E| = m = dn/2$, and so $|V \times V| = n^2, |E \times E| = d^2n^2/4, |V \times E| = |E \times V| = dn^2/2$. The number of qubits is $N = (1+d^2/4)n^2$ and the number of checks is dn^2.*
2) *$\mathcal{C}_{\times}$ is a quantum code on the space of $\mathbb{F}_2^{V \times V} \oplus \mathbb{F}_2^{E \times E} = \mathbb{F}_2^N$, constrained by the $d+2$-local checks from the columns of $\{H_x, H_z\}$.*
3) *The following set of vectors, indexed by $v \in V, e \in E$, generates S_z,*

   $$s_z(v, e) = H_z^T(v \otimes e) = v \otimes \partial^T e + \partial v \otimes e \tag{34}$$

   Likewise S_x is generated by the vectors

   $$s_x(e, v) = H_x^T(e \otimes v) = \partial^T e \otimes v + e \otimes \partial v. \tag{35}$$

4) *$\dim(S_x^{\perp}/S_z) = 1 + \dim(\mathcal{C}^T)^2$. This follows from Proposition 14 in [2].*
5) *The distance of the code is given by the minimum of the distance of the code $\mathcal{C}$ and the transposed code $\mathcal{C}^T$.*

We can also specialize our characterization of logical operators from Fact 28 to the repetition code with 2-bit check operators.

Proposition 30. *Let $\mathcal{C}_{\times} = \mathcal{C} \times \mathcal{C} = \mathcal{C}_{\times}(G)$, where G is a connected graph, and $\mathcal{C}(G)$ is the repetition code constrained by parity checks corresponding to the edges of G. There exists a spanning set $\mathcal{B}_z$ of $S_x^{\perp}$, and a spanning set $\mathcal{B}_x$ of $S_z^{\perp}$, as follows:*

$$\mathcal{B}_z := \{b_1^z\} \cup \{e \otimes c\}_{e \in E, c \in \mathcal{C}^T} \cup S_z \tag{36a}$$

$$\mathcal{B}_x := \{b_1^x\} \cup \{c \otimes e\}_{e \in E, c \in \mathcal{C}^T} \cup S_x \tag{36b}$$

where $\mathcal{C}^T = \ker \partial^T$ denotes the linear span of all indicator vectors of edges corresponding to cycles in G.

Proof: This follows from [2] as follows. From the proof of Lemma 17 of [2] we have that b_1^z and $e \otimes c$, for each $c \in \mathcal{C}^T$ are in $S_x^{\perp} - S_z$. By Proposition 14 of [2] it follows that these words, with S_z, span the entire $S_x^{\perp}$ space. The argument for $\mathcal{B}_x$ is the same. ■

1) Fractal Structure: Another important property of the hypergraph product of a connected graph, is that the hypergraph product exhibits a fractal structure as follows:

Proposition 31. *Let $G = (V, E)$ be some graph, and let $\mathcal{C}_{\times}(G)$ denote the hypergraph product of the repetition code induced by equality constraints of E, with itself. Let $V_l \subseteq V, E_l \subseteq E$ denote some subsets. Then there exists a graph $G' = (V_l, E_l \cap V_l \times V_l)$ such that $\mathcal{C}_{\times}(G')$ is supported on $V_l \times V_l \cup E_l \times E_l$.*

Proof: By definition, the checks of $\mathcal{C}_{\times}$ are the Cartesian product $E \times V$ for S_x and $V \times E$ for S_z. Define $G' = (V', E')$ as in the statement of the proposition, i.e. with E' the set of edges in E_l that have both endpoints in V_l. Hence $E' \subseteq E$, $V' \subseteq V$, and so in particular $E' \times V' \cup V' \times E' \subseteq E \times V \cup V \times E$. ■

D. The Hypergraph Product of an Expander Graph

In this section, we consider the hypergraph product $\mathcal{C}_{\times}(G) = \mathcal{C}(G) \times \mathcal{C}(G)$, where G is a d-regular Ramanujan expander graph. We note that while the minimal distance of $\mathcal{C}$ is exactly n, as it is the repetition code, the minimal distance of $\mathcal{C}^T$ is much smaller, i.e. $O(\log(n))$ - given by the minimum length cycle in the expander graph. Hence

$$\delta_{\min}(\mathcal{C}_{\times}) = \min\{\delta_{\min}(\mathcal{C}), \delta_{\min}(\mathcal{C}^T)\} =$$

$$\min\{O(n), O(\log(n))\} = O(\log(n)).$$

1) Comparison to the toric code: One can first compare $\mathcal{C}_\times(G)$ to the toric code. The toric code can be seen as the hypergraph product of the repetition code, with equality constraints in a cycle, i.e. $x_1 = x_2, x_2 = x_3, \ldots, x_n = x_1$. (By contrast our code has equality constraints $x_i = x_j$ for (i, j) running over the set of edges in an expander graph.) It follows from the hypergraph product, that the distance of such a code is precisely n (out of n^2 total qubits), which is larger than the $O(\log n)$ minimum distance of our code. However, the toric code also has low-error trivial states, since we can delete an $O(\varepsilon)$ fraction of constraints and leave it disconnected into blocks of $1/\varepsilon^2$ qubits.

2) Localized Minimal Distance: As stated above we have $\delta_{\min}(\mathcal{C}_\times) = O(\log(n))$. However, not all logical qubits are equally protected: we focus on the logical qubit with distance n, meaning that all elements of C_1^Z and C_1^X have weight $\geq n$. It turns out, that for this logical qubit, an even stronger property is true: we will show that any element of C_1^Z or C_1^X must have weight $\Omega(n)$ in some row or column of $V \times V$ or $E \times E$. In other words, the minimal distance of this logical qubit is manifested *locally*:

Lemma 32. ***Locally-manifested minimal distance*** *Let $\mathcal{C}_\times(V' \times V' \cup E' \times E') = \mathcal{C}(G')$ denote the hypergraph product of a graph $G' = (V', E')$, which is a connected ε-residual graph of a Ramanujan graph of degree d. If $d \geq 14$ and $\varepsilon \leq \frac{1}{620d}$ then*

$$\forall w \in C_1^Z \quad \left(\exists v \in V' \quad |w_{V' \times v}| \geq \frac{1}{2} n' \right. \\ \left. \text{or} \quad \exists e \in E' \;\; |w_{E' \times e}| \geq \frac{3}{8d} n' \right). \tag{37}$$

where $n' = |V'|$. Similarly,

$$\forall w \in C_1^X \quad \left(\exists v \in V' \quad |w_{v \times V'}| \geq \frac{1}{2} n' \right. \\ \left. \text{or} \quad \exists e \in E' \;\; |w_{e \times E'}| \geq \frac{3}{8d} n' \right). \tag{38}$$

VIII. Explicit QNC^1-Robust Local Hamiltonians

A. The construction

In this section, we show how to construct QNC^1-robust local Hamiltonians based on CSS codes. Let $\mathcal{G}$ be an explicit family of 14-regular Ramanujan graphs, as discussed in Section II-C. We define

$$\mathcal{C}_\times = \mathcal{C}(G). \tag{39}$$

B. NLETS *Theorem Statement*

Theorem 33. NLETS
Let $\mathcal{C}_\times^{(N)}$ denote the hypergraph product above that is defined on a space of $N = (1 + d^2/4)n^2$ qubits. The family of local Hamiltonians $\left\{ H\left(\mathcal{C}_\times^{(N)}\right) \right\}_N$ is NLETS *for $d = 14$ and $\varepsilon = 10^{-8}$.*

(Our proof applies to any $d \geq 14$ and sufficiently small $\varepsilon > 0$, which may depend on d.)
The proof (found in [15]) has 3 steps.

In the first part of the proof we show that any quantum state $|\psi\rangle$ that is an ε-impostor of $H(\mathcal{C}_\times)$ obeys, in fact, a more stringent constraint on a *subsystem* of the full Hilbert space, which is the uniform low-weight error condition: there exists some large subset $V_l \subseteq V$ and large subset $E_l \subseteq E$ such that for *each* $v \in V_l$ at most an $O(\sqrt{\varepsilon})$ fraction of the qubits $V \times v$ have errors, and the same holds for a large fraction of columns $E \times e$, for $e \in E_l$.

A certain "fractal" property of the hypergraph product of the repetition code defined by an expander graph, allows us to argue that inside $\mathcal{C}_\times$ there exists a complete smaller product-hypergraph of a connected sub-graph (V', E') induced by (V_l, E_l). Hence, we can reduce the problem of an ε-impostor to the hypergraph product code of G to the problem of an ε-impostor to the hypergraph product code of G_l, with the extra condition of uniform low-weight error.

In the second part we show that this "uniform low-weight error condition" implies that there exists a distance partition in either the X or Z basis.

In the third part, we finish the proof by using the distance partition above to argue that the $|\psi\rangle$ has low vertex expansion in at least the X or Z basis.

Acknowledgements

We thank Dorit Aharonov, and Jeongwan Haah for useful conversations, Fernando Brandão, Toby Cubitt, Isaac Kim, Anthony Leverrier, Cedric Lin and Kevin Thompson for useful and detailed comments and Alex Lubotzky for pointing out the fundamental importance of the Tillich-Zémor construction. We thank an anonymous reviewer for pointing out a fundamental flaw in our previous paper claiming the NLTS conjecture. We are both funded by the Templeton foundation, AWH is funded by NSF grants CCF-1111382 and CCF-1452616 and ARO contract W911NF-12-1-0486, and LE is funded by NSF grant CCF-1629809.

References

[1] M. H. Freedman and M. B. Hastings, "Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs," *Quantum Info. Comput.*, vol. 14, no. 1-2, pp. 144–180, Jan. 2014.

[2] J.-P. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$," in *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 2*, ser. ISIT'09, 2009, pp. 799–803.

[3] B. M. Terhal and D. P. DiVincenzo, "Adaptive quantum computation, constant depth quantum circuits and arthur-merlin games," *Quant. Inf. Comp.*, vol. 4, no. 2, pp. 134–145, 2004.

[4] X. Chen, Z.-C. Gu, and X.-G. Wen, "Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order," *Phys. Rev. B*, vol. 82, p. 155138, Oct 2010.

[5] A. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, no. 1, pp. 2 – 30, 2003.

[6] D. Aharonov, I. Arad, and T. Vidick, "Guest column: The quantum PCP conjecture," *SIGACT News*, vol. 44, no. 2, pp. 47–79, Jun. 2013.

[7] D. Aharonov and L. Eldar, "Quantum locally testable codes," *SIAM Journal on Computing*, vol. 44, no. 5, pp. 1230–1262, 2015.

[8] M. B. Hastings, "Quantum codes from high-dimensional manifolds," 2016, arXiv:1608.05089.

[9] S. Bravyi and M. B. Hastings, "Homological product codes," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, ser. STOC '14. New York, NY, USA: ACM, 2014, pp. 273–282.

[10] J. Friedman and J.-P. Tillich, "Laplacian eigenvalues and distances between subsets of a manifold," *J. Differential Geom.*, vol. 56, no. 2, pp. 285–299, 10 2000.

[11] I. Arad, A. Kitaev, Z. Landau, and U. Vazirani, "An area law and sub-exponential algorithm for 1D systems," in *Proceedings of the 4th Innovations in Theoretical Computer Science (ITCS)*, 2013.

[12] J. Chen, Z. Ji, B. Zeng, and D. L. Zhou, "From ground states to local Hamiltonians," *Phys. Rev. A*, vol. 86, p. 022339, Aug 2012.

[13] S. Bravyi, M. Hastings, and F. Verstraete, "Lieb-Robinson bounds and the generation of correlations and topological quantum order," *Phys. Rev. Lett.*, vol. 97, p. 050401, 2006, arXiv:quant-ph/0603121.

[14] J. Haah, "An invariant of topologically ordered states under local unitary transformations," *Communications in Mathematical Physics*, vol. 342, no. 3, pp. 771–801, Mar 2016.

[15] L. Eldar and A. W. Harrow, "Local Hamiltonians whose ground states are hard to approximate," 2015, arXiv:1510.02082.

[16] H. P. Robertson, "The uncertainty principle," *Phys. Rev.*, vol. 34, pp. 163–164, Jul 1929.

[17] H. F. Hofmann and S. Takeuchi, "Violation of local uncertainty relations as a signature of entanglement," *Phys. Rev. A*, vol. 68, p. 032103, Sep 2003.

[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. New York, NY, USA: Cambridge University Press, 2011.

[19] S. Lovett and E. Viola, "Bounded-depth circuits cannot sample good codes," *Computational Complexity*, vol. 21, no. 2, pp. 245–266, 2012.

[20] L. H. Harper, "Optimal assignments of numbers to vertices," *Journal of the Society for Industrial and Applied Mathematics*, vol. 12, no. 1, pp. 131–135, 1964.

[21] S. Bravyi, M. B. Hastings, and F. Verstraete, "Lieb-Robinson bounds and the generation of correlations and topological quantum order," *Phys. Rev. Lett.*, vol. 97, p. 050401, Jul 2006.

[22] M. Freedman, D. Meyer, and F. Luo, "$\mathbb{Z}_2$-systolic freedom and quantum codes," in *Math. of Quantum Computation*, R. K. Brylinski and G. Chen, Eds. Chapman & Hall/CRC, 2002, pp. 287–320.

[23] M. B. Hastings, "Locality in quantum systems," 2010, lecture notes from Les Houches summer school, arXiv:1008.5137.

[24] M. Hastings, "Topological order at non-zero temperature," *Phys. Rev. Lett.*, vol. 107, p. 210501, 2011.