A construction of Combinatorial NLTS

Anurag Anshu[1, a)] and Nikolas P. Breuckmann[2, b)]

[1)] *School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA*

[2)] *Department of Computer Science, University College London, WC1E 6BT London, United Kingdom*

(Dated: 26 July 2023)

The NLTS (No Low-Energy Trivial State) conjecture [M.H. Freedman & M.B. Hastings, Quantum Info. Comput., 14, 144 (2014)] posits that there exist families of Hamiltonians with all low energy states of high complexity (with complexity measured by the quantum circuit depth preparing the state). Here, we prove a weaker version called the combinatorial NLTS, where a quantum circuit lower bound is shown against states that violate a (small) constant fraction of local terms. This generalizes the prior NLETS results [L. Eldar & A.W. Harrow, FOCS, 58, 427 (2017)] and [C. Nirkhe, U. Vazirani & H. Yuen, ICLAP, 45 (2018)]. Our construction is obtained by combining tensor networks with expander codes [M. Sipser & D. Spielman, IEEE ToIT, 42, 1710 (1996)]. The Hamiltonian is the parent Hamiltonian of a perturbed tensor network, inspired by the 'uncle Hamiltonian' of [C. Fernández-González et al., Communications in Mathematical Physics, 333, 299 (2015)]. Thus, we deviate from the quantum CSS code Hamiltonians considered in most prior works.

[a)]Electronic mail: anuraganshu@fas.harvard.edu

[b)]Electronic mail: n.breuckmann@ucl.ac.uk

I. INTRODUCTION

The approximation of the ground energy of a local Hamiltonian continues to be a leading goal of quantum complexity theory and quantum many-body physics. While a generic, accurate and efficient approximation method is unlikely, due to the seminal result of Kitaev[3], physically motivated ansatzes such as tensor networks[26] and low depth quantum circuits[6,18,30] continue to explore the low energy spectrum of many interesting Hamiltonians.

A fundamental question on the power of low-depth quantum circuits is the NLTS conjecture[14], which posits the existence of local Hamiltonians with all low energy states having high quantum circuit complexity. This is a necessary consequence of the quantum PCP conjecture[1], under the reasonable assumption that QMA $\neq$ NP. We refer the reader to existing works[1,7,8,12,22] for a detailed discussion on the NLTS conjecture and its close connection with quantum error correction, robustness of entanglement and the power of variational quantum circuits.

To formally define the NLTS conjecture, we introduce a n-qubit local Hamiltonian H as a sum of local terms $H = \sum_{i=1}^{m} h_i$ (each $0 \preceq h_i \preceq \mathbb{I}$ is supported on $O(1)$ qubits and each qubit participates in $O(1)$ local terms) with $m = \Theta(n)$. The ground states of H are the eigenstates with eigenvalue $\lambda_{\min}(H)$. An ε-energy state ψ satisfies $\mathrm{Tr}\,(H\psi) \leq \varepsilon m + \lambda_{\min}(H)$.

Conjecture 1 (NLTS[14])**.** There exists a fixed constant $\varepsilon > 0$ and an explicit family of $O(1)$-local Hamiltonians $\{H^{(n)}\}_{n=1}^{\infty}$, such that for any family of ε-energy states $\{\psi_n\}$, the circuit complexity $\mathrm{CC}(\psi_n)$ grows faster than any constant.

Here, $\mathrm{CC}(\psi)$ is *quantum circuit depth*, the depth of the smallest quantum circuit that prepares ψ. An interesting property of any (potential) NLTS Hamiltonian is that it must live on an expanding interaction graph, ruling out all the finite-dimensional lattice Hamiltonians that have been very well studied in quantum many-body physics. The same holds for (potential) Hamiltonians that may witness the quantum PCP conjecture[1].

A weaker version of this conjecture is known, called the NLETS theorem. A local Hamiltonian H (as defined above) is frustration-free if $\lambda_{\min}(H) = 0$. A state ψ is called *ε-error* if there exists a set S of qubits of size at least $(1-\varepsilon)n$ such that $\psi_S = \phi_S$, where ϕ is some ground state of H and the subscript S means that we take a partial trace over the qubits in $[n] \setminus S$.

Theorem 2 ([12,22]). *There exists a fixed constant $\varepsilon > 0$ and an explicit family of $O(1)$-local frustration-free Hamiltonians $\{H^{(n)}\}_{n=1}^{\infty}$, such that for any family of ε-error states $\{\psi_n\}$, the circuit complexity $\mathrm{CC}(\psi_n)$ is $\Theta(\log n)$.*

Note that the ε-energy states include the set of $O(\varepsilon)$-error states, but the reverse direction is not true. The NLETS theorem was first proved by[12], by considering the hypergraph product[34] of two Tanner codes on expander graphs[32]. In the follow-up work,[22] constructed an NLETS Hamiltonian that in fact lived on a one-dimensional lattice. In the recent work[7], super-constant circuit lower bounds were shown for $o(1)$-energy states (such as $O(\frac{1}{\log n})$-energy) of all quantum code Hamiltonians that have near-linear rank or near-linear distance. Interestingly, such lower bounds are again possible with the two-dimensional, punctured toric code, showing that expansion of the underlying interaction graph is not needed for circuit lower bounds on 'almost constant' energy states.

Both[12,22] identified the intermediate question of *combinatorial NLTS* (cNLTS), which aims at finding frustration-free Hamiltonians with super-constant circuit lower bounds for states ψ that satisfy at least $1-\varepsilon$ fraction of local terms. The main interest in this question stems from the fact that any (potential) cNLTS Hamiltonian must also live on an expanding interaction hypergraph, hence exhibiting the geometric features of an NLTS Hamiltonian. Here, we provide the first construction of a cNLTS Hamiltonian.

Theorem 3 (Main result). *There exists a fixed constant $\varepsilon > 0$ and an explicit family of $O(1)$-local frustration-free Hamiltonians $\{H^{(n)}\}_{n=1}^{\infty}$, where $H^{(n)} = \sum_{i=1}^{m} h_i^{(n)}$ acts on n particles and consists of $m = \Theta(n)$ local terms, such that for any family of states $\{\psi_n\}$ satisfying*

$$\frac{|i : \mathrm{Tr}\left(h_i^{(n)}\psi_n\right) > 0|}{m} \leq \varepsilon,$$

the circuit complexity $\mathrm{CC}(\psi_n)$ is $\Theta(\log n)$.

The set of states that satisfy $1-\varepsilon$ fraction of local terms also include $O(\varepsilon)$-error states. Thus, the above family of Hamiltonians are also NLETS.

Other related results

In[11], thermal states of certain quantum codes were shown to have circuit lower bounds.[8] showed circuit lower bounds for quantum states with a 'Z_2 symmetry'. The work[12] showed

that locally testable quantum CSS codes[2] of linear distance are NLTS. Such codes are not known to exist, with the best distance thus far being $\sqrt{n}$[19]. However, the dramatic recent progress in quantum codes[9,15,27,28] opens up the exciting possibility that such codes may exist.

New results: The follow-up work[5] supersedes the main result here, as it shows the NLTS property for good quantum codes[19,28]. It uses a different Hamiltonian family, but the underlying connection is that it proves a quantum analogue of Theorem 9. We believe that the Hamiltonian family in this work are also NLTS, when the parameter δ is set to a constant.

Outline of the construction

Our starting point is the NLETS theorem shown in[22]. It is based on the observation that the CAT state $\frac{1}{\sqrt{2}}|00\ldots0\rangle + \frac{1}{\sqrt{2}}|11\ldots1\rangle$ is close to the unique ground state of Kitaev's clock Hamiltonian. This clock Hamiltonian is obtained from the circuit preparing the CAT state and then padding with identity gates. We observe that yet another Hamiltonian can be constructed, by viewing the CAT state as a Matrix Product State (MPS). The MPS representation of the CAT state is obtained by starting with $\frac{n}{2}$ EPR pairs

$$(|00\rangle + |11\rangle)_{1,2} \otimes (|00\rangle + |11\rangle)_{3,4} \otimes \ldots (|00\rangle + |11\rangle)_{n-1,n}$$

and then projecting qubits $i, i+1$, for even i, with the projector $M = |00\rangle\langle 00| + |11\rangle\langle 11|$. Most MPS are the unique ground states of a parent Hamiltonian (such MPS are called injective). But the CAT state MPS clearly does not have this privilege, since M is not an invertible map. However, inspired by[13], we can perturb M to consider a state obtained by mapping qubits $i, i+1$ with $M + \delta\mathbb{I}$ (for $\delta \approx \frac{1}{\sqrt{n}}$). This is an invertible map, which makes the resulting MPS injective. Using the corresponding parent Hamiltonian, we obtain another construction of the NLETS Hamiltonian.[23]

Since any cNLTS Hamiltonian must be on an expanding interaction graph, an approach to construct the desired Hamiltonian is to write down a tensor network for the CAT state on an expanding graph, perturb the tensors and then take the parent Hamiltonian. Unfortunately, this argument seems not to work, since the tensor network for the CAT state is extremely brittle. If we remove one EPR pair and allow arbitrary inputs to the tensors acting on this

EPR pair, we can produce the states $|00\ldots0\rangle$ or $|11\ldots1\rangle$. This brittleness reflects in the nearby parent Hamiltonian and there are product states that violate just one local term. Our second observation is that the CAT state tensor network can be viewed as a *repetition Tanner code* on an expanding graph. Thus, we can generalize the tensor network and look at Tanner codes defined on expander graphs, as proposed by Sipser-Spielman[32] (Section III). The tensor network state is now a uniform superposition over all the codewords of this Tanner code. With (1) linear distance and (2) linear rank (and with a suitable choice of parameters) such a code protects us from two sources of brittleness:

1. Removing an ε fraction of EPR pairs (analogously, local terms of the Hamiltonian) weakens the expansion properties of the underlying graph. Linear distance ensures that the codewords, while no longer far away from each other, are partitioned into distant groups for a small constant ε.

2. Removing an ε fraction of EPR pairs (analogously, local terms of the Hamiltonian) can drastically reduce the number of strings appearing in the superposition. Linear rank ensures that the number of strings is large enough, if ε is a small constant.

See Section IV for full details. We note that tensor networks have previously been combined with local (quantum) codes to obtain global properties[29].

Local systems and non-isotropic Gauß's laws

Tanner codes can be understood in terms of homology with local systems[33], where differentials take values in the space of local checks[21]. A trivial example is the toric code, where the differential at each vertex detects violations of $\mathbb{Z}_2$-flux conservation, or in other words, violations of a local parity-check code (this is of course nothing but the usual simplicial $\mathbb{Z}_2$-homology). The family of Hamiltonians that we construct can be understood in terms of differentials defined from more complicated local codes. The Hamiltonians ensure that these differentials are zero for ground states, which means they enforce a non-isotropic Gauß's law that takes the directionality of the incoming fluxes into account. Together with the expansion of the underlying graph, this leads to the cNLTS property.

Tensor networks and quantum complexity

Kitaev's clock construction is a powerful method to map quantum computations to the ground states of local Hamiltonians. It turns out that the tensor networks provide a similar mapping. As shown in[31], any measurement-based quantum computation can be mapped onto a tensor network. One could thus imagine a form of circuit-to-Hamiltonian mapping different from Kitaev's: perturb the above tensor network and consider its parent Hamiltonian. A standard objection to this approach is that the mapping also works for post-selected quantum circuits, which is far more powerful than QMA. However, this objection is not expected to apply to our case, as injective tensors cannot post-select on events of very small probability. We leave an understanding of the promise gap of this mapping for future work.

II. TANNER CODE

In this section we review a construction of linear codes from regular graphs called Tanner codes. A (classical) linear code C of length n and rank k is a subspace of dimension k of the vector space $\mathbb{F}_2^n = \{0,1\}^n$. A linear code C can be defined by specifying a parity check matrix $H \in \mathbb{F}_2^{m\times n}$, such that $\ker H = C$. We call the m rows of H checks of the code C.

Consider a regular graph $G = (V, E)$ with degree d and $n = |V|$ vertices. For $S, S' \subset V$, we denote the number of edges between S and S' as $E(S, S')$ (we count an edge $\{u, v\}$ twice if $u, v \in S \cap S'$). Let $\lambda = \max(|\lambda_2|, |\lambda_n|)$, where λ_2, λ_n are the second largest and the smallest eigenvalues of the adjacency matrix.

A Tanner code $T(C, G) \subset \{0,1\}^{|E|}$ is defined using the graph G and a classical linear code $C \subset \{0,1\}^d$ of rank k_0 and distance Δ_0. We imagine bits on edges and checks on the vertices. Let the edges be numbered using the integers $\{1, 2, \ldots |E|\}$ in some arbitrary manner. Given a string $x \in \{0,1\}^{|E|}$ and a vertex v, let $x_v \in \{0,1\}^d$ be the restriction of x to the edges incident to v, where the ith bit of x_v is the value on the edge with the ith smallest number. Formally,

$$T(C, G) = \{x : x_v \in C \quad \forall v \in V\}. \tag{1}$$

We will abbreviate $T(C, G)$ as T for convenience. Since there are $d - k_0$ independent checks in C, the number of independent checks in T is at most $n(d - k_0)$. Thus, the rank k

of T is $k \geq \frac{nd}{2} - n(d - k_0) = n\left(k_0 - \frac{d}{2}\right)$.

Lemma 4. *Suppose $\Delta_0 \geq 2\lambda$. The distance of T is lower bounded by $\frac{n\Delta_0^2}{4d} = \frac{|E|\Delta_0^2}{2d^2}$.*

Proof. Let $x \in T$ be the non-zero code-word of smallest Hamming weight and let E_x be the edges where x takes value 1. Let S be the set of all vertices on which at least one edge in E_x is incident. Since the distance of C is Δ_0, at least Δ_0 edges from any vertex in S stay within S (and those edges belong to E_x). Thus, $|E(S,S)| \geq |S|\Delta_0$. However, the expander mixing lemma[35] (Lemma 4.15) ensures that

$$|E(S,S)| \leq \frac{d|S|^2}{n} + \lambda|S|.$$

Thus,

$$|S|\Delta_0 \leq |E(S,S)| \leq \frac{d|S|^2}{n} + \lambda|S| \leq \frac{d|S|^2}{n} + \frac{\Delta_0|S|}{2} \implies |S| \geq \frac{n\Delta_0}{2d}.$$

Since $|E_x| \geq \frac{|S|\Delta_0}{2}$ (every vertex in S is associated to at least Δ_0 edges in E_x and every edge in E_x is associated to 2 vertices in S), the lemma concludes. □

III. INJECTIVE TENSOR NETWORK FROM THE CODE $T(C,G)$

Let $|\mathrm{EPR}\rangle = |00\rangle + |11\rangle$ be an unnormalized EPR pair. Given G, we consider a Hilbert space consisting of nd qubits, with d qubits for each vertex $v \in V$. For a $v \in V$, we identify each qubit with a unique edge incident on v and label the qubit as v_e. As a result, given an edge $e = (v, v')$, qubits v_e, v'_e come in pairs (Figure 1). We will often denote the joint Hilbert space $\mathcal{H}_{v_e} \otimes \mathcal{H}_{v'_e}$ as $\mathcal{H}_e$ and abbreviate $|0\rangle_{v_e}|0\rangle_{v'_e}$ as $|0\rangle_e$ and $|1\rangle_{v_e}|1\rangle_{v'_e}$ as $|1\rangle_e$. Thus, $|0\rangle_{v_e}|0\rangle_{v'_e} + |1\rangle_{v_e}|1\rangle_{v'_e}$ will be referred to as $|\mathrm{EPR}\rangle_e$. Define the unnormalized state

$$|\Theta_0\rangle := \bigotimes_{e\in E} |\mathrm{EPR}\rangle_e .$$

For each vertex v, define the projector that only accepts the codewords of the local code at v:

$$P_v := \sum_{c\in C} |c_1\rangle\langle c_1|_{v_{e_1}} \otimes |c_2\rangle\langle c_2|_{v_{e_2}} \otimes \cdots \otimes |c_d\rangle\langle c_d|_{v_{e_d}} ,$$

where c_i is the ith bit of c and e_i is the ith edge incident on v (in the ascending numbering specified on the edges). The tensor network state is obtained by projecting the d qubits on

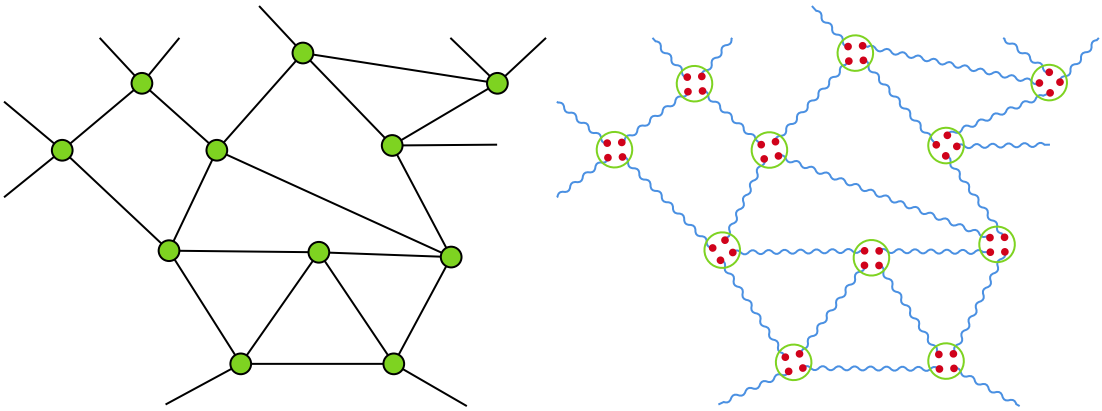

FIG. 1: (Left) A degree $d = 4$ graph with a Tanner code defined on it. (Right) The associated tensor network, where d qubits (red) are placed on each vertex (green circle) and qubits are connected according to the edge structure using EPR pairs (blue wavy lines). The qubits on each vertex are projected according to the local code.

each vertex using these projectors:

$$|\Phi\rangle := \frac{1}{\sqrt{2^k}} \bigotimes_v P_v \, |\Theta_0\rangle = \frac{1}{\sqrt{2^k}} \sum_{x \in T} \bigotimes_{e=(v,v')} |x_e\rangle_e \, .$$

Note that the normalization follows since there are 2^k codewords in T. We can think of the string x as an *edge assignment* and $|\Phi\rangle$ as a uniform superposition over edge assignments from T. Now, we can make the tensor network 'injective' by defining

$$Q_v := P_v + \delta \mathbb{I} = (1+\delta) P_v + \delta(\mathbb{I} - P_v), \quad |\Psi\rangle := \frac{1}{\sqrt{Z}} \bigotimes_v Q_v \, |\Theta_0\rangle \, .$$

Claim 5. It holds that

$$Z \leq 2^k (1 + 2\delta + \delta^2 2^{(d-k_0)})^n$$

and

$$|\, \langle \Psi | \Phi \rangle \,| \geq \frac{(1+\delta)^n}{(1 + 2\delta + \delta^2 2^{(d-k_0)})^{\frac{n}{2}}}$$

Proof. Consider,

$$\begin{aligned} Z &= \langle \Theta_0 | \bigotimes_v Q_v^2 \, |\Theta_0\rangle = \langle \Theta_0 | \bigotimes_v \left((1+2\delta) P_v + \delta^2 \mathbb{I} \right) |\Theta_0\rangle \\ &= \sum_{S \subset V} (1+2\delta)^{|S|} \delta^{2n-2|S|} \, \langle \Theta_0 | \bigotimes_{v \in S} P_v \, |\Theta_0\rangle \end{aligned}$$

Let us evaluate $\langle\Theta_0|\bigotimes_{v\in S} P_v|\Theta_0\rangle$. This is essentially the number of codewords when parity checks only act on the vertices in S. If we were to include the parity checks in $V\setminus S$ as well, we would obtain the original code. Since there are at most $(d-k_0)(n-|S|)$ independent checks, the following inequality holds:

$$\langle\Theta_0|\bigotimes_{v\in S} P_v|\Theta_0\rangle\cdot 2^{-(d-k_0)(n-|S|)}\leq 2^k \implies \langle\Theta_0|\bigotimes_{v\in S} P_v|\Theta_0\rangle\leq 2^k\cdot 2^{(d-k_0)(n-|S|)}.$$

This shows that

$$\begin{aligned}Z &\leq 2^k\cdot\sum_{S\subset V}(1+2\delta)^{|S|}\delta^{2n-2|S|}\cdot 2^{(d-k_0)(n-|S|)} = 2^k\cdot\sum_{S\subset V}(1+2\delta)^{|S|}\left(\delta^2 2^{(d-k_0)}\right)^{(n-|S|)}\\ &= 2^k(1+2\delta+\delta^2 2^{(d-k_0)})^n.\end{aligned}$$

Further,

$$\begin{aligned}\langle\Psi|\Phi\rangle &= \frac{1}{\sqrt{2^k Z}}\langle\Theta_0|\bigotimes_v Q_v P_v|\Theta_0\rangle = \frac{(1+\delta)^n}{\sqrt{2^k Z}}\langle\Theta_0|\bigotimes_v P_v|\Theta_0\rangle\\ &= \frac{(1+\delta)^n\sqrt{2^k}}{\sqrt{Z}}\geq\frac{(1+\delta)^n}{(1+2\delta+\delta^2 2^{(d-k_0)})^{\frac{n}{2}}}.\end{aligned}$$

This completes the proof. □

The nice property of $|\Psi\rangle$ is that it is the unique ground state of a local Hamiltonian. For $e=(v,v')$, define

$$g_e = (Q_v\otimes Q_{v'})^{-1}\left(\mathbb{I}-|\mathrm{EPR}\rangle\langle\mathrm{EPR}|_e\right)(Q_v\otimes Q_{v'})^{-1},\quad h_e=\mathrm{span}\,(g_e)$$

where 'span' means that h_e is the projector onto the image of g_e. Since $g_e|\Psi\rangle=0$, we have $h_e|\Psi\rangle=0$. Let

$$H:=\sum_{e\in E} h_e.$$

Then $|\Psi\rangle$ is a ground state of H with ground energy 0. In fact, we have the following claim, which is well known about injective tensor networks.

Claim 6. $|\Psi\rangle$ is the unique ground state of H.

Proof. Suppose $|\Psi'\rangle$ is a ground state of H. Then it is also a ground state of $\sum_e g_e$. Write $|\Psi'\rangle=\bigotimes_{v\in V}Q_v|\Theta'\rangle$, for a (possibly unnormalized) quantum state $|\Theta'\rangle$. This is possible since $\bigotimes_{v\in V}Q_v$ is invertible. Observe that $|\Theta'\rangle$ is a ground state of $\sum_e(\mathbb{I}-|\mathrm{EPR}\rangle\langle\mathrm{EPR}|_e)$. This is possible only if $|\Theta'\rangle=|\Theta_0\rangle$, which proves the claim. □

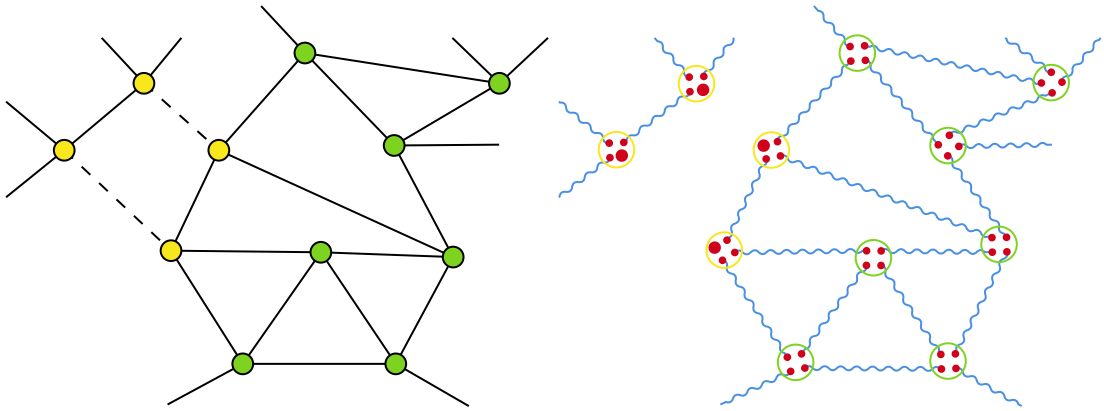

FIG. 2: (Left) The dashed edges have been removed. W denotes the set of yellow vertices. The remaining edges are E_1. (Right) In the tensor network picture, some qubits are no longer required to be connected by an EPR pair. These qubits, called residuals, are shown as thick red dots inside yellow circles. Their set is R.

IV. THE HAMILTONIAN H IS CNLTS

Suppose $\varepsilon|E|$ local terms from H are removed (see Figure 2). Since each local term corresponds to an edge, let E_1 be the remaining edges and let $H_1 = \sum_{e\in E_1} h_e$ be the Hamiltonian that remains. We will show that any state $|\psi\rangle$ that is a ground state of H_1 has a large circuit complexity, if ε is a sufficiently small constant.

A. Structure of the ground space of H_1

Let $W \subset V$ be the set vertices on which the removed edges were incident. Among the $d|W|$ qubits in these vertices, some qubits were associated to the removed edges. We will call these qubits 'residual' and denote their set by $R = \{1, 2, \ldots 2\varepsilon|E|\}$. We are free to choose any 'assignment' $|0\rangle, |1\rangle$ to the residual qubits. Since we have been thinking of assignments as occurring on the edges, we will sometimes refer to R as a set of edges (Figure 2). Thus, we will continue using the terminology of 'edge assignment'. Note the following cardinality bounds:

$$|W| \leq |R| = 2\varepsilon|E|, \quad |E_1| = |E|(1-\varepsilon) = \frac{d|V| - |R|}{2}. \tag{2}$$

Let

$$|\Theta_1\rangle := \bigotimes_{e\in E_1} |\mathrm{EPR}\rangle_e .$$

We have the following claim, which is analogous to Claim 6.

Claim 7. The ground space of H_1 is

$$\mathcal{G} := \mathrm{span}\left(\bigotimes_{v\in V} Q_v(|\Theta_1\rangle \otimes_{r\in R} |b_r\rangle_r), \text{ such that } b := b_1, \dots b_{|R|} \in \{0,1\}^{|R|}\right).$$

Proof. Let $|\omega\rangle = \bigotimes_{v\in V} Q_v |\tau\rangle$ be a ground state of H_1 for some $|\tau\rangle$, which is possible since $\bigotimes_{v\in V} Q_v$ is invertible. Note that

$$H_1 |\omega\rangle = 0 \implies \forall e \in E_1, \quad h_e |\omega\rangle = 0 \implies \forall e \in E_1, \quad g_e |\omega\rangle = 0.$$

Thus, for all $e \in E_1$, $(\mathbb{I} - |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_e) |\tau\rangle = 0$. This shows that $|\tau\rangle$ belongs to the space spanned by the vectors $\{|\Theta_1\rangle \otimes_{r\in R} |b_r\rangle_r , \text{ such that } b := b_1, \dots b_{|R|} \in \{0,1\}^{|R|}\}$, as there are no constraints on the residual qubits. This completes the proof. □

Consider the following basis within $\mathcal{G}$:

$$|\Psi_b\rangle \propto \bigotimes_{v\in V} Q_v(|\Theta_1\rangle \otimes_{r\in R} |b_r\rangle_r), \forall b \in \{0,1\}^{|R|},$$

where each $|\Psi_b\rangle$ is normalized as $\langle\Psi_b|\Psi_b\rangle = 1$. Note that this is an orthonormal basis, as the residual qubits are fixed according to b (the operators Q_v do not change any computational basis state). Along the lines of Claim 5, we would expect that this state is close to the following state (ignoring normalization)

$$\bigotimes_{v\in V} P_v(|\Theta_1\rangle \otimes_{r\in R} |b_r\rangle_r), \forall b \in \{0,1\}^{|R|}.$$

But we have to be careful: if $P_v(\otimes_{r\in R} |b_r\rangle_r) = 0$ for any $v \in W$[24], the above state is 0; whereas $|\Psi_b\rangle$ is non-zero for all b. With this in mind, we let $W_b \subset W$ denote all the vertices with which b is consistent (Figure 3 (left)). We observe that

$$|\Psi_b\rangle = \frac{1}{\sqrt{Z_b}} \bigotimes_{v\in(V\setminus W)\cup W_b} Q_v(|\Theta_1\rangle \otimes_{r\in R} |b_r\rangle_r),$$

since Q_v acts as $\delta\mathbb{I}$ at any $v \in W \setminus W_b$ (above Z_b is a normalization constant) and define

$$|\Phi_b\rangle = \frac{1}{\sqrt{2^{k_b}}} \bigotimes_{v\in(V\setminus W)\cup W_b} P_v(|\Theta_1\rangle \otimes_{r\in R} |b_r\rangle_r),$$

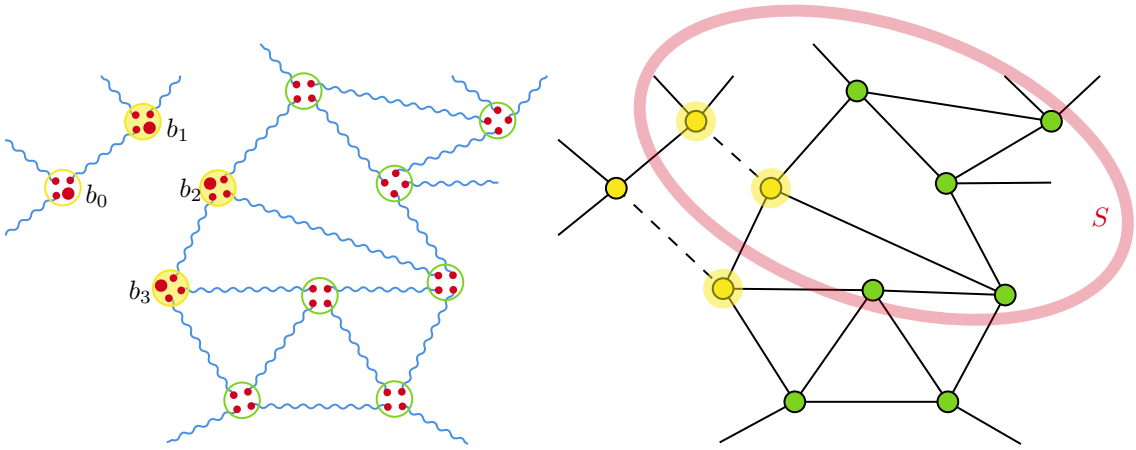

FIG. 3: (Left) The residual qubits are no longer connected by EPR pairs. Thus, they can be assigned any computational-basis state $|b\rangle : b \in \{0,1\}^{|R|}$ (in fact, they can be assigned any quantum state on $|R|$ qubits; but we focus on computational-basis states at the moment). A given assignment b may violate checks on some vertices in W (yellow circle). Here, we depict shaded yellow circles, where b does not cause any violated checks. This is the set $W_b \subset W$. (Right) Vertices in W_b are now depicted by yellow dots with shaded surrounding. In Claim 8, a set $S \subset (V \setminus W) \cup W_b$ is considered. Equation 4 can be verified from here.

where k_b will be determined shortly. Note that the states $\{|\Phi_b\rangle\}_{b\in\{0,1\}^{|R|}}$ are mutually orthogonal. The following claim is analogous to Claim 5.

Claim 8. It holds that

$$k_b \geq \left(\frac{2k_0}{d} - 1\right)|E| - |R|$$

and

$$|\langle\Phi_b|\Psi_b\rangle| \geq \frac{(1+\delta)^n}{(1+2\delta+\delta^2 2^{(d-k_0)})^{\frac{n}{2}}}.$$

Proof. We write down an expression for k_b. Note that $|\Phi_b\rangle$ is simply a superposition over edge assignments that satisfy the Tanner code with checks on $(V \setminus W) \cup W_b$, where we condition the edges in R to have fixed edge assignments according to b. Conditioning the edge assignments in R to be b leads to a set of parity check over edges in E_1 (some of these checks may also impose a parity of 1 on the edge assignments in E_1). Each vertex in $V \setminus W$ contributes to $d - k_0$ checks. Each vertex in W_b contributes to anywhere between 0 to $d - k_0$

independent checks. If we define c_v as the number of independent checks due to $v \in W_b$ that involve edges in E_1, we have

$$k_b \geq |E_1| - (d-k_0)(|V \setminus W|) - \sum_{v \in W_b} c_v. \tag{3}$$

Since $c_v \leq d - k_0$ and $W_b \subseteq W$, a lower bound on k_b is

$$\begin{aligned} k_b &\geq |E_1| - (d-k_0)(|V \setminus W| + |W_b|) \geq |E_1| - (d-k_0)|V| \\ &\overset{Eq.2}{=} |E_1| - \frac{d-k_0}{d}(2|E_1| + |R|) = \left(\frac{2k_0}{d} - 1\right)|E_1| - \frac{d-k_0}{d}|R| \\ &\geq \left(\frac{2k_0}{d} - 1\right)|E_1| - |R|. \end{aligned}$$

Next,

$$\begin{aligned} Z_b &= \langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in (V \setminus W) \cup W_b} Q_v^2 \, | \Theta_1 \rangle \otimes_{r \in R} | b_r \rangle_r \\ &= \langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in (V \setminus W) \cup W_b} ((1+2\delta)P_v + \delta^2 \mathbb{I}) \, | \Theta_1 \rangle \otimes_{r \in R} | b_r \rangle_r \\ &= \sum_{S \subset (V \setminus W) \cup W_b} (1+2\delta)^{|S|} \delta^{2(|(V \setminus W) \cup W_b| - |S|)} \langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in S} P_v \, | \Theta_1 \rangle \otimes_{r \in R} | b_r \rangle_r \\ &\overset{(1)}{\leq} 2^{k_b} \sum_{S \subset (V \setminus W) \cup W_b} (1+2\delta)^{|S|} \delta^{2(|(V \setminus W) \cup W_b| - |S|)} \cdot 2^{(d-k_0)(|V \setminus W| - |S \setminus W|) + \sum_{v \in W_b \setminus S} c_v} \\ &\leq 2^{k_b} \sum_{S \subset (V \setminus W) \cup W_b} (1+2\delta)^{|S|} \delta^{2(|(V \setminus W) \cup W_b| - |S|)} \cdot 2^{(d-k_0)(|V \setminus W| - |S \setminus W| + |W_b \setminus S|)} \\ &\overset{(2)}{=} 2^{k_b} \sum_{S \subset (V \setminus W) \cup W_b} (1+2\delta)^{|S|} \left(\delta^2 \cdot 2^{d-k_0}\right)^{(|(V \setminus W) \cup W_b| - |S|)} \\ &= 2^{k_b} (1 + 2\delta + \delta^2 \cdot 2^{d-k_0})^{(|(V \setminus W) \cup W_b|)}. \end{aligned}$$

For (1), note that $\langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in S} P_v \, | \Theta_1 \rangle \otimes_{r \in R} | b_r \rangle_r$ is the number of edge assignments that satisfy parity checks in S (with the condition that edges in R are assigned b). If we were to add parity checks on remaining vertices in $(V \setminus W) \setminus S$ and $W_b \setminus S$, we would obtain the 2^{k_b} codewords accounted for in Eq. 3. The number of such linearly independent parity checks that are added is at most $(d-k_0)(|V \setminus W| - |S \setminus W|) + \sum_{v \in W_b \setminus S} c_v$. This gives us the upper bound

$$\langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in S} P_v \, | \Theta_1 \rangle \otimes_{r \in R} | b_r \rangle_r \cdot 2^{-(d-k_0)(|V \setminus W| - |S \setminus W|) - \sum_{v \in W_b \setminus S} c_v} \leq 2^{k_b},$$

and (2) uses (see Figure 3(right))

$$|V \setminus W| - |S \setminus W| + |W_b \setminus S| = |V \setminus W| + |W_b| - |S| = |(V \setminus W) \cup W_b| - |S|, \tag{4}$$

where we repeatedly used the fact that $S \subset (V \setminus W) \cup W_b$. Thus,

$$\begin{aligned}
|\langle \Phi_b | \Psi_b \rangle| &= \frac{1}{\sqrt{2^{k_b} Z_b}} \langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in (V \setminus W) \cup W_b} P_v Q_v |\Theta_1\rangle \otimes_{r \in R} |b_r\rangle_r \\
&= \frac{(1+\delta)^{|(V \setminus W) \cup W_b|}}{\sqrt{2^{k_b} Z_b}} \langle \Theta_1 | \otimes_{r \in R} \langle b_r |_r \bigotimes_{v \in (V \setminus W) \cup W_b} P_v |\Theta_1\rangle \otimes_{r \in R} |b_r\rangle_r \\
&= \frac{(1+\delta)^{|(V \setminus W) \cup W_b|}}{\sqrt{2^{k_b} Z_b}} \cdot 2^{k_b} = (1+\delta)^{|(V \setminus W) \cup W_b|} \cdot \sqrt{\frac{2^{k_b}}{Z_b}} \\
&\geq (1+\delta)^{|(V \setminus W) \cup W_b|} \cdot \frac{1}{\sqrt{(1 + 2\delta + \delta^2 \cdot 2^{d-k_0})^{(|(V \setminus W) \cup W_b|)}}} \\
&\geq \frac{(1+\delta)^n}{(1 + 2\delta + \delta^2 2^{(d-k_0)})^{\frac{n}{2}}}.
\end{aligned}$$

Above, last inequality holds since $|(V \setminus W) \cup W_b| \leq n$. □

Thus, if δ is small enough, it suffices to understand the properties of the space

$$\mathcal{G}' := \text{span}\left(|\Phi_b\rangle, \text{ such that } b \in \{0,1\}^{|R|}\right).$$

From Claim 8, each $|\Phi_b\rangle$ is a superposition over 2^{k_b} edge assignments. Moreover, each such edge assignment satisfies all the checks in $V' := V \setminus W$. Thus, let us understand the properties of edge assignments that satisfy such checks. Define a new Tanner code $T' := T(C, G')$, where $G' = (V', E' \cup F)$, E' is the set of edges in the subgraph induced by V' and F is the set of edges which connected V' with W. We will think of each edge in F as 'free', being incident to just one vertex in V' (Figure 4). Theorem 9 below shows that the Hamming distance between the codewords of T' is either small or large.

B. Properties of the Tanner code T'

Let $I \subset V'$ be the set of vertices on which an edge in F is incident (Figure 4). From Eq. 2, note the following bounds

$$|I| \leq |F| \leq d|W| \leq 2d\varepsilon|E| \text{ and } |E| \geq |E'| \geq |E_1| - d|W| \geq |E|(1 - 3d\varepsilon). \tag{5}$$

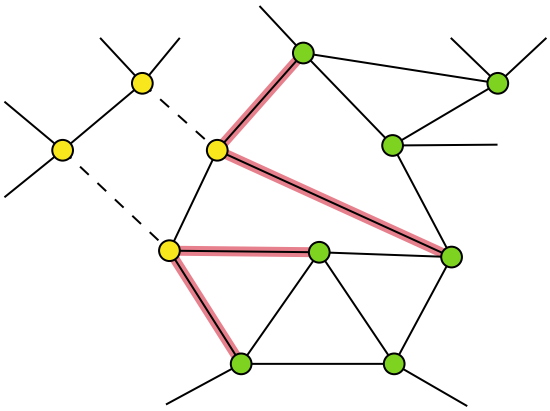

FIG. 4: Any edge assignment appearing in $|\Phi_b\rangle$ still satisfies all the checks at the green vertices (V'). If we restrict to V', the shaded edges have only one end-point in V'. We will call such edges F. $I \subset V'$ is the set of vertices on which the edges in F are incident. In Theorem 9, some care is needed in analyzing the Hamming weight of edge assignments satisfying checks on V', as vertices in I are responsible for the breakdown of expansion in V'. While checks on I are satisfied, this may happen due to edges in F and may not contribute to expansion.

Since G' may no longer be an expander, we do not have any guarantees on the distance of T'. But we can show some structure in the codewords of T'.

Theorem 9. *Suppose $\varepsilon \leq \frac{1}{6d}$ and $\Delta_0 \geq 4\lambda$. The Hamming distance between the codewords of T' is either $\leq 8d^2\varepsilon|E' \cup F|$ or $\geq \frac{\Delta_0^2}{4d^2} \cdot |E' \cup F|$.*

Proof. Since T' is a linear code, we show that the Hamming weight of a non-zero codeword x is either $\leq 8d^2\varepsilon|E' \cup F|$ or $\geq \frac{\Delta_0^2}{8d^2} \cdot |E' \cup F|$. Let $J_x \subset E' \cup F$ be the set of edges on which x assigns 1. Suppose $|J_x| \leq 8d^2\varepsilon|E' \cup F|$; then we are done. Else

$$|J_x| \geq 8d^2\varepsilon|E' \cup F| \geq 8d^2\varepsilon|E'| \overset{Eq.5}{\geq} 8d^2\varepsilon|E|\,(1 - 3d\varepsilon) \geq 4d^2\varepsilon|E|.$$

We consider this case and show that $|J_x|$ must be significantly larger. Let $S \subset V'$ be the vertices on which the edges in J_x are incident. We can apply expander mixing lemma to the *original graph* G and obtain

$$|E(S,S)| \leq \frac{d|S|^2}{n} + \lambda|S|.$$

On the other hand, we can lower bound $|E(S,S)|$ as follows. Every vertex in $S \setminus I$ has degree at least Δ_0 and each edge incident to such a vertex belongs to $E(S,S)$ (since such an edge

is not in F, both its endpoint are in S). Edges incident to vertices in $S \cap I$ may not belong to $E(S,S)$, thus we won't count them (see Figure 4). Overall, we have

$$|E(S,S)| \geq \Delta_0 |S \setminus I| \overset{Eq.5}{\geq} \Delta_0(|S| - 2d\varepsilon|E|) = \Delta_0 \left(\frac{|S|}{2} + \frac{|S|}{2} - 2d\varepsilon|E| \right). \tag{6}$$

Since $|J_x| \geq 4d^2\varepsilon|E|$, we can naively bound $|S| \geq \frac{|J_x|}{d} \geq 4d\varepsilon|E|$. Thus,

$$\frac{d|S|^2}{n} + \lambda|S| \geq |E(S,S)| \overset{Eq.6}{\geq} \frac{\Delta_0}{2}|S| \overset{\lambda \leq \frac{\Delta}{4}}{\Longrightarrow} |S| \geq \frac{n\Delta_0}{4d}.$$

From here, we obtain

$$|J_x| \overset{(1)}{\geq} \frac{\Delta_0|S|}{2} \geq \frac{n\Delta_0^2}{8d} = |E| \cdot \frac{\Delta_0^2}{4d^2} \geq |E' \cup F| \cdot \frac{\Delta_0^2}{4d^2}.$$

Here, (1) follows since every vertex in S is associated to at least Δ_0 edges in J_x and every edge in J_x is associated to at most 2 vertices in S. This completes the proof. □

C. Structure of the states $|\Phi_b\rangle$

Recall that $|\Phi_b\rangle$ is a superposition over the edge assignments to $E_1 \cup R$. We now show that these edge assignments form distant clusters.

Theorem 10. *Suppose $\varepsilon \leq \frac{\Delta_0^2}{300d^4}$ and $\Delta_0 \geq 4\lambda$. There are disjoint sets $B_1, B_2, \ldots \subset \{0,1\}^{|E_1 \cup R|}$ such that for any $x, y \in B_i$, the Hamming distance between x and y is $\leq 10d^2\varepsilon|E_1 \cup R|$ and for any $x \in B_i$ and $y \in B_j$ with $i \neq j$, the Hamming distance between x, y is $\geq \frac{\Delta_0^2}{10d^2} \cdot |E_1 \cup R|$. Furthermore, the states $\{|\Phi_b\rangle\}_{b \in \{0,1\}^{|R|}}$ are uniform superpositions over some edge assignments in $\cup_i B_i$.*

Proof. Any two edge assignments x, y appearing in $|\Phi_b\rangle$, when restricted to the edges in G' (which we denote $x_{G'}, y_{G'}$), belong to T'. The edge assignment x is obtained from $x_{G'}$ by appending assignments to the edges in $(E_1 \cup R) \setminus (E' \cup F)$. There are at most $d|W| \overset{Eq.2}{\leq} 2d\varepsilon|E|$ such edges. Thus, invoking Theorem 9, the Hamming distance between x, y is either at most

$$8d^2\varepsilon|E' \cup F| + 2d\varepsilon|E| \leq 8d^2\varepsilon|E_1 \cup R| + 2d\varepsilon|E| \overset{Eq2}{\leq} 8d^2\varepsilon|E_1 \cup R| + 2d\varepsilon|E_1 \cup R| \leq 10d^2\varepsilon|E_1 \cup R|$$

or at least

$$\begin{aligned} &\frac{\Delta_0^2}{4d^2} \cdot |E' \cup F| - 2d\varepsilon|E| \geq \frac{\Delta_0^2}{4d^2} \cdot |E_1 \cup R| - \frac{\Delta_0^2}{4d^2} \cdot 2d\varepsilon|E| - 2d\varepsilon|E| \\ &\overset{Eq.2}{\geq} \frac{\Delta_0^2}{4d^2} \cdot |E_1 \cup R| - 4d\varepsilon|E_1 \cup R| \geq \frac{\Delta_0^2}{10d^2} \cdot |E_1 \cup R|. \end{aligned}$$

Next, consider a relation $\mathcal{R}$ between the edge assignments: $x, y \in \mathcal{R}$ if the Hamming distance between them is $\leq 10d^2\varepsilon|E_1 \cup R|$. The relation is transitive: $x, y \in \mathcal{R}$ and $y, z \in \mathcal{R}$ implies the Hamming distance between x, z is $\leq 20d^2\varepsilon|E_1 \cup R| < \frac{\Delta_0^2}{10d^2} \cdot |E_1 \cup R|$, which in turn requires that the Hamming distance between x, z is $\leq 10d^2\varepsilon|E_1 \cup R|$. This forces $x, z \in \mathcal{R}$. The sets $B_1, B_2, \ldots$ are the equivalence classes formed by this relation, which completes the proof. □

Let

$$\Pi_{B_i} := \sum_{x \in B_i} \bigotimes_{e \in E_1} |x_e\rangle\langle x_e|_e \bigotimes_{r \in R} |x_r\rangle\langle x_r|_r$$

be the projector onto the edge assignments in B_i. The following claim holds.

Claim 11. Let $\delta^2 \leq \frac{2^{-d}}{10000n}$, $\varepsilon \leq \frac{1}{20000d^2}$ and $k_0 \geq 0.55d$. For any i and any $b, b' \in \{0,1\}^{|R|}$ (with $b \neq b'$), $\langle\Psi_b| \Pi_{B_i} |\Psi_b\rangle \leq \frac{1}{50}$ and $\langle\Psi_b| \Pi_{B_i} |\Psi_{b'}\rangle = 0$.

Proof. Since $|\Phi_b\rangle$ is a uniform superposition over 2^{k_b} edge assignments and the size of each B_i is at most $\binom{|E_1 \cup R|}{10d^2\varepsilon|E_1 \cup R|} \leq 2^{2d\sqrt{10\varepsilon}|E_1 \cup R|} \leq 2^{8d\sqrt{\varepsilon}|E|}$, we have

$$\langle\Phi_b| \Pi_{B_i} |\Phi_b\rangle \leq 2^{-k_b} \cdot 2^{8d\sqrt{\varepsilon}|E|} \overset{Claim 8}{\leq} 2^{8d\sqrt{\varepsilon}|E| - 0.1|E| + |R|} \overset{Eq. 2}{\leq} 2^{10d\sqrt{\varepsilon}|E| - 0.1|E|} \leq \frac{1}{100}.$$

Above, the last inequality assumes that $|E|$ is larger than some constant. Now, Claim 8 ensures that

$$|\langle\Phi_b|\Psi_b\rangle| \geq \frac{(1+\delta)^n}{(1 + 2\delta + \delta^2 2^{(d-k_0)})^{\frac{n}{2}}} \geq \left(\frac{1}{1 + 2^d\delta^2}\right)^{\frac{n}{2}} \geq e^{-\frac{1}{20000}} \geq 1 - \frac{1}{10000}.$$

Thus, $\frac{1}{2}\| |\Phi_b\rangle\langle\Phi_b| - |\Psi_b\rangle\langle\Psi_b| \|_1 \leq \frac{1}{100}$, which ensures that

$$\mathrm{Tr}\left(\Pi_{B_i} |\Psi_b\rangle\langle\Psi_b|\right) \leq \mathrm{Tr}\left(\Pi_{B_i} |\Phi_b\rangle\langle\Phi_b|\right) + \frac{1}{100} \leq \frac{1}{50}.$$

To argue that $\langle\Psi_b| \Pi_{B_i} |\Psi_{b'}\rangle = 0$, note that $|\Psi_b\rangle$ is a superposition over edge assignments with the fixed b on the edges in R. That is, $|\Psi_b\rangle = |\ldots\rangle \otimes_{r \in R} |b_r\rangle_r$. Thus, Π_{B_i}, being a projector onto computational basis states, satisfies $\Pi_{B_i} |\Psi_b\rangle = |\ldots\rangle \otimes_{r \in R} |b_r\rangle_r$. Similarly, $|\Psi_{b'}\rangle = |\ldots'\rangle \otimes_{r \in R} |b'_r\rangle_r$. Since $b \neq b'$, the claim follows. □

D. Circuit lower bound

We will assume that $\varepsilon \leq \frac{1}{20000d^2}, \frac{\Delta_0^2}{300d^4}$; $\Delta_0 \geq 4\lambda$; $k_0 \geq 0.55d$ and $\delta^2 \leq \frac{2^{-d}}{10000n}$. Note that these conditions can be met with constant k_0, Δ_0, d, which ensures that ε is a constant (see Section V). Our main theorem is below, which proves that H is cNLTS. The argument is directly inspired by the quantum circuit lower bound argument in[12], based on the partitioning of quantum codewords. However, we consider a simpler argument based on the tight polynomial approximations to the AND function[4,10,16], inspired by[17].

Theorem 12. *Let $|\rho\rangle = U|0\rangle^{\otimes m}$ on $m \geq nd$ qubits, where U is a depth t quantum circuit, such that $\frac{1}{2}\| |\Gamma\rangle\langle\Gamma| - |\rho\rangle\langle\rho| \|_1 \leq 0.1$ for some ground state[25] $|\Gamma\rangle$ of H_1. It holds that*

$$t = \Omega\left(\log \frac{n\Delta_0^4}{d^3}\right).$$

Proof. Note that $m \leq 2^t nd$ without loss of generality, as H_1 acts on nd qubits (see[7] (Section 2.3) for a justification based on the light cone argument). We can expand

$$|\Gamma\rangle = \sum_{b\in\{0,1\}^{|R|}} |\mu_b\rangle \otimes |\Psi_b\rangle,$$

such that $\sum_{b\in\{0,1\}^{|R|}} \| |\mu_b\rangle \|^2 = 1$. The (possibly unnormalized) vectors $|\mu_b\rangle$ act on $m - nd$ qubits outside V. Using Claim 11, we find that for any i,

$$\langle\Gamma| \Pi_{B_i} |\Gamma\rangle = \sum_{b,b'\in\{0,1\}^{|R|}} \langle\mu_{b'}|\mu_b\rangle \langle\Psi_{b'}| \Pi_{B_i} |\Psi_b\rangle = \sum_{b\in\{0,1\}^{|R|}} \| |\mu_b\rangle \|^2 \langle\Psi_b| \Pi_{B_i} |\Psi_b\rangle \leq \frac{1}{50}. \quad (7)$$

On the other hand, all edge assignments over $E_1 \cup R$ appearing in $|\Gamma\rangle$ belong to some B_i. In other words, $\sum_i \langle\Gamma| \Pi_{B_i} |\Gamma\rangle = 1$. Thus, we can find two disjoint sets of indices M, M', such that

$$\sum_{i\in M} \langle\Gamma| \Pi_{B_i} |\Gamma\rangle \geq \frac{1}{2} - \frac{1}{50} \geq \frac{1}{3}, \quad \sum_{i\in M'} \langle\Gamma| \Pi_{B_i} |\Gamma\rangle \geq \frac{1}{2} - \frac{1}{50} \geq \frac{1}{3}.$$

Define $B_M = \cup_{i\in M} B_i$, $B_{M'} = \cup_{i\in M'} B_i$, $\Pi_M = \sum_{i\in M} \Pi_{B_i}$ and $\Pi_{M'} = \sum_{i\in M'} \Pi_{B_i}$. From Theorem 10, the Hamming distance between the sets B_M and $B_{M'}$ is $\geq \frac{\Delta_0^2}{10d^2} \cdot |E_1 \cup R| \geq \frac{\Delta_0^2}{20d^2} \cdot nd$. On the other hand, we just established that $\langle\Gamma| \Pi_M |\Gamma\rangle \geq \frac{1}{3}$ and $\langle\Gamma| \Pi_{M'} |\Gamma\rangle \geq \frac{1}{3}$. From[4,10,16], there exists a $f \cdot 2^t$-local operator L such that

$$\| |\rho\rangle\langle\rho| - L \|_\infty \leq e^{-\frac{f^2}{2^t \cdot 100nd}}.$$

Setting $f \cdot 2^t = \frac{\Delta_0^2}{100d^2} \cdot nd$, we obtain

$$\| |\rho\rangle\langle\rho| - L\|_\infty \leq e^{-n \cdot \frac{\Delta_0^4}{2^{3t} \cdot 10^6 d^3}}.$$

Since $\Pi_M L \Pi_{M'} = 0$, we have

$$\|\Pi_M |\rho\rangle\langle\rho| \Pi_{M'}\|_\infty \leq e^{-n \cdot \frac{\Delta_0^4}{2^{3t} \cdot 10^6 d^3}}.$$

However

$$\begin{aligned}\|\Pi_M |\rho\rangle\langle\rho| \Pi_{M'}\|_\infty &= \sqrt{\langle\rho| \Pi_M |\rho\rangle \cdot \langle\rho| \Pi_{M'} |\rho\rangle} \\ &\geq \sqrt{(\langle\Gamma| \Pi_M |\Gamma\rangle - 0.1) \cdot (\langle\Gamma| \Pi_{M'} |\Gamma\rangle - 0.1)} \geq e^{-2}.\end{aligned}$$

Thus, $2^{3t} \geq n \cdot \frac{\Delta_0^4}{2 \cdot 10^6 \cdot d^3}$, which completes the proof. □

V. EXPLICIT CONSTRUCTION OF THE TANNER CODE $T(C, G)$

In this section we give an explicit construction of a suitable family of Tanner codes $\{T(C, G_i)\}_{i=1}^\infty$ from which the family of cNLTS-Hamiltonians $\{H^{(i)}\}_{i=1}^\infty$ of Theorem 3 is obtained.

For the graphs G_i underlying the Tanner codes, we employ a construction of spectral Cayley-expanders due to Lubotzky, Phillips and Sarnak.

Theorem 13 ([20]). *Assume that p and q are distinct, odd primes such that $q > 2\sqrt{p}$ and q is a square modulo p. Then there exists a symmetric generating set Γ of $\mathrm{PSL}_2(\mathbb{F}_q)$ such that the Cayley graph $\mathrm{Cay}(\mathrm{PSL}_2(\mathbb{F}_q), \Gamma)$ is a non-bipartite, $p+1$-regular expander graph with $\lambda < 2\sqrt{p}$.*

By fixing a suitable prime p we obtain a family of regular graphs G_i of degree $d = p + 1$ and order $q(q^2 - 1)/2$ with spectral bound $\lambda < 2\sqrt{d-1}$. We mention in passing that by a result due to Alon and Boppana, this is the best possible bound that any family of regular graphs can achieve and such families are called *Ramanujan graphs*.

Further, we require a linear, binary code C. More specifically, for the construction of the cNLTS-Hamiltonians to go through, we require the existence of a classical linear binary code C of block size d encoding at least $k_0 \geq 0.55\, d$ bits with distance $\Delta_0 \geq 4\lambda$. As the degree d of the graphs is constant, it suffices to show that a suitable code C exist, as a brute-force search has time-complexity bounded by a constant $O(1)$. The existence of a suitable code is guaranteed by the Gilbert–Varshamov bound (see e.g.[36] (Chapter 5) for a proof).

Theorem 14 (Gilbert-Varshamov). *Let* $0 \leq \mu \leq 0.5$ *and let* $0 \leq R_0 \leq 1 - H_2(\mu)$*, then there exists a binary, linear code of block size* d*, rank* $k_0 = R_0 d$ *and distance* $\Delta_0 = \mu d$*.*

We can now give an explicit construction of a suitable code family $\{T(C, G_i)\}_{i=1}^{\infty}$. By Theorem 14 there exists a code C encoding $k_0 \geq 0.55d$ bits when $\mu \leq 0.09$. We further require that C has distance $\Delta_0 = \mu d \geq 4\lambda$. This is the case via Theorem 13 by choosing, for example, $\mu = 0.09$ and prime $p = 7901$.

Acknowledgement

We thank Chinmay Nirkhe for helpful discussions. We also thank Robbie King and the anonymous referee for carefully reading our manuscript. AA acknowledges support through the NSF award QCIS-FF: Quantum Computing & Information Science Faculty Fellow at Harvard University (NSF 2013303). NPB acknowledges support through the EPSRC Prosperity Partnership in Quantum Software for Simulation and Modelling (EP/S005021/1).

REFERENCES

[1] Aharonov, D., Arad, I., and Vidick, T., SIGACT News **44**, 47–79 (2013).

[2] Aharonov, D. and Eldar, L., SIAM Journal on Computing **44**, 1230 (2015), https://doi.org/10.1137/140975498.

[3] Aharonov, D. and Naveh, T., "Quantum NP - A Survey," (2002), arXiv:quant-ph/0210077.

[4] Anshu, A., Arad, I., and Gosset, D., in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2022 (Association for Computing Machinery, New York, NY, USA, 2022) p. 12–18.

[5] Anshu, A., Breuckmann, N. P., and Nirkhe, C., "NLTS Hamiltonians from good quantum codes," (2022).

[6] Anshu, A., Gosset, D., Morenz Korol, K. J., and Soleimanifar, M., Phys. Rev. Lett. **127**, 250502 (2021).

[7] Anshu, A. and Nirkhe, C., in *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 215, edited

by M. Braverman (Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2022) pp. 6:1–6:22.

[8]Bravyi, S., Kliesch, A., Koenig, R., and Tang, E., https://arxiv.org/abs/1910.08980 (2019).

[9]Breuckmann, N. P. and Eberhardt, J. N., IEEE Transactions on Information Theory **67**, 6653 (2021).

[10]Buhrman, H., Cleve, R., De Wolf, R., and Zalka, C., *Proc. of FOCS 99'*, , 358 (1999).

[11]Eldar, L., in *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 185, edited by J. R. Lee (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2021) pp. 49:1–49:20.

[12]Eldar, L. and Harrow, A. W., in *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)* (2017) pp. 427–438.

[13]Fernández-González, C., Schuch, N., Wolf, M. M., Cirac, J. I., and Pérez-García, D., Communications in Mathematical Physics **333**, 299 (2015).

[14]Freedman, M. H. and Hastings, M. B., Quantum Info. Comput. **14**, 144–180 (2014).

[15]Hastings, M. B., Haah, J., and O'Donnell, R., "Fiber Bundle Codes: Breaking the $\sqrt{n}polylog(n)$ Barrier for Quantum LDPC Codes," in *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing* (Association for Computing Machinery, New York, NY, USA, 2021) p. 1276–1288.

[16]Kahn, J., Linial, N., and Samorodnitsky, A., Combinatorica **16**, 465 (1996).

[17]Kuwahara, T., Arad, I., Amico, L., and Vedral, V., Quantum Science and Technology **2**, 015005 (2017).

[18]LaRose, R., Tikku, A., O'Neel-Judy, É., Cincio, L., and Coles, P. J., npj Quantum Information **5**, 57 (2019).

[19]Leverrier, A., Londe, V., and Zémor, G., Quantum **6**, 661 (2022).

[20]Lubotzky, A., Phillips, R., and Sarnak, P., Combinatorica **8**, 261 (1988).

[21]Meshulam, R., arXiv preprint arXiv:1803.05643 (2018).

[22]Nirkhe, C., Vazirani, U., and Yuen, H., in *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 107, edited by I. Chatzigiannakis, C. Kaklamanis, D. Marx, and

D. Sannella (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2018) pp. 91:1–91:11.

[23]One may note that the local terms of the resulting parent Hamiltonian do not have norm ≤ 1 and may scale as $\frac{1}{\delta}$. But we can fix this by the standard trick of replacing each local term by the projector onto its image. Frustration-free property of the parent Hamiltonian ensures that the ground state is unchanged.

[24]This would happen iff the edge assignment b were simply inconsistent with the codewords allowed at v. For example, v may connect with $d-1$ edges in R and b may assign $\Delta_0 - 2$ number of '1's on those edges.

[25]While $|\Gamma\rangle$ may act on more qubits than included in V, we say that $|\Gamma\rangle$ is a ground state of H_1 if its reduced state on the qubits in V belongs to the ground space of H_1.

[26]Orus, R., Annals of Physics **349**, 117 (2014).

[27]Panteleev, P. and Kalachev, G., "Quantum LDPC Codes with Almost Linear Minimum Distance," (2020), 2012.04068.

[28]Panteleev, P. and Kalachev, G., "Asymptotically Good Quantum and Locally Testable Classical LDPC Codes," (2021), to appear in STOC 2022.

[29]Pastawski, F., Yoshida, B., Harlow, D., and Preskill, J., Journal of High Energy Physics **2015**, 149 (2015).

[30]Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., Aspuru-Guzik, A., and O'Brien, J. L., Nature Communications **5**, 4213 (2014).

[31]Schuch, N., Wolf, M. M., Verstraete, F., and Cirac, J. I., Phys. Rev. Lett. **98**, 140506 (2007).

[32]Sipser, M. and Spielman, D., IEEE Transactions on Information Theory **42**, 1710 (1996).

[33]Steenrod, N. E., Annals of Mathematics , 610 (1943).

[34]Tillich, J. and Zemor, G., in *2009 IEEE International Symposium on Information Theory* (2009) pp. 799–803.

[35]Vadhan, S. P., Foundations and Trends in Theoretical Computer Science **7**, 1 (2012).

[36]Van Lint, J. H., *Introduction to Coding Theory*, Vol. 86 (Springer Science & Business Media, 2012).