How much entanglement is needed for quantum error correction?

Sergey Bravyi,[1] Dongjin Lee,[2,3] Zhi Li,[2] and Beni Yoshida[2]

[1] *IBM Quantum, IBM T. J. Watson Research Center, Yorktown Heights, NY 10598, USA*
[2] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*
[3] *Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*

It is commonly believed that logical states of quantum error-correcting codes have to be highly entangled such that codes capable of correcting more errors require more entanglement to encode a qubit. Here we show that this belief may or may not be true depending on a particular code. To this end, we characterize a tradeoff between the code distance d quantifying the number of correctable errors, and geometric entanglement of logical states quantifying their maximal overlap with product states or more general "topologically trivial" states. The maximum overlap is shown to be exponentially small in d for three families of codes: (1) low-density parity check (LDPC) codes with commuting check operators, (2) stabilizer codes, and (3) codes with a constant encoding rate. Equivalently, the geometric entanglement of any logical state of these codes grows at least linearly with d. On the opposite side, we also show that this distance-entanglement tradeoff does not hold in general. For any constant d and k (number of logical qubits), we show there exists a family of codes such that the geometric entanglement of some logical states approaches zero in the limit of large code length.

Quantum error correction [1] and entanglement theory are vibrant research fields that are often closely interlinked. A deep connection between the two fields stems from the hallmark feature of entangled states known as local indistinguishability [2, 3]— two entangled states may be perfectly distinguishable globally while looking identical for any local observer who can only examine few-qubit subsystems. Accordingly, a logical qubit encoded into entangled states that span multiple physical qubits and satisfy the local indistinguishability property becomes protected from all few-qubit errors enabling error correction.

The exchange of ideas between these fields has led to several breakthroughs. For example, the study of many-body entangled states with a topological quantum order [4] has led to the development of fault-tolerant architectures based on the surface code [5, 6]. Conversely, coding theory constructions such as holographic quantum codes [7, 8] provided a fruitful perspective on the connection between geometry and entanglement in quantum gravity. More recently, one of the most significant open questions about many-body entanglement — the existence of local Hamiltonians without low-energy topologically trivial states [9] has been resolved by employing the construction of good Low Density Parity Check (LDPC) codes [10, 11].

Given the profound role of entanglement in quantum coding theory, a natural question is *how much entanglement is needed for quantum error correction?* Here we begin addressing this question by exploring distance-entanglement tradeoffs for quantum codes. Recall that a quantum code encoding k logical qubits into n physical qubits is simply a linear subspace $\mathcal{C}$ of dimension 2^k embedded into the 2^n-dimensional Hilbert space describing n physical qubits. Any normalized vector $|\psi\rangle \in \mathcal{C}$ represents a logical (encoded) state. The error correcting capability of a code is usually measured by its *distance*. A code is said to have distance d if logical states are locally indistinguishable on any subset of less than d physical qubits. Put differently, the reduced density matrix of a logical state $|\psi\rangle \in \mathcal{C}$ describing any subset of less than d qubits is the same for all logical states. A distance-d code can correct any error affecting less than $d/2$ physical qubits [2, 3, 12]. It is easy to check that logical states of non-trivial codes (those with $k \geq 1$ and $d \geq 2$) must have *some* entanglement [13]. But what is the minimum amount of entanglement required for a distance-d code?

First, let us agree on how to quantify the entanglement of n-qubit states. Our starting point is the geometric entanglement measure [14, 15]. It quantifies the maximum overlap between a given n-qubit state and tensor products of single-qubit states. Unfortunately, this measure can be "spoofed" by states exhibiting only short-range entanglement. For example, a tensor product of $n/2$ EPR pairs scores high on the geometric entanglement even though this state can be disentangled by applying a single layer of CNOT gates. To detect genuine many-body entanglement we generalize the geometric entanglement beyond product states. For any $h \geq 1$ define a depth-h quantum circuit acting on n qubits as a composition of h layers of two-qubit gates such that gates within each layer are non-overlapping. We allow two-qubit gates acting on any pair of qubits (all-to-all qubit connectivity). A depth-0 circuit is defined as a product of single-qubit gates. Define a depth-h Geometric Entanglement Measure (GEM) of an n-qubit state $|\psi\rangle$ as

$$E_h(\psi) = - \max_{U\,:\,\mathrm{depth}(U)=h} \log_2 |\langle\psi|U|0^n\rangle|^2. \qquad (1)$$

The maximum is taken over all n-qubit depth-h circuits. By definition, $E_h(\psi) \in [0, n]$ and $E_h(\psi) = 0$ iff $|\psi\rangle$ can be prepared by a depth-h circuit. We shall be interested in the regime when $h = O(1)$ is a constant independent of n. Then $E_h(\psi)$ quantifies the maximum overlap between $|\psi\rangle$ and "topologically trivial" states [9], i.e. states that can be prepared by a constant-depth circuit starting from a product state. The standard GEM coincides with $E_0(\psi)$, see e.g. [15]. We shall also consider Clifford GEM $E_h^C(\psi)$ defined by Eq. (1) with a restriction that U contains only Clifford gates (Hadamard, CNOT, and $S=\sqrt{Z}$).

I. MAIN RESULTS

First, consider quantum LDPC (qLDPC) codes. Such codes are often used to model systems with topological quantum order, see e.g. [5, 16]. The codespace $\mathcal{C}$ of a qLDPC code with n physical qubits is defined as

$$\mathcal{C}=\{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,:\, \Pi_a|\psi\rangle = |\psi\rangle \;\; \forall\, a=1,\ldots,m\} \quad (2)$$

where $\Pi_1,\ldots,\Pi_m$ are pairwise commuting Hermitian projectors. Equivalently, $\mathcal{C}$ is the ground subspace of a gapped Hamiltonian $H=-\sum_{a=1}^m \Pi_a$. The code is said to have *sparsity* s if each projector Π_a acts non-trivially on at most s qubits and each qubit participates in at most s projectors. The LDPC condition demands that s is a constant independent of n.

Our first result is the distance-entanglement tradeoff for qLDPC codes:

Theorem 1. *For any $d>s^4 2^{5h}$, any s-sparse, distance-d qLDPC code $\mathcal{C}$, and any logical state $|\psi\rangle\in\mathcal{C}$ one has*

$$E_h(\psi)\ge \alpha d, \quad (3)$$

where $\alpha>0$ is a constant that depends only on s and h.

As a consequence, the overlap between any logical state and any topologically trivial state is exponentially small in d. Moreover, since the bound Eq. (3) does not depend on the number of physical qubits n, the constant depth circuit that creates a topologically trivial state may act on an arbitrary number of ancillary qubits initialized in $|0\rangle$. The bound Eq. (3) confirms the belief that high-distance codes capable of correcting more errors require more entanglement to encode a qubit. We emphasize that this bound is extremely general as it applies to *all* qLDPC codes. The linear scaling with d in Eq. (3) cannot be improved since $E_h(\psi)\le n$ for any state $|\psi\rangle$ and there exist qLDPC codes with the distance $d\sim n$ [11]. Although the bound Eq. (3) is easy to state, its proof is rather non-trivial. It combines the characterization of entanglement present in logical states of qLDPC codes stated as the Disentangling Lemma in [17] and the Hamming weight concentration bound for shallow peaked quantum circuits (slightly improved upon [18]).

Our second result is the distance-entanglement tradeoff for stabilizer codes [19]. The codespace $\mathcal{C}$ of a stabilizer code with n physical qubits is defined as

$$\mathcal{C}=\{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,:\, S_a|\psi\rangle = |\psi\rangle \;\; \forall\, a=1,\ldots,m\} \quad (4)$$

where $S_a\in\{\pm 1\}\cdot\{I,X,Y,Z\}^{\otimes n}$ are pairwise commuting Pauli operators and $m=n-k$. We show that

Theorem 2. *For any stabilizer code $\mathcal{C}$ and any logical state $|\psi\rangle\in\mathcal{C}$ one has*

$$E_0(\psi)\ge d-1. \quad (5)$$

As a consequence, the overlap between any logical state and any n-qubit product state is at most 2^{1-d}. Moreover, this bound is tight as it can be saturated exactly by Shor's code [1], see Appendix A for details. The proof of Eq. (5), which relies on the Cleaning Lemma [20], is pleasingly simple. Although we were not able to prove a lower bound $\Omega(d)$ for the depth-h GEM, a simple corollary of Eq. (5) is

$$E_h^C(\psi)\ge \frac{d}{2^h}-1. \quad (6)$$

In other words, the overlap between any logical state and any n-qubit state that can be prepared by a depth-h Clifford circuit is at most $2^{1-d/2^h}$, exponentially small in d for any constant depth h.

While the above results depend only on d (but not k), our third result contains k-dependent lower bounds, which is particularly useful for codes with constant rates. Let $H(x)=-x\log_2 x-(1-x)\log_2(1-x)$, and $H^{-1}(x)$ be its inverse function restricting to $x\in[0,\frac{1}{2}]$.

Theorem 3. *(i) For any code $\mathcal{C}$ and any logical state $|\psi\rangle\in\mathcal{C}$ one has*

$$E_h(\psi)\ge\Big(\frac{d}{2^h}-1\Big)H^{-1}\Big(\frac{k}{n}\Big). \quad (7)$$

(ii) For a qLDPC code such that $d>s^4 2^{5h}$,

$$E_h(\psi)\ge \beta n H^{-1}\Big(\frac{k}{n}\Big). \quad (8)$$

where $\beta=\Theta(s^{-4}2^{-4h})>0$ is a constant that depends only on s and h.

In particular, if the code has constant rate $k/n=\Theta(1)$, then for general codes, we have

$$E_h(\psi)\ge\Theta\Big(\frac{d}{2^h}\Big); \quad (9)$$

for qLDPC code such that $d>s^4 2^{5h}$, we have

$$E_h(\psi)\ge\Theta\Big(\frac{n}{2^{4h}}\Big). \quad (10)$$

Eq.(7) is proved by combining an entropic argument inspired by [17, 21] and a general observation about making measurements on a code. Eq.(8) relies on similar ideas towards Eq. (3).

Finally, one might expect that a similar distance-entanglement tradeoff holds for all quantum codes. Surprisingly, we show that this is not the case. To this end, we consider Permutation Invariant (PI) codes [22, 23]. Logical states of such codes are invariant under any permutation of physical qubits. We construct a family of distance-2 PI codes $\mathcal{C}_n$ encoding $k=1$ logical qubit into n physical qubits and a family of logical states $|\psi_n\rangle \in \mathcal{C}_n$ with an asymptotically vanishing GEM:

$$E_0(\psi_n) \le \frac{O(1)}{n}. \tag{11}$$

Hence the overlap between $|\psi_n\rangle$ and some n-qubit product state approaches 1 in the limit $n \to \infty$. By concatenating the code $\mathcal{C}_n$ with itself several times we obtain a family of codes with arbitrarily large d and k such that a logical state obeys $E_0(\psi_n) \to 0$ as $n \to \infty$. This example shows that some logical states of high-distance codes may have very little entanglement.

Related works. Circuit lower bounds for low-energy states of quantum code Hamiltonians have been studied before by many authors [9, 10, 21, 24, 25]. Upper bounds on the overlap between logical states and low-depth states similar to ours were reported by Anshu and Nirkhe [21] who showed $E_h(\psi) \ge \Theta(\frac{k^2 d}{n^2 s 2^{4h} \log^4 ds})$ for quantum LDPC codes (Lemma 13 therein). Compared with Eq. (3), this bound depends on the code length n and is sub-linear in d (even up to logarithm) unless the code has constant rate k/n, in which case the LDPC condition is actually not necessary, see Eq. (9). Ref. [21] also showed $E_h(\psi) \ge \Theta(d^2/n2^{2h})$ for any code (Lemma 14 therein). In particular, $E_h(\psi) \ge \Theta(d)$ for codes with linear distance and $h = O(1)$, which complements our results. Ref. [26] used GEM to probe quantum phase transitions in several 1D spin chain models, see also [27–29]. Ref. [15] studied GEM for some examples of topological quantum codes. In an accompanying work [30], we will study the GEM E_h for many-body systems that support emergent anyons and fermions.

II. PROOFS

We proceed to the proof of the distance-entanglement tradeoffs stated above.

A. Stabilizer codes

We begin with Theorem 2 since its proof is the simplest one. Suppose $\mathcal{C}$ is a stabilizer code with distance d and $|\psi\rangle \in \mathcal{C}$ is a logical state. By definition, $2^{-E_0(\psi)} = \langle\psi|\rho|\psi\rangle$ for some product state $\rho = \rho_1 \otimes \cdots \otimes \rho_n$. Partition n qubits into two disjoint registers A, B and let $\rho_A = \mathrm{Tr}_B \rho$. Since ρ is a product state, one has $\rho \le \rho_A \otimes I_B$. Accordingly,

$$2^{-E_0(\psi)} = \langle\psi|\rho|\psi\rangle \le \langle\psi|\rho_A \otimes I_B|\psi\rangle = \mathrm{Tr}(\rho_A \eta_A), \tag{12}$$

where $\eta = |\psi\rangle\langle\psi|$ and $\eta_A = \mathrm{Tr}_B \eta$. Suppose $|A| < d$. The local indistinguishability property implies that the reduced density matrix η_A is the same for all logical states. Thus one can compute η_A by pretending that η is the maximally mixed logical state $\eta = (1/2^k)\Pi_{\mathcal{C}}$, where $\Pi_{\mathcal{C}}$ is the projector onto $\mathcal{C}$. It is well known [12] that

$$\Pi_{\mathcal{C}} = \frac{1}{2^{n-k}} \sum_{S \in \mathcal{S}} S, \tag{13}$$

where $\mathcal{S} = \langle S_1, \ldots, S_m\rangle$ is the stabilizer group of $\mathcal{C}$. Taking the partial trace over B gives

$$\eta_A = \frac{1}{2^k} \mathrm{Tr}_B \Pi_{\mathcal{C}} = \frac{1}{2^{|A|}} \sum_{S \in \mathcal{S}(A)} S, \tag{14}$$

where $\mathcal{S}(A)$ is the subgroup of $\mathcal{S}$ that includes all stabilizers supported on A. We shall need the following lemma.

Lemma 1. *For any distance-d stabilizer code, there exists a subset of qubits A such that $|A| \ge d$ and the only stabilizer supported on A is the identity operator.*

Applying Eqs. (12,14) to a subset of qubits A such that $\mathcal{S}(A) = \{I\}$ and $|A| = d-1$ gives $\eta_A = 2^{1-d} I$ and

$$2^{-E_0(\psi)} \le 2^{1-d} \mathrm{Tr}(\rho_A) = 2^{1-d}, \tag{15}$$

which proves the distance-entanglement tradeoff Eq. (5).

Furthermore, suppose U is a depth-h Clifford circuit, then $U \cdot \mathcal{C}$ is also a stabilizer code and the standard lightcone argument shows that its distance is at least $d/2^h$. Applying Eq. (5) to the stabilizer code $U \cdot \mathcal{C}$ proves Eq. (6).

Proof of Lemma 1. We shall use induction in $\ell = |A|$. The base of induction is $\ell = 0$ in which case $A = \emptyset$ and $\mathcal{S}(A) = \{I\}$ by definition. Consider the induction step. Let A be a subset of ℓ qubits such that $\mathcal{S}(A) = \{I\}$. If $\ell = d$ we are done. Otherwise $|A| = \ell < d$. The Cleaning Lemma [20] asserts that for any logical Pauli operator $\overline{P}$ and any subset of qubits A with $|A| < d$ there exists an equivalent logical Pauli operator $\overline{Q} \in \overline{P} \cdot \mathcal{S}$ such that $\overline{Q}$ acts trivially on A. Thus one can choose an anti-commuting pair of logical Pauli operators $\overline{X}$ and $\overline{Z}$ that both act trivially on A. Then there must exist a qubit $i \notin A$ such that $\overline{X}$ and $\overline{Z}$ locally anti-commute on i. Assume wlog that $\overline{X}$ and $\overline{Z}$ act on the i-th qubit as Pauli X and Z respectively (otherwise, perform a local Clifford change of basis on the i-th qubit). Consider a set $A' = A \cup \{i\}$ of size $\ell+1$. We claim that $\mathcal{S}(A') = \{I\}$. Indeed, let $S \in \mathcal{S}$ be a stabilizer supported on A'. Let $S_i \in \{I, X, Y, Z\}$ be the restriction of S onto the i-th qubit. Since S commutes with all logical operators and S overlaps with $\overline{X}$ and $\overline{Z}$ *only* on the i-th qubit, one infers that S_i commutes with both Pauli X and Z. This is only possible if $S_i = I$. Thus $S \in \mathcal{S}(A) = \{I\}$, that is, $S = I$ and $\mathcal{S}(A') = \{I\}$. This completes the induction step. □

B. Quantum LDPC codes

Let us prove Theorem 1. It suffices to consider an arbitrary logical state $|\psi\rangle \in \mathcal{C}$ and prove that

$$-\log_2 |\langle\psi|0^n\rangle|^2 \ge d \cdot g(s) \tag{16}$$

for some function $g(s) > 0$. Indeed, since a local change of basis on each qubit does not affect the distance and sparsity of $\mathcal{C}$, we can assume wlog that $E_0(\psi)$ is achieved by $-\log_2 |\langle\psi|0^n\rangle|^2$. Moreover, suppose U is a depth-h circuit, then $U \cdot \mathcal{C}$ is a qLDPC code defined by commuting projectors $U\Pi_a U^\dagger$. The standard lightcone argument shows that $U \cdot \mathcal{C}$ has sparsity at most $s2^h$ and distance at least $d/2^h$. Hence, $E_0(\psi) \geq d \cdot g(s)$ implies $E_h(\psi) \geq d \cdot g(s2^h)/2^h$.

The key is to consider the probability distribution of bit strings corresponding to measuring $|\psi\rangle$ in the computational basis:

$$\Pr_\psi(x) = |\langle x|\psi\rangle|^2, \quad x \in \{0,1\}^n. \tag{17}$$

The following lemma characterizes such probability distribution.

Lemma 2. *Suppose $d > s^4$. Then*

(i) Each bit of x is independent of all but at most K other bits.

(ii) $\mathbb{E}_\psi(|x|) \leq -(K+1)\log|\langle\psi|0^n\rangle|^2$.

(iii) There exists a function $c(s)$ such that $\Pr_\psi[|x| \geq t] \leq \exp[\mathbb{E}_\psi(|x|) - t]$ for any $t \geq c(s)\mathbb{E}_\psi(|x|)$.

Here $K = s^2 + s^4$; $|x| = \sum_{i=1}^n x_i$ is the Hamming weight of x; log stands for the natural logarithm. In the following, we omit the subscripts in $\Pr_\psi$ and $\mathbb{E}_\psi$.

Now let us show how Eq. (16) follows from Lemma 2. We denote $R = -(K+1)\log|\langle\psi|0^n\rangle|^2$. If $d < c(s)R$, or equivalently

$$-\log|\langle\psi|0^n\rangle|^2 > \frac{d}{(K+1)c(s)}, \tag{18}$$

then we already have the desired form Eq. (16).

Consider the case $d \geq c(s)R$. For each integer $i \in [1,n]$ we define a quantity

$$S_i = \sum_{1\leq p_1<\cdots<p_i\leq n} \Pr[x_{p_1} = \cdots = x_{p_i} = 1]. \tag{19}$$

Then we have (recall Bonferroni's inequality):

$$\begin{aligned}
&(-1)^{d-1}\left[\Pr[|x|>0] - \sum_{i=1}^{d-1}(-1)^{i-1}S_i\right] \\
&= \sum_{t=d}^{n}\binom{t-1}{d-1}\Pr[|x|=t] = \sum_{t=d}^{n}\binom{t-2}{d-2}\Pr[|x|\geq t] \\
&\leq \sum_{t=d}^{\infty}\binom{t-2}{d-2}e^{R-t} = e^{-1+R}(e-1)^{1-d}.
\end{aligned} \tag{20}$$

Here the inequality uses Lemma 2 (ii) and (iii). The condition $t \geq c(s)\mathbb{E}(|x|)$ in (iii) is satisfied since $d \geq c(s)R$. The last equality in Eq. (20) follows from binomial expansion (with a negative exponent); $e \equiv \exp(1)$. Note that $S_1, \ldots, S_{d-1}$ depend only on reduced density matrices of $|\psi\rangle$ describing subsets of less than d qubits. The local indistinguishability property implies that $S_1, \ldots, S_{d-1}$ are the same for any logical state $|\psi\rangle$.

Eq. (20) shows the overlap $|\langle\psi|0^n\rangle|^2 = 1 - \Pr[|x|>0]$ is approximately the same for any logical state, up to the correction $e^{-1+R}(e-1)^{1-d}$. However, since $\dim\mathcal{C} \geq 2$, there always exists a logical state $|\psi'\rangle \in \mathcal{C}$ such that $\langle\psi'|0^n\rangle = 0$. Therefore, for any logical state $|\psi\rangle \in \mathcal{C}$ one must have

$$|\langle\psi|0^n\rangle|^2 \leq e^{-1+R}(e-1)^{1-d}. \tag{21}$$

It is equivalent to

$$-\log|\langle\psi|0^n\rangle|^2 \geq \frac{1+(d-1)\log(e-1)}{K+2}, \tag{22}$$

which is in the desired form Eq. (16). More precisely, since either Eq. (18) or Eq. (22) must hold, we have proved Eq. (16) with $g(s) = \frac{1}{\log(2)}\min\left[\frac{1}{(K+1)c(s)}, \frac{\log(e-1)}{K+2}\right]$.

Proof of Lemma 2. *(i)* We claim that any logical state $|\psi\rangle \in \mathcal{C}$ has zero correlation length. More precisely, consider any subset of qubits $M \subseteq [n]$ and let $M^c = [n]\setminus M$ be the complement of M. Let ∂M be the boundary of M defined as the set of qubits covered by supports of projectors Π_a that overlap with both M and M^c. The Disentangling Lemma of Ref. [17] implies that if $|M| < d$ and $|M^c \cap \partial M| < d$ then

$$\mathrm{Tr}_{\partial M}|\psi\rangle\langle\psi| = \rho_{M\setminus\partial M} \otimes \rho_{M^c\setminus\partial M}, \tag{23}$$

where ρ_A is the reduced density matrix of $|\psi\rangle\langle\psi|$ describing a subset of qubits A. Consider any qubit j. We choose M as the union of j and all neighbors of j in the "interaction graph" determined by the projectors Π_a. Then $j \in M\setminus\partial M$ and Eq. (23) implies that measuring $|\psi\rangle$ in the standard basis, the j-th measured bit is independent of all bits in $M^c\setminus\partial M$. The number of remaining bits that can possibly be correlated with the j-th bit is at most $|M\cup\partial M| - 1$. A simple calculation shows that $|M\cup\partial M| \leq s^2 + s^4$ while conditions of the Disentangling Lemma are satisfied whenever $d > s^4$.

(ii) The proof is based on [18]. Define a dependency graph $G = (V,E)$ with n vertices such that the i-th bit of x can be correlated only with the nearest neighbors of i in G. We have already shown that the vertex degree of G is at most K. If $V_I \subset V$ is an independent set of vertices then all bits x_j with $j \in V_I$ are independent. Let $m_j = \mathbb{E}(x_j)$. Then

$$\begin{aligned}
|\langle\psi|0^n\rangle|^2 &\leq \Pr[x_j = 0 \quad \forall j \in V_I] \\
&= \prod_{j\in V_I}\Pr[x_j=0] = \prod_{j\in V_I}(1-m_j) \\
&\leq \exp(-\sum_{j\in V_I} m_j).
\end{aligned} \tag{24}$$

Using a simple greedy algorithm one can show that any graph with the maximum vertex degree K and vertex weights $m_j \in [0,1]$ has an independent set V_I such that

$$\sum_{j\in V_I} m_j \geq \frac{1}{K+1}\sum_{j=1}^{n} m_j = \frac{\mathbb{E}(|x|)}{K+1}. \tag{25}$$

Combining Eqs. (24,25) gives the desired lower bound on $\mathbb{E}(|x|)$.

(iii) Theorem 2.3 of [31] gives the following Chernoff-type bound for a sum of partly dependent random variables x_i and all $t \geq 0$:

$$\Pr[|x| \geq \mathbb{E}(|x|) + t] \leq \exp\left[-\frac{S}{K+1}\phi\left(\frac{4t}{5S}\right)\right]. \tag{26}$$

Here $\phi(x) = (1+x)\log(1+x) - x$, and $S = \sum_i \mathrm{Var}(x_i) \leq \mathbb{E}(|x|)$. Since the function $\phi(x)$ is superlinear in x, there exists $x_0 = x_0(s)$ such that $\phi(x) > \frac{5}{4}(K+1)x$ when $x > x_0$. Hence, if $t > \frac{5}{4}x_0\mathbb{E}(|x|)$, then

$$\Pr[|x| \geq \mathbb{E}(|x|) + t] \leq \exp(-t). \tag{27}$$

Now we replace t with $t - \mathbb{E}(|x|)$ and set $c(s) = \frac{5}{4}x_0(s) + 1$. A simple algebra gives $x_0(s) = \exp[1 + (5/4)(K+1)]$. Accordingly, the function $g(s)$ defined in Eq. (16) can be chosen as $g(s) = 1/(\log(2)(K+1)c(s))$ with $K = s^2 + s^4$. □

C. Constant rate codes

Now let us prove Theorem 3. Let us again consider $|\langle 0^n|\psi\rangle|^2$ without loss of generality.

To prove item (i), we will inductively measure $(d-1)$ qubits, one at a time. The following lemma guarantees the existence of a qubit that is "mixed enough":

Lemma 3. *For any code state, there exists a qubit q that the von Neumann entropy satisfies $S_q \geq k/n$.*

Assuming it is the first qubit wlog, lemma 3 guarantees that we can expand $|\psi\rangle$ as:

$$|\psi\rangle = \lambda_0 |0\rangle |\psi_0\rangle + \lambda_1 |1\rangle |\psi_1\rangle, \tag{28}$$

such that $\lambda_0, \lambda_1 \neq 0$. Moreover, it also follows that $H(|\lambda_0|^2) \geq S_1 \geq k/n$, hence $|\lambda_0|^2 \leq 1 - H^{-1}(k/n)$.

The state $|\psi_0\rangle$ is a post-measurement state after measuring the first qubit in the computational basis. As a general principle, it must be a logical state of a (different) code:

Lemma 4. *Measuring one qubit in a distance d code, the post-measurement state (regardless of the measurement outcome) is a logical state of a code with $k' = k$ and $d' \geq d-1$.*

Both lemma 3 and 4 are direct consequences of the local indistinguishability of quantum codes, and are proved in Appendix B and C. With them in mind, let us repeat the procedure at least $(d-1)$ times until the code distance might decrease to 1. Each time we can upper bound the corresponding amplitude using lemma 3. The overlap is then bounded by the product:

$$|\langle 0^n|\psi\rangle|^2 \leq \prod_{i=0}^{d-2}\left[1 - H^{-1}\Big(\frac{k}{n-i}\Big)\right]. \tag{29}$$

Eq.(7) then follows from $-\log(1-x) > x$ and that a depth-h circuit at most decreases the code distance by a factor 2^h.

For item (ii), we use Lemma 2. Due to the linearly of the expectation value and the local indistinguishability of quantum codes, $\mathbb{E}_\psi(|x|)$ is the same for $\forall\,|\psi\rangle \in \mathcal{C}$. In particular, if choosing a so that $H(\frac{a}{n}) = \frac{k}{n}$, then $\dim\mathcal{C}$ is large enough so that there always exists $|\psi\rangle \in \mathcal{C}$ such that $\langle\psi|x\rangle = 0$ for all x whose Hamming weight $|x| \leq a$:

$$\sum_{i=0}^{a}\binom{n}{i} < 2^{nH(\frac{a}{n})} \leq 2^k. \tag{30}$$

For such $|\psi\rangle$, it is clear that $\mathbb{E}_\psi(|x|) > a$. If follows from Lemma 2(ii) that

$$-\log|\langle\psi|0^n\rangle|^2 > \frac{a}{K+1} = \frac{n}{K+1}H^{-1}\Big(\frac{k}{n}\Big). \tag{31}$$

D. Permutation Invariant codes

Consider a code $\mathcal{C}$ with $k=1$ logical qubit and $n \geq 4$ physical qubits such that the logical states encoding $|0\rangle$ and $|1\rangle$ are

$$|\psi_0\rangle = \sqrt{1-\frac{2}{n}}|0^n\rangle + \sqrt{\frac{2}{n}}|1^n\rangle \tag{32}$$

and

$$|\psi_1\rangle = \sqrt{\frac{2}{n(n-1)}}\sum_{x\in\{0,1\}^n\,:\,|x|=2}|x\rangle \tag{33}$$

respectively. In other words, $\mathcal{C}$ is the two-dimensional subspace spanned by $|\psi_0\rangle$ and $|\psi_1\rangle$. The code $\mathcal{C}$ is an example of a permutation invariant code [22, 23] since the logical states $|\psi_i\rangle$ are invariant under any permutation of n qubits. A simple calculation reveals that $\mathcal{C}$ has distance $d=2$, see Appendix D. By definition of GEM,

$$2^{-E_0(\psi_0)} \geq |\langle\psi_0|0^n\rangle|^2 = 1 - \frac{2}{n}. \tag{34}$$

Hence $E_0(\psi_0) \leq -\log_2(1-(2/n)) \leq 4/n$. By concatenating the code $\mathcal{C}$ with itself several times we obtain a family of distance-d codes with an arbitrarily large d and k such that their logical states have GEM approaching zero in the limit $n \to \infty$, see Appendix D for details.

III. CONCLUSIONS

We have established distance-entanglement tradeoffs for three broad families of quantum codes: LDPC codes with commuting check operators, stabilizer codes, and constant rate codes. Logical states of such codes are shown to be highly entangled such that the geometric entanglement measure grows at least linearly with the code distance. This highlights the role of entanglement as a resource enabling quantum error correction based on the above code families. At the same time, we show that there exist families of high-distance codes such that some logical states may have very little entanglement.

ACKNOWLEDGMENTS

SB thanks Chinmay Nirkhe for helpful discussions. Research at Perimeter Institute is supported in part by the Government of Canada through the Department of Innovation, Science and Economic Development and by the Province of Ontario through the Ministry of Colleges and Universities.

---

[1] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995.
[2] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, 1997.
[3] Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824, 1996.
[4] Xiao-Gang Wen and Qian Niu. Ground-state degeneracy of the fractional quantum Hall states in the presence of a random potential and on high-genus Riemann surfaces. *Physical Review B*, 41(13):9377, 1990.
[5] A Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of physics*, 303(1):2–30, 2003.
[6] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002.
[7] Fernando Pastawski, Beni Yoshida, Daniel Harlow, and John Preskill. Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence. *Journal of High Energy Physics*, 2015(6):1–55, 2015.
[8] Ahmed Almheiri, Xi Dong, and Daniel Harlow. Bulk locality and quantum error correction in ads/cft. *Journal of High Energy Physics*, 2015(4):1–34, 2015.
[9] Michael H Freedman and Matthew B Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *arXiv preprint arXiv:1301.1363*, 2013.
[10] Anurag Anshu, Nikolas P Breuckmann, and Chinmay Nirkhe. NLTS hamiltonians from good quantum codes. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1090–1096, 2023.
[11] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 375–388, 2022.
[12] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
[13] Indeed, if $d \geq 2$ then all logical states must have the same single-qubit marginals. However, any state sharing the same single-qubit marginals with an unentangled (product) state must be equal to the unentangled state itself. Hence, a code with $k \geq 1$ and $d \geq 2$ cannot have an unentangled logical state.
[14] Tzu-Chieh Wei and Paul M Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Physical Review A*, 68(4):042307, 2003.
[15] Román Orús, Tzu-Chieh Wei, Oliver Buerschaper, and Maarten Van den Nest. Geometric entanglement in topologically ordered states. *New Journal of Physics*, 16(1):013015, 2014.
[16] Sergey Bravyi, Matthew B Hastings, and Spyridon Michalakis. Topological quantum order: stability under local perturbations. *Journal of mathematical physics*, 51(9), 2010.
[17] Sergey Bravyi, David Poulin, and Barbara Terhal. Tradeoffs for reliable quantum information storage in 2d systems. *Physical review letters*, 104(5):050503, 2010.
[18] Sergey Bravyi, David Gosset, and Yinchen Liu. Classical simulation of peaked shallow quantum circuits. *arXiv preprint arXiv:2309.08405*, 2023.
[19] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Physical Review A*, 57(1):127, 1998.
[20] Sergey Bravyi and Barbara Terhal. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New Journal of Physics*, 11(4):043029, 2009.
[21] Anurag Anshu and Chinmay Nirkhe. Circuit lower bounds for low-energy states of quantum code hamiltonians. *arXiv preprint arXiv:2011.02044*, 2020.
[22] Harriet Pollatsek and Mary Beth Ruskai. Permutationally invariant codes for quantum error correction. *Linear algebra and its applications*, 392:255–288, 2004.
[23] Yingkai Ouyang. Permutation-invariant quantum codes. *Physical Review A*, 90(6):062317, 2014.
[24] Dorit Aharonov and Yonathan Touati. Quantum circuit depth lower bounds for homological codes. *arXiv preprint arXiv:1810.03912*, 2018.
[25] Lior Eldar and Aram W Harrow. Local hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th annual symposium on foundations of computer science (FOCS)*, pages 427–438. IEEE, 2017.
[26] Alonso Botero and Benni Reznik. Scaling and universality of multipartite entanglement at criticality. *arXiv preprint arXiv:0708.3391*, 2007.
[27] Román Orús. Universal geometric entanglement close to quantum phase transitions. *Physical review letters*,

100(13):130502, 2008.

[28] Román Orús. Geometric entanglement in a one-dimensional valence-bond solid state. *Physical Review A*, 78(6):062332, 2008.

[29] Tzu-Chieh Wei. Entanglement under the renormalization-group transformations on quantum states and in quantum phase transitions. *Physical Review A*, 81(6):062313, 2010.

[30] Sergey Bravyi, Dongjin Lee, Zhi Li, and Beni Yoshida. How much entanglement is needed for emergent anyons and fermions? *to appear*, 2024.

[31] Svante Janson. Large deviations for sums of partly dependent random variables. *Random Structures & Algorithms*, 24(3):234–248, 2004.

[32] Ramis Movassagh and Yingkai Ouyang. Constructing quantum codes from any classical code and their embedding in ground space of local hamiltonians. *arXiv preprint arXiv:2012.01453*, 2020.

Appendix A: Shor's code

Distance-d Shor's code [1] is a stabilizer code defined on a two-dimensional grid of qubits of size $d \times d$. It encodes one logical qubit into $n = d^2$ physical qubits. The code has Pauli stabilizers $Z_{i,j}Z_{i+1,j}$ acting on pairs of adjacent qubits located in the same column and $\prod_{i=1}^{d} X_{i,j}X_{i,j+1}$ acting on pairs of adjacent columns. Logical Pauli operators can be chosen as $X_L = \prod_{i=1}^{d} X_{i,1}$ along a column and $Z_L = \prod_{j=1}^{d} Z_{1,j}$ along a row.

It is well known and can be easily checked that the code space is spanned by

$$\begin{aligned} |\psi_0\rangle &= \Big(\frac{|0^d\rangle + |1^d\rangle}{\sqrt{2}}\Big)^{\otimes d}, \\ |\psi_1\rangle &= \Big(\frac{|0^d\rangle - |1^d\rangle}{\sqrt{2}}\Big)^{\otimes d}, \end{aligned} \tag{A1}$$

where each $(|0^d\rangle \pm |1^d\rangle)/\sqrt{2}$ is a GHZ state associated with a column of the grid. Then $|\psi_+\rangle = (|\psi_0\rangle + |\psi_1\rangle)/\sqrt{2}$ is a normalized logical state and $E_0(\psi_+) \le -\log_2 |\langle\psi_+|0^n\rangle|^2 = d-1$ which matches the lower bound of Theorem 2.

Appendix B: Proof of Lemma 3

Here we prove lemma 3 in the main text, copied below for convenience:

Lemma 3. *For any code state $|\psi\rangle$ in a quantum code $\mathcal{C}$ (code distance $d \ge 2$), there exists at least one qubit q that the reducing $|\psi\rangle\langle\psi|$ on that qubit, the von-Neumann entropy satisfies $S_q \ge k/n$. Here $k = \log_2(\dim \mathcal{C})$.*

Proof. We denote the von Neumann entropy of the reduced state of $|\psi\rangle\langle\psi|$ on qubit i as S_i. Consider the maximally mixed state in the code space $\mathcal{C}$, denoted by ρ. By definition, $S(\rho) = k$.

Due to the local indistinguishability, S_i can be equally computed by reducing ρ to qubit i. The subadditivity of entropy then implies

$$k = S(\rho) \le \sum_{i=1}^{n} S_i. \tag{B1}$$

Hence there exists at least one qubit q such that $S_q \ge k/n$. ∎

Appendix C: Measuring a Quantum Code

In the proof of Theorem 3, we considered an inductive procedure to measure $d-1$ qubits. It is based on the following:

Lemma 4′. *Given a code with distance d, postselecting $m < d$ qubits either (1) annihilates all states, or (2) results in a code with the same dimension and code distance $d' \ge d - m$.*

Proof. Denote $\{|\psi_i\rangle\}$ as a orthonormal basis of the code space $\mathcal{C}$; denote P as the postselection operator. By the Knill-Laflamme (KL) condition, we have

$$\langle\psi_i| P^\dagger P |\psi_j\rangle = c(P^\dagger P)\delta_{ij}. \tag{C1}$$

If P does not annihilate $\mathcal{C}$, then $c(P^\dagger P) > 0$. The space after projection, $\mathcal{C}'$, is spanned by $\{P|\psi_i\rangle\}$, for which an orthonormal basis is $\{P|\psi_i\rangle/\sqrt{c(P^\dagger P)}\}$, hence $\dim \mathcal{C}' = \dim \mathcal{C}$.

For any operator $\mathcal{O}$ applied on non-postselected $(d-m-1)$ qubits, $P^\dagger \mathcal{O} P$ applies on at most $(d-1)$ qubits. Therefore, by KL condition (applied to $|\psi_i\rangle$),

$$\langle\psi_i| P^\dagger \mathcal{O} P |\psi_j\rangle = c(P^\dagger \mathcal{O} P)\delta_{ij} \stackrel{\text{def}}{=} c'(\mathcal{O})\delta_{ij}. \tag{C2}$$

Hence, again due to KL condition (applied to $P|\psi_i\rangle$), $\mathcal{C}'$ is a code with code distance at least $d - m$. ∎

As a simple corollary, we prove a lower bound regarding the number of terms in the wavefunction of any logical state.

Theorem 4. *Expanding any logical state of a distance-d code in any computational basis, the number of terms must be at least 2^{d-1}.*

Proof. We prove the theorem by induction on d. First, $d = 2$ case. $\forall |\psi\rangle, |\phi\rangle \in \mathcal{C}$, for each qubit i, we have $(|\psi\rangle\langle\psi|)_i = (|\phi\rangle\langle\phi|)_i$. If $|\psi\rangle$ is a product state, we must have $|\phi\rangle = |\psi\rangle$. Therefore, in a code $(k \ge 1)$, no logical state can be a product state, implying the number of terms must be at least 2.

Assuming we have proved the $(d-1)$ case, let us consider distance-d codes. For any logical state $|\psi\rangle$, using $d = 2$ case, we know there exists a qubit, say the first qubit, that is not pure if we trace out its complement. We can then expand $|\psi\rangle$ as

$$|\psi\rangle = \lambda_0 |0\rangle |\psi_0\rangle + \lambda_1 |1\rangle |\psi_1\rangle, \tag{C3}$$

where $\lambda_i \neq 0$. Postselecting on $|0\rangle$, we know from lemma 4 that $|\psi_0\rangle$ is a logical state in a code of distance $d' \geq d-1$, hence must have at least 2^{d-2} terms by induction. The same applies to $|\psi_1\rangle$. Therefore, the number of terms in $|\psi\rangle$ must be at least $2^{d-2} + 2^{d-2} = 2^{d-1}$. □

This bound is also tight, as it can be saturated by the Shor's code as shown in Appendix A.

Appendix D: Concatenation of PI codes

Let us check that the permutation invariant code $\mathcal{C}$ defined by Eqs. (32,33) has distance $d = 2$. Suppose $\sigma \in \{X_i, Y_i, Z_i\}$ is a single-qubit error. The assumption $n \geq 4$ implies $\langle\psi_0|\sigma|\psi_1\rangle = 0$. Thus it suffices to check that

$$\langle\psi_0|\sigma|\psi_0\rangle = \langle\psi_1|\sigma|\psi_1\rangle. \tag{D1}$$

If $\sigma \in \{X_i, Y_i\}$ then both sides of Eq. (D1) are zero. Suppose $\sigma = Z_i$. We have

$$\langle\psi_0|Z_i|\psi_0\rangle = (1 - \frac{2}{n}) - \frac{2}{n} = 1 - \frac{4}{n} \tag{D2}$$

and

$$\begin{aligned}\langle\psi_1|Z_i|\psi_1\rangle &= \frac{2}{n(n-1)}\left(\binom{n-1}{2} - \binom{n-1}{1}\right) \\ &= 1 - \frac{4}{n}.\end{aligned} \tag{D3}$$

Here the terms $\binom{n-1}{2}$ and $\binom{n-1}{1}$ count n-bit strings x with $|x| = 2$ such that $x_i = 0$ and $x_i = 1$ respectively. This proves Eq. (D1). As a side remark, we note that the code $\mathcal{C}$ is a special case of a general construction that maps classical (non-linear) codes to quantum codes proposed in [32]. In particular, the quantum code $\mathcal{C}$ is constructed from a classical distance-2 length-n code whose codewords are n-bit strings x with $|x| \in \{0, 2, n\}$ by applying the framework of [32].

Next, let us show how to improve the distance of $\mathcal{C}$ by concatenation. We will show that the concatenated code has logical states with the geometric entanglement approaching zero in the limit of large n. Let $\mathcal{C}_n$ be the distance-2 code with one logical qubit and n physical qubits defined by Eqs. (32,33). For any integer sequence $n_1, n_2, \ldots, n_\ell$ let $\mathcal{C}$ be the concatenation of codes $\mathcal{C}_{n_1}, \ldots, \mathcal{C}_{n_\ell}$, where $\mathcal{C}_{n_1}$ is at the lowest and $\mathcal{C}_{n_\ell}$ is at the highest level of concatenation. In other words, each consecutive block of n_1 physical qubits defines a level-1 logical qubit encoded by $\mathcal{C}_{n_1}$, each consecutive block of n_2 level-1 logical qubits defines a level-2 logical qubit encoded by $\mathcal{C}_{n_2}$, etc. The code $\mathcal{C}$ has one logical qubit, $N_\ell = \prod_{i=1}^{\ell} n_i$ physical qubits, and distance $d_\ell = 2^\ell$, assuming that $n_i \geq 4$ for all i. Let F_ℓ be the overlap between the logical-0 state of the level-ℓ logical qubit and the product state $|0^{N_\ell}\rangle$. From Eq. (32) one easily gets

$$F_i = \left(1 - \frac{2}{n_i}\right)(F_{i-1})^{n_i} \tag{D4}$$

with $i = 1, \ldots, \ell$ and $F_0 \equiv 1$. Thus

$$F_\ell = \prod_{i=1}^{\ell}\left(1 - \frac{2}{n_i}\right)^{n_{i+1}n_{i+2}\cdots n_\ell}, \tag{D5}$$

(for $i = \ell$, $n_{i+1}n_{i+2}\cdots n_\ell = 1$).

Let $d \geq 2$ be the desired code distance and $\ell = \lceil \log_2(d) \rceil$. Let us choose $\{n_i\}$ properly to ensure that the geometric entanglement approaches zero. Let $M \geq 1$ be a large integer. Set $n_\ell = 2M$ and

$$n_i = 2Mn_{i+1}n_{i+2}\cdots n_\ell \tag{D6}$$

for all $i \in [1, \ell - 1]$ so that

$$F_\ell = \prod_{i=1}^{\ell}\left(1 - \frac{1}{Mn_{i+1}n_{i+2}\cdots n_\ell}\right)^{n_{i+1}n_{i+2}\cdots n_\ell}. \tag{D7}$$

One can easily check that $(1 - 1/(Mx))^x$ is a monotone increasing function of x for $x \geq 1$. Thus

$$F_\ell \geq \left(1 - \frac{1}{M}\right)^\ell. \tag{D8}$$

Denoting $|\psi_0^\ell\rangle$ the logical-0 state of the level-ℓ logical qubit, we conclude that

$$E_0(\psi_0^\ell) \leq -\log_2(F_\ell) = O(\ell/M) = O(2^d/M). \tag{D9}$$

Thus, for any constant $d \geq 2$ there exists a family of codes (by increasing M) such that $E_0(\psi_0^\ell) \to 0$.

Solving Eq. (D6) gives $n_i = (2M)^{2^{\ell-i}}$, thus the number of physical qubits in resulting distance-d code $\mathcal{C}$ equals

$$N_\ell = \prod_{i=1}^{\ell} n_i = (2M)^{2^\ell - 1} < (2M)^{2d}. \tag{D10}$$

To construct a code with k logical qubits, we simply take k independent copies of the concatenated code. Equivalently, we concatenate it further with the trivial $[[k, k, 1]]$ code. An example of a logical state is $|\psi\rangle = |\psi_0^\ell\rangle^{\otimes k}$. The geometric entanglement $E_0(\psi) \leq O(k2^d/M)$, which can also be made arbitrarily small by choosing large enough M.

Finally, let us point out that some distance-d PI codes exhibit GEM scaling at most logarithmically with d (without concatenation). Indeed, let $d \geq 3$ be an odd integer and $n = d^2$. Following Ref. [23], consider a PI code encoding $k = 1$ logical qubit into n physical qubits such that the codespace has an orthonormal basis

$$|\psi_\pm\rangle = \frac{1}{\sqrt{2^d}}\sum_{\ell=0}^{d}(\pm 1)^\ell \sqrt{\binom{d}{\ell}}|D_{d\ell}^n\rangle, \tag{D11}$$

where $|D_m^n\rangle$ is the n-qubit Dicke state with m particles,

$$|D_m^n\rangle = \frac{1}{\sqrt{\binom{n}{m}}}\sum_{\substack{x \in \{0,1\}^n \\ |x| = m}} |x\rangle. \tag{D12}$$

Theorem 4 of [23] proves that $\mathcal{C} = \mathrm{span}(\psi_+, \psi_-)$ is a distance-d code. Simple algebra gives

$$\langle +^{\otimes n} | \psi_+ \rangle = \frac{1}{\sqrt{2^{d+n}}} \sum_{\ell=0}^{d} \sqrt{\binom{d}{\ell}\binom{n}{d\ell}}. \tag{D13}$$

The sum over ℓ is lower bounded by a single term with $\ell = (d-1)/2$. It is well known that

$$\binom{n}{m} \geq 2^{nH(m/n)} \sqrt{\frac{n}{8m(n-m)}}. \tag{D14}$$

for all $n \geq 2$ and $m \in [1, n-1]$. Noting that $H(1/2-x) \geq 1 - O(x^2)$ one gets

$$\binom{d}{(d-1)/2} \geq \Omega\Big(\frac{2^d}{\sqrt{d}}\Big) \tag{D15}$$

and

$$\binom{n}{d(d-1)/2} \geq \Omega\Big(\frac{2^n}{d}\Big). \tag{D16}$$

It follows that $\langle +^{\otimes n}|\psi_+\rangle \geq \Omega(d^{-3/4})$ and thus $E_0(\psi_+) \leq -\log_2 |\langle +^{\otimes n}|\psi_+\rangle|^2 = O(\log d)$.