2014 IEEE Annual Symposium on Foundations of Computer Science

Local tests of global entanglement and a counterexample to the generalized area law

Dorit Aharonov
The Hebrew University
Jerusalem, Israel
doria@cs.huji.ac.il

Aram W. Harrow
MIT
Cambridge, MA USA
aram@mit.edu

Zeph Landau
UC Berkeley
Berkeley, CA, USA
zeph.landau@gmail.com

Daniel Nagaj
Slovak Academy of Sciences
Bratislava, Slovakia
dnagaj@gmail.com

Mario Szegedy
Rutgers University
New Brunswick, NJ, USA
szegedy@dragon.rutgers.edu

Umesh Vazirani
UC Berkeley
Berkeley, CA, USA
vazirani@eecs.berkeley.edu

***Abstract*—We introduce a technique for applying quantum expanders in a distributed fashion, and use it to solve two basic questions: testing whether a bipartite quantum state shared by two parties is the maximally entangled state and disproving a generalized area law. In the process these two questions which appear completely unrelated turn out to be two sides of the same coin. Strikingly in both cases a constant amount of resources are used to verify a global property.**

I. Introduction

In this paper we address two basic questions:

1) Can Alice and Bob test whether their joint state is maximally entangled while exchanging only a constant number of qubits? More precisely, Alice and Bob hold two halves of a quantum state $|\psi\rangle$ on a D^2-dimensional space for large D, and would like to check whether $|\psi\rangle$ is the maximally entangled state $|\phi_D\rangle = \frac{1}{\sqrt{D}} \sum_x |x\rangle|x\rangle$ or whether it is orthogonal to that state. So far, all known protocols for this task require resources (clasical or quantum communication, as well as shared randomness) which grow with D ([5], and see below).
2) Is there a counterexample to the generalized area law? A sweeping conjecture in condensed matter physics, and one of the most important open questions in quantum Hamiltonian complexity theory, is the so called Area Law, which asserts that ground states of quantum many body systems on a lattice have limited entanglement. Specifically, assume the system is described by a gapped local Hamiltonian $H = H_1 + \ldots + H_m$, where each H_i describes a local interaction between two neighboring particles of a lattice. The area law conjectures that for every subset S of the particles, the entanglement entropy between S and $\bar{S}$ for the ground state of H is bounded by a constant times the size of the boundary of S. The area law, which has been proven for 1D lattices [15] and is conjectured for higher degree lattices, is of central importance in condensed matter physics as it provides the basic reason to hope that ground states of such systems might have a succinct classical description. The *generalized* area law (a folklore conjecture) transitions from this physically motivated phenomenon to a very clean and general graph theoretic formulation, where in place of edges of the lattice, the terms of the Hamiltonian correspond to edges of an arbitrary graph. The generalized area law then states that for any subset S of vertices (particles), the entanglement entropy between S and $\bar{S}$ for the ground state is bounded by some constant times the cut-set of S (the number of edges leaving S).

We affirmatively answer both questions, based on a common technique that may be thought of as applying quantum expanders in a distributed fashion. Indeed these two questions which at first sight seem completely unrelated turn out to be two sides of the same coin.

For the entanglement testing problem, we show that Alice and Bob can solve it by communicating only a constant number of qubits: for any D and any $\epsilon > 0$, there is a protocol that uses $O(\log 1/\epsilon)$ qubits of communication from Alice to Bob, after which Bob always accepts if the shared state is $|\phi_D\rangle$. If the shared state is orthogonal to $|\phi_D\rangle$, he accepts with probability at most ϵ. If Alice and Bob do start with the maximally entangled state $|\phi_D\rangle$, the protocol does not damage the state.

For a counterexample to the generalized area law, we exhibit a gapped local Hamiltonian acting on the graph featured in Figure I a, for which the entanglement entropy of the ground state across the middle cut is $\Omega(n^c)$ for some $0 < c < 1$ (rather than $O(1)$ as predicted by the generalized area law). The core step in generating this example is the construction of a

0272-5428/14 $31.00 © 2014 IEEE
DOI 10.1109/FOCS.2014.34

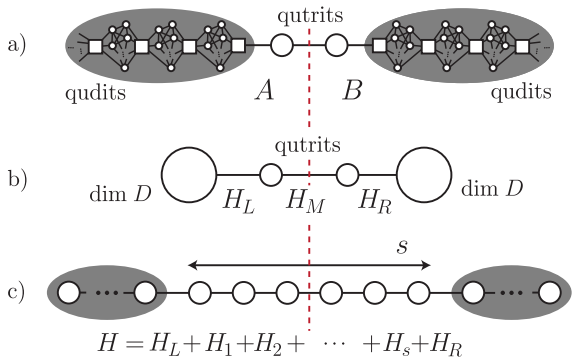

Figure 1. a) A counterexample to the generalized area law, consisting of a chain of complete graphs separated by the middle edge. The entropy across the cut grows as $\Omega(n^c)$, where n is the total number of particles. b) A four-particle construction. c) Short chain framework for proving 1D area law.

simpler system consisting of four particles on a line (see Figure 1b): two particles of dimension $d = 3$ (qutrits) in the middle, and two particles of dimension D at the two ends, with D is arbitrarily large. The gapped Hamiltonian is of the form $H = H_L + H_M + H_R$, where H_L acts between the left particle and the left qutrit, H_M between the two qutrits, and H_R between the right qutrit and the right particle. Crucially, the entanglement entropy of the ground state across the middle cut is $\Omega(\log D)$. This enforcing of a large amount of entanglement by a single such constraint is a surprising quantum phenomenon — in the analogous probabilistic situation, in which we consider the uniform distribution over the set of all possible solutions to constraints set on the graph, the middle constraint can only enforce a convex combination of a constant number of product distributions.

This simple example of a four body Hamiltonian is already important within the context of proofs of the 1D area law and prospects for extending those techniques to higher dimensions. The best bounds for the 1D area law [3] show that an area law must hold in a model similar to our four body Hamiltonian, when the middle link is extended into a finite chain of $s = \Omega(\log^2 d/\epsilon)$ particles, each of -dimension d (see figure 1c). This yields an area law bound of $S_{1D} = O(\log^3 d/\epsilon)$ across the middle cut. Moreover, any slight improvement in the exponent of $\log d$ in this bound would imply a non-trivial sub-volume law for 2D systems. The crucial parameter in improving the result is the length of the middle chain. Our four particle example establishes that an area law does not hold when the chain is length 1. Understanding the intermediate regime is an important open question.

Our approach to both questions is to apply quantum expanders distributively. We rely on the existence of a quantum expander which consists of a set of d unitaries U_i with the property that the map $\mathcal{E}(X) = \frac{1}{d}\sum_{i=1}^{d} U_i X U_i^\dagger$ has the unique eigenvalue 1 for the eigenvector $X = \mathbb{I}$ and next highest singular value $\lambda < 1$. In the entanglement testing problem, the expander is applied distributively by communicating which of the d unitaries is being applied. In the generalized area law problem, synchronizing the application of the expander on the left and right sides requires only a single term of the Hamiltonian, acting on two d-dimensional particles. This yields the core four-particle example above, which is then converted to an interaction graph on bounded dimensional particles by applying Kitaev's circuit to Hamiltonian construction to implement the U_i. In Section VI (and discussion in Section VII) we explore whether there is a deeper connection between very efficient communication protocols for entanglement testing and violations of generalized area laws.

Notation: For a matrix X, let X^* be the entry-wise complex conjugate of X and $X^\dagger$ the transpose of X^*. Define the Frobenius norm $|X| := \sqrt{\mathrm{tr}\, X^\dagger X}$; the operator norm $\|X\|$ is the largest singular value of X.

II. Quantum Expanders

The key structural component to our results are quantum expanders. We will only make use here of expanders based on applying one out of d unitaries at random (a more general definition using Kraus operators exists).

Definition 1. The operator $\mathcal{E} : L(\mathbb{C}^D) \to L(\mathbb{C}^D)$ (here we use $L(\mathbb{C}^D)$ to denote the set of linear operators on $\mathbb{C}^D$) is termed a (D, d, λ) *quantum expander* if

- There are d unitaries, $U_1 = \mathbb{I}, U_2, ..., U_d$, such that $\mathcal{E}(X) = \frac{1}{d}\sum_{i=1}^{d} U_i X U_i^\dagger$.
- Interpreted as a linear map, $\mathcal{E}$ has second-largest singular value $\leq \lambda$.

Just as classical expanders may be thought of as constant degree approximations to the complete graph, quantum expanders are constant-degree approximations to the application of unitaries drawn at random from the Haar measure.

By definition, the identity map $X = \mathbb{I}$ is the unique fixed point of $\mathcal{E}$. The second condition is equivalent to saying that for any X with $\mathrm{tr}(X) = 0$

$$|\mathcal{E}(X)| \leq \lambda |X|. \tag{1}$$

This interpretation suggests an alternate formulation where we think of each $X \in L(\mathbb{C}^D)$ as a vector in $\mathbb{C}^D \otimes \mathbb{C}^D$ and the operator $\mathcal{E}$ then gets mapped to the operator $\hat{\mathcal{E}} = \frac{1}{d}\sum_{i=1}^{d} U_i \otimes U_i^*$. Then $\hat{\mathcal{E}}$ fixes the

maximally entangled state $|\phi_D\rangle = \frac{1}{\sqrt{D}} \sum_{x\in[D]} |x\rangle|x\rangle$, and has second largest singular value λ.

Quantum expanders were introduced independently in [16] and [6] although many of the relevant ideas were implicit in [2]. In [17], it was proved that taking U_i for $i \in \{1,...,d\}$ to be Haar uniform results in a "Ramanujan" expander with high probability; that is, $\lambda \approx \frac{2\sqrt{d-1}}{d}$. Since random unitaries cannot be constructed efficiently, other work [7], [13], [11], [18] gave efficient constructions, in which the unitaries can be applied by a polynomial size quantum circuits. Essentially all of these constructions achieve $\log(d) = O(\log 1/\lambda)$. For our communication protocols, we will need d to be a variable (since the error depends on it); whereas for the area law counter example, we will take d to be a small constant. In what follows we will assume $d = 3$ is possible, although the smallest d that has been verified is $d = 8$ using [11].

Why are expanders relevant to our results? To understand the gap condition better, let us see why $|\phi_D\rangle$, the maximally entangled state on $\mathbb{C}^D \otimes \mathbb{C}^D$, is a $+1$ eigenvector. Observe that for any $D \times D$ matrix X, we have $(X \otimes I)|\phi_D\rangle = (I \otimes X^T)|\phi_D\rangle$. Thus $\frac{1}{d}\sum_{i=1}^{d}(U_i \otimes U_i^*)|\phi_D\rangle = \frac{1}{d}\sum_{i=1}^{d}(U_i U_i^\dagger \otimes I)|\phi_D\rangle = |\phi_D\rangle$. Since the second-largest singular value of $\hat{\mathcal{E}}$ is λ, then we have

$$\left\|\hat{\mathcal{E}} - |\phi_D\rangle\langle\phi_D|\right\| = \lambda. \tag{2}$$

Thus, $\hat{\mathcal{E}}$ gives an approximation of a projector onto $|\phi_D\rangle$ up to operator-norm error λ.

III. A communication protocol for certifying global entanglement

A. The EPR testing problem

As above, set $|\phi_D\rangle$ to be the maximally entangled state on $\mathbb{C}^D \otimes \mathbb{C}^D$. The EPR testing problem is to determine whether a given shared state $|\psi\rangle \in \mathbb{C}^D \otimes \mathbb{C}^D$ is equal to or orthogonal to $|\phi_D\rangle$. More precisely, two parties (Alice and Bob) would like to simulate the joint two-outcome POVM $\{\phi_D, I - \phi_D\}$ where we have defined the shorthand $\phi_D := |\phi_D\rangle\langle\phi_D|$.

An (D,ε) EPR tester is a communication protocol for performing a two-outcome measurement $\{M, I - M\}$ such that $\|M - |\phi_D\rangle\langle\phi_D|\| \leq \varepsilon$.

In general EPR testers may differ in a variety of ways:

- If $M \geq \phi_D$ then we say the EPR tester has *perfect completeness*.
- The communication requirements and computational efficiency may vary.
- The protocol may be performed with quantum or classical communication. If quantum communication is used, then it is reasonable to assume that upon input ρ the post-measurement state is $M^{1/2}\rho M^{1/2}/\operatorname{tr}[M\rho]$ or $(I-M)^{1/2}\rho(I-M)^{1/2}/\operatorname{tr}[(I-M)\rho]$, depending on the outcome. If classical communication is used, we need to also consume some entanglement. We say that the test consumes k EPR pairs if given an input of n EPR pairs, it outputs at least $n-k$ EPR pairs (up to ε error) when it reports success. There are no guarantees for orthogonal input states.

We are aware of two previous implementations of EPR testers. The foundational work of quantum information theory [8] gave a $\left(2^n, 2^{-k}\right)$ EPR tester with perfect completeness that used a message of $O(nk)$ classical bits and consumed k EPR pairs. This was improved by [5] to a $(2^n, \frac{2n}{k(2^k+1)})$ EPR tester that sent $2k$ classical bits, consumed k EPR pairs and used $\approx n/k$ bits of shared randomness.

B. EPR testing with constant quantum communication

Our main result in this section is an EPR tester using only a constant amount of quantum communication that is *independent* of the dimension D.

Theorem 1. *For any D and any $\varepsilon > 0$ there exists a (D,ε) EPR tester with perfect completeness using one-way communication from Alice to Bob. The protocol has several variants:*

- *Using $(2 + o(1))\log(1/\varepsilon)$ qubits sent from Alice to Bob, but $\operatorname{poly}(D)$ run-time.*
- *Using $C\log(1/\varepsilon)$ qubits sent from Alice to Bob and $\operatorname{poly}\log(D)$ run-time for some universal constant $C > 0$.*
- *Using either $(8 + o(1))\log(1/\varepsilon)$ or $\approx 4C\log(1/\varepsilon)$ classical bits sent from Alice to Bob (depending on whether computational efficiency is needed) and consuming the same number of EPR pairs.*

We remark that replacing the state $|\phi_D\rangle$ in Theorem 1 with a general entangled state can result in a much larger (and D-dependent) communication cost [14]. Thus we refer to the result as an EPR tester rather than a general entanglement tester.

One application of this result relates to the open question of whether entanglement helps quantum communication complexity. Classically, shared randomness does not significantly reduce communication complexity because large random strings can be replaced by pseudo-random strings that fool protocols[22]. This is called a blackbox reduction because it replaces the random input but does not change the protocol. Quantumly such blackbox reductions are ruled out by efficient entanglement-testing protocols, since they cannot be fooled by any low-entanglement state. A similar result is in [19] but their construction does not yield an EPR tester. See also [23] for a non-blackbox entanglement

reduction that increases the communication cost by an exponential amount.

Proof of Theorem 1:

The main idea is to interpret the results of Section II as a way to test maximally entangled states. By Section II it suffices for Alice and Bob to implement a two-outcome measurement $\{M, I-M\}$ on their shared state with $M = \hat{\mathcal{E}}$ for $\mathcal{E}$ a (D,k,ε) expander. However, it is not immediately clear how to implement this measurement. To do this, we will use a trick that has been used in a variety of contexts (e.g. [4], [14] and Section 2.2.2 of [21]) The protocol (depicted in Figure 3a) is as follows.

1) Alice & Bob initially share a state in registers L, R.
2) Alice prepares the $\log(d)$-qubit state $\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle$ in register a.
3) She performs $W = \sum_{i=1}^{d}|i\rangle\langle i|\otimes U_i$ on a, L.
4) She sends system a to Bob.
5) Bob performs $W^* = \sum_{i=1}^{d}|i\rangle\langle i|\otimes U_i^*$ on a, R.
6) Bob does a two-outcome measurement on a, with the accept outcome corresponding to the state $\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle$ and the "reject" outcome corresponding to the orthogonal subspace.

The measurement operator corresponding to acceptance can be calculated to be $M = \frac{1}{d}\sum_{i=1}^{d} U_i\otimes U_i^*$. By Eq. (2), this is ε close to the desired measurement operator $|\phi_D\rangle\langle\phi_D|$.

The communication cost is $\log(d)$. If we do not care about computationally efficiency, we can obtain $\varepsilon \approx 1/\sqrt{d}$ using random unitaries [17]. For a $\operatorname{poly}\log(d)$ run-time, we can iterate an efficient expander; e.g. applying the construction of [11] k times yields $d = 8^k$ and $\varepsilon \le (2\sqrt{5}/8)^k$. To using classical bits instead we first use the construction of [5] to verify $O(\log 1/\varepsilon)$ EPR pairs that use to teleport the qubits used to verify the rest of the EPR pairs. ∎

This test can be viewed in matrix form as follows. If the initial state of the left/right registers was $|x\rangle_L|y\rangle_R$, after Alice's operation, the state has to have the form

$$\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle(U_i|x\rangle_L)|y\rangle_R. \tag{3}$$

After Bob gets the ancilla and performs his operation W^*, the state has to have the form

$$\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle\left(U_i|x\rangle_L\right)\left(U_i^*|y\rangle_R\right). \tag{4}$$

Let us represent the initial state $|\psi\rangle_{AB} = \sum_{k,\ell}x_{k,\ell}|k,\ell\rangle$ by a matrix X, such that $X_{k,\ell} = x_{k,\ell}$. We now rewrite the final state as a matrix with components $\beta_{(a,L),R}$:

$$\beta = \frac{1}{\sqrt{d}}\begin{bmatrix} U_1XU_1^\dagger \\ U_2XU_2^\dagger \\ \vdots \end{bmatrix}. \tag{5}$$

Passing the final test now means that

$$U_iXU_i^\dagger = U_jXU_j^\dagger, \quad \forall i,j, \tag{6}$$

which is possible (if we have a quantum expander) only for $X = \mathbb{I}$. This means the initial state was $|\psi\rangle_{LR} = |\phi_D\rangle$, and that the final state is $\left(\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle_a\right)\otimes|\phi_D\rangle$.

IV. A COUNTEREXAMPLE TO THE GENERALIZED AREA LAW

In this Section we present our second result – a Hamiltonian with a small bridge term connecting two large halves of a system. Strikingly, this single-link bridge of constant dimensions has a large influence on the entanglement entropy between the two parts of the system, in the ground state.

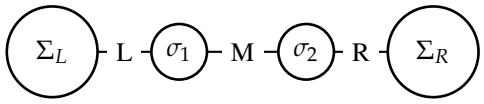

Figure 2. A single-link chain with side operators L and R.

Let the system W consists of two qutrits (σ_1 and σ_2) and two high dimensional systems (Σ_L and Σ_R):

$$W = \Sigma_L\otimes\sigma_1\otimes\sigma_2\otimes\Sigma_R = C^D\otimes C^3\otimes C^3\otimes C^D.$$

We design a gapped Hamiltonian $H = L + M + R$, where L (left) M (middle) and R (right) are projectors acting on $\Sigma_L\otimes\sigma_1$, $\sigma_1\otimes\sigma_2$ and $\sigma_2\otimes\Sigma_R$, respectively, that defies the area law through the cut $\Sigma_L\otimes\sigma_1 \mid \sigma_2\otimes\Sigma_R$. For convenience we write all elements of W in the form

$$\sum_{i,j\in[3]}|\psi_{i,j}\rangle|i\rangle|j\rangle,$$

where $\psi_{i,j}\in\Sigma_L\otimes\Sigma_R$, and $\sum_{i,j\in[3]}|\psi_{i,j}|^2 = 1$. If we fix a basis in Σ_L and Σ_R, respectively, we can think of $\psi_{i,j}$ for every $i,j\in[3]$ as $D\times D$ matrices. Our construction will rely on quantum expanders, i.e. (unitary) $D\times D$ matrices U_2 and U_3 such that for any $D\times D$ matrix X with $|X|^2 = \operatorname{tr}(XX^\dagger) = 1$, $\operatorname{tr}(X) = 0$ we have:

$$|\mathcal{E}(X)| = \frac{1}{3}|X + U_2XU_2^\dagger + U_3XU_3^\dagger| \le (1-c), \tag{7}$$

where $c := 1-\lambda > 0$ is a fixed constant, independent of D. Equation (7) and the triangle inequality imply that for any $D\times D$ matrix X with $|X| = 1$, $\operatorname{tr}(X) = 0$:

$$|U_2XU_2^\dagger - X| + |U_3XU_3^\dagger - X| \ge 3c \tag{8}$$

We now define projectors L, R and M via their zero subspaces $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{M}$. We describe these subspaces by writing states of W in the block matrix form

$$\begin{pmatrix} \psi_{1,1} & \psi_{1,2} & \psi_{1,3} \\ \psi_{2,1} & \psi_{2,2} & \psi_{2,3} \\ \psi_{3,1} & \psi_{3,2} & \psi_{3,3} \end{pmatrix}$$

Note that our way to present a (pure) state of W is unlike the density matrix presentation, and it is only meaningful, because W is a tensor product of four components. The above matrix form (of a vector) is simply a convenient way of rendering the $(3D)^2$ coordinates of a state in W. In this presentation $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{M}$ have convenient expressions. $\mathcal{L}$ is the set of states of the form

$$\begin{pmatrix} \psi_{1,1} & \psi_{1,2} & \psi_{1,3} \\ U_2\psi_{1,1} & U_2\psi_{1,2} & U_2\psi_{1,3} \\ U_3\psi_{1,1} & U_3\psi_{1,2} & U_3\psi_{1,3} \end{pmatrix},$$

where $\psi_{1,1}$, $\psi_{1,2}$ and $\psi_{1,3}$ are arbitrary. $\mathcal{R}$ is the set of states of the form

$$\begin{pmatrix} \psi_{1,1} & \psi_{1,1}U_2 & \psi_{1,1}U_3 \\ \psi_{2,1} & \psi_{2,1}U_2 & \psi_{2,1}U_3 \\ \psi_{3,1} & \psi_{3,1}U_2 & \psi_{3,1}U_3 \end{pmatrix},$$

where $\psi_{1,1}$, $\psi_{2,1}$ and $\psi_{3,1}$ are arbitrary. $\mathcal{M}$ is the set of states of the form

$$\begin{pmatrix} \psi_{1,1} & X & Y \\ X & \psi_{2,2} & \psi_{2,3} \\ Y & \psi_{3,2} & \psi_{3,3} \end{pmatrix},$$

where X, Y and the remaining $\psi_{i,j}$'s are arbitrary. It is easy to check that $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{M}$ are local, as needed. For instance $\mathcal{M}$ is a tensor product of $\Sigma_L \otimes \Sigma_R$ with the subspace S of $\sigma_1 \otimes \sigma_2$ that equates the coefficients of $|1\rangle|2\rangle$ and $|2\rangle|1\rangle$ and also the coefficients of $|1\rangle|3\rangle$ and $|3\rangle|1\rangle$.

Lemma 2. *The unique normalized ground state $|G\rangle$ of $H = L + R + M = (I - \Pi_{\mathcal{L}}) + (I - \Pi_{\mathcal{R}}) + (I - \Pi_{\mathcal{M}})$ written out as a matrix is*

$$G = \frac{1}{3\sqrt{D}} \begin{pmatrix} I & U_2 & U_3 \\ U_2 & U_2^2 & U_2U_3 \\ U_3 & U_3U_2 & U_3^2 \end{pmatrix}$$

Proof: Equation (8) guarantees that I is the only $D \times D$ matrix that commutes with both U_2 and U_3. From this together with the above forms of $\mathcal{L}, \mathcal{R}$ and $\mathcal{M}$, it follows that $|G\rangle$ is the only normalized state vector in $\mathcal{L} \cap \mathcal{R} \cap \mathcal{M}$.

Lemma 3. *The entanglement entropy of $|G\rangle$ along the $\Sigma_L \otimes \sigma_1 \mid \sigma_2 \otimes \Sigma_R$ cut is $\log_2 D$.*

Proof: The reduced density matrix of the $\Sigma_L \otimes \sigma_1$ systems can be directly calculated to be $GG^\dagger$. Since $G = \frac{1}{3\sqrt{D}} \sum_{i,j=1}^{3} U_iU_j \otimes |i\rangle\langle j|$ (letting $U_1 := \mathbb{I}$), we have

$$GG^\dagger = \frac{1}{3D} \sum_{i,i'=1}^{3} U_iU_{i'}^\dagger \otimes |i\rangle\langle i'|. \tag{9}$$

To diagonalize $GG^\dagger$, let $W := \sum_{i=1}^{3} U_i \otimes |i\rangle\langle i|$. Then

$$W^\dagger(GG^\dagger)W = \frac{I}{D} \otimes \frac{1}{3} \sum_{i,i'=1}^{3} |i\rangle\langle i'| \tag{10}$$

which has D eigenvalues equal to $1/D$.

Lemma 4. *The Hamiltonian H has a constant gap.*

Proof: We show that any normalized state $|\psi\rangle$ with energy below the threshold $\tau = c/100$ (where c comes from Equation (8)) should "look similar to" $|G\rangle$. Therefore no (normalized) $|\psi\rangle$ with energy below threshold τ can be orthogonal to $|G\rangle$, and so the eigenvalue gap of H is at least τ. Indeed, let $|\psi\rangle$ be any unit vector with energy at most τ. Since $\langle\psi|I - \Pi_{\mathcal{L}}|\psi\rangle + \langle\psi|I - \Pi_{\mathcal{R}}|\psi\rangle \leq \tau$ there are vectors $|\psi_L\rangle \in \mathcal{L}$ and $|\psi_R\rangle \in \mathcal{R}$ such that $|||\psi\rangle - |\psi_L\rangle||^2 + |||\psi\rangle - |\psi_R\rangle||^2 \leq \tau$. By Lemma 10 of the Appendix there is a $|\psi_{LR}\rangle \in \mathcal{L} \cap \mathcal{R}$ such that $|||\psi_L\rangle - |\psi_{LR}\rangle||^2 + |||\psi_R\rangle - |\psi_{LR}\rangle||^2 = |||\psi_L\rangle - |\psi_R\rangle||^2 \leq 2\tau$, which in turn implies that $|\psi_{LR}\rangle$ and $|\psi\rangle$ have distance at most 3τ. That is, $|\psi\rangle$ is 3τ-close to

$$|\psi_{LR}\rangle = \begin{pmatrix} X & XU_2 & XU_3 \\ U_2X & U_2XU_2 & U_2XU_3 \\ U_3X & U_3XU_2 & U_3XU_3 \end{pmatrix} \tag{11}$$

In particular, all nine blocks of $|\psi\rangle$ are at most 3τ-far to the corresponding blocks of $|\psi_{LR}\rangle$ This together with the fact that $|\psi\rangle$ has small energy with respect to M also implies that $4\tau \geq |U_2X - XU_2| = |U_2XU_2^\dagger - X|$ and $4\tau \geq |U_3X - XU_3| = |U_3XU_3^\dagger - X|$ (for the equalities recall that U_2 and U_3 are unitary), which then by Equation (8) implies that X has to be $1/100$-close to $\frac{1}{3\sqrt{D}}I$ (since its component that is orthogonal to I must be smaller in Frobenius norm than $1/100$). This in turn implies that $|\psi\rangle$ cannot be orthogonal to $|G\rangle$.

V. The abstract Hamiltonian can be implemented locally

The Hamiltonian construction in Section IV has very interesting properties (a unique, very entangled ground state and a constant gap), but the H_L and H_R terms are nonlocal. We now wish to decompose them into local terms, while retaining their desirable properties. This is done in several steps.

We first use a variant of Kitaev's Local Hamiltonian construction to find a local Hamiltonian H_L^{Kit} with ground states similar to those of H_L in Section IV except with an additional ancilla. The price we pay in this construction is an inverse polynomial gap instead

of a constant one. We can multiply the local interaction terms in H_L^{Kit} by a large prefactor to get a Hamiltonian H'_L with a constant gap, as stated in Claim 5. However, its terms have polynomially large, unphysical norms.

Second, in Claim 6 we derive a Hamiltonian with similar properties to the four-particle Hamiltonian H from Section IV. To do this we use H'_L twice, once on the left side and once on the right side of a new larger system, together with the original middle interaction H_M. This gives us a local Hamiltonian $H'_{LMR} = H'_L + H'_R + H_M$ with a constant gap, and a unique, entangled ground state, just as we had for H. Note that the large interaction terms appear only in $H'_L + H'_R$, and that the central interaction is $O(1)$.

Finally, in Theorem 9, we decompose each high-norm local interaction term in H'_L and H'_R into many local, constant-norm terms. Thus, we end up with a local Hamiltonian H_{LMR}^{gadget} with all the desired properties of H_{LMR} form Section IV. However, we again pay a price – each particle is involved in polynomially many 2-body interactions.

A. Evaluating a quantum expander locally (3 computations in parallel)

Let us translate the Hamiltonian from Section IV into a local one. We start by mimicking H_L by a sum of local terms. The Hamiltonian H_L acts on a space of dimension $3D$, and its ground states have form

$$|\Phi_x\rangle = \frac{1}{\sqrt{3}} \sum_{i=1}^{3} |i\rangle \otimes U_i |x\rangle. \tag{12}$$

We will now enlarge our system and find a local Hamiltonian H'_L, whose ground state will be close to

$$|\Phi_x\rangle \otimes |w\rangle, \tag{13}$$

with $|w\rangle$ some state of an extra register.

Claim 5. *There exists a local Hamiltonian with constant spectral gap, set on a 1D chain of n qudits, such that all ground states are ϵ-close to the form* (13)*. The local terms of the Hamiltonian are of norm bounded by* $O(\mathrm{poly}(n))$.

We construct this Hamiltonian following Kitaev's Local Hamiltonian approach [20]. It allows us to write down a Hamiltonian whose ground states are history states of a quantum computation V, i.e.

$$|\psi_y^{hist}\rangle = \frac{1}{\sqrt{T}} \sum_{t=0}^{T} |t\rangle_k \otimes V_t \dots V_1 \left(|y\rangle \otimes |0\rangle_a\right), \tag{14}$$

where k is an extra "clock" register, a is an ancilla register, $|y\rangle$ is some initial state of a data register and V_t are the gates of some circuit V, acting on the data register. Our data register will contain N data qubits (for simplicity, set $2^N = D$) and a "control" qutrit c. We want to get the history state of the circuit V with unitaries

$$V_t = \sum_{i=1}^{3} |i\rangle\langle i|_c \otimes U_{i,t} \tag{15}$$

for $t = 1, \dots, \tau$, where $U_{i,t}$ are the gates of the quantum expander[1], with τ gates. On top of this, we pad the circuit V with many identity gates $V_t = \mathbb{I}$ for $\tau < t \leq T$, for some $T \gg \tau$, setting $\epsilon = \frac{\tau}{T} = \frac{1}{\mathrm{poly}(N)}$. We will require an extra clock register k capable of locally implementing a clock with $T+1$ clock states, as well as an ancilla scratch register a. The ground states (history states of V) for the new Hamiltonian H'_L are of the form:

$$|\Psi_x\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_k \otimes \\ \otimes V_t \dots V_1 \left(\frac{1}{\sqrt{3}} \sum_{i=1}^{3} |i\rangle_c |x\rangle_d |0 \cdots 0\rangle_a \right). \tag{16}$$

We will build $H_L^{Kit} = H_{init} + H_{prop}$ from two parts. First, propagation-checking:

$$H_{prop} = \frac{1}{2} \sum_{t=1}^{T} \left(|t-1\rangle\langle t-1|_k + |t\rangle\langle t|_k\right) \\ - \frac{1}{2} \sum_{t=1}^{T} \left(|t-1\rangle\langle t|_k \otimes V_t^\dagger + |t\rangle\langle t-1|_k \otimes V_t\right). \tag{17}$$

Second, we need to ensure proper initialization by adding a projector that prefers a uniform superposition on the control qutrit when the clock register is $|0\rangle_k$ (we want all three computations to run on the same input). Adding standard ancilla initialization-checking, we get

$$H_{init} = |0\rangle\langle 0|_k \otimes \left[\mathbb{I} - |u_3\rangle\langle u_3|_c + \sum_{i=1}^{s} |1\rangle\langle 1|_{a_i}\right],$$

with $|u_3\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + |3\rangle)$. We can now implement the clock register and the corresponding projectors by a a 5-local, unary clock with $T+1$ qubits [20]. The Hamiltonian H_L^{Kit} is positive-semidefinite, and frustration-free. It has a zero-energy state of the form (16) for any basis state $|x\rangle$ of the N working qubits. Furthermore, the energy gap of H_L^{Kit} to eigenstates with nonzero energy is $\Delta_L^{Kit} = \Theta\left(T^{-2}\right)$. Using the 1D construction for a line of 8-dimensional qudits from [1] or [12], which also have a gap that scales as an inverse polynomial in T. This results in a 1D Hamiltonian with the properties we want.

Let us consider the groundstates more closely. For $t \gg \tau$, the data register is in the desired state $|\Phi_x\rangle$

[1]Furthermore, we want these $U_{i,t}$ in a form that uncomputes the scratch ancilla register a at the end.

(12), the ancilla register is uncomputed, and it is only the clock register that changes. Recalling $T \gg \tau$, we realize that each $|\Psi_x\rangle$ can be rewritten as

$$\begin{aligned}|\Psi_x\rangle &= \frac{1}{\sqrt{T}}\sum_{t=1}^{\tau}|\varphi_{x,t}\rangle \\ &+ |\Phi_x\rangle_{cd}\otimes\frac{1}{\sqrt{T}}\left(\sum_{t=\tau+1}^{T}|t\rangle_k\right)\otimes|0\cdots0\rangle_a \\ &= \sqrt{\epsilon}\,|v_x\rangle + \sqrt{1-\epsilon}\,|\Phi_x\rangle_{cd}\otimes|w\rangle, \end{aligned} \tag{18}$$

with some normalized vectors $|v_x\rangle$ and $|w\rangle$. Each ground state is thus as close to $|\Phi_x\rangle|w\rangle$ (13) as we want, because we are free to choose T.

The gap of the Hamiltonian H_L^{Kit} is however not constant. We rescale the interaction strengths of all terms in H_L^{Kit} by T^2 (or by a higher polynomial in T for the 1D clock construction), and look at $H'_L = poly(T)\times H_L^{Kit}$. This new H'_L satisfies the requirements of Claim 5.

B. A local Hamiltonian with an entangled ground state

We now take two copies of the system from the previous Section, and construct a Hamiltonian $H'_{LMR} = H'_L + H'_R + H_M$, with a 2-local middle term

$$\begin{aligned}H_M = &\frac{1}{2}\left(|12\rangle - |21\rangle\right)\left(\langle 12| - |21\rangle\right)_{a_L,a_R} \\ &+ \frac{1}{2}\left(|13\rangle - |31\rangle\right)\left(\langle 13| - |31\rangle\right)_{a_L,a_R}, \end{aligned} \tag{19}$$

an implementation of the projector M from Section IV.

Claim 6. *The 1D, qudit Hamiltonian $H'_{LMR} = H'_L + H'_R + H_M$ with terms of norm* poly(n)*, has a unique, entangled ground state, and a constant energy gap.*

Let us take the Hamiltonian H'_L with a ground state subspace spanned by basis states of the form (18). The energy gap above this ground state subspace is a constant. Let us take another copy of such a system and call its Hamiltonian H'_R. The ground state subspace of these two copies is spanned by basis states of the form

$$\begin{aligned}|\Psi_x\rangle|\Psi_y\rangle = &\sqrt{\epsilon(2-\epsilon)}\,|z^{\epsilon}_{xy}\rangle \\ &+ (1-\epsilon)|\Phi_x\rangle|\Phi_y\rangle|w\rangle^{\otimes 2}. \end{aligned} \tag{20}$$

Note that each basis state $|\Psi_x\rangle|\Psi_y\rangle$ is close to the state

$$|\Phi_x\rangle|\Phi_y\rangle|w\rangle|w\rangle. \tag{21}$$

The Hamiltonians H'_L and H'_R act on independent subspaces, while both Hamiltonians have a constant energy gap above the ground state subspace. Therefore, the ground state subspace of $H'_L + H'_R$ is spanned by states of the form (20), with a constant gap above this subspace. Let us now look at how a state with energy less than some constant E_{LR} must look like.

Claim 7. *Any state $|c_{LR}\rangle$ that has an energy less than a small constant E_{LR} for the Hamiltonian $H'_L + H'_R$, has overlap at least $1-\left(\epsilon+\sqrt{\frac{E_{LR}}{\Delta'_{LR}}}\right)$ with the subspace spanned by states of the form* (21)*.*

Proof: Let us write

$$|c_{LR}\rangle = \sqrt{1-|q|^2}\left(\sum_{x,y}c_{xy}|\Psi_x\rangle|\Psi_y\rangle\right) + q|q\rangle, \tag{22}$$

and deduce that

$$\begin{aligned}E_{LR} &\geq \langle c_{LR}|H'_L + H'_R|c_{LR}\rangle = |q|^2\langle q|H'_L + H'_R|q\rangle \\ &\geq \Delta'_{LR}|q|^2. \end{aligned} \tag{23}$$

Therefore, the overlap of $|c_{LR}\rangle$ with the subspace spanned by (20) is at least $1-\sqrt{\frac{E_{LR}}{\Delta'_{LR}}}$. Continuing from there, the overlap of such state $|c_{LR}\rangle$ with the subspace spanned by (21) is at least $1-\left(\epsilon+\sqrt{\frac{E_{LR}}{\Delta'_{LR}}}\right)$, assuming ϵ and E_{LR} are small enough constants.

We are now ready to use the results of Section IV to prove that the ground state of $H'_L + H'_R + H_M$ is unique and entangled.

First, let us rewrite the components of any superposition of basis states (21) as a matrix. The $|w\rangle|w\rangle$ part is a single state of the extra (clock and ancilla) registers. Therefore, the top left corner (corresponding to the $|w\rangle|w\rangle$ state of the extra register) of (21) as a matrix then is the same as in (11) in Section IV (without loss of generality, we assume $U_0 = \mathbb{I}$):

$$\frac{1}{3}\begin{bmatrix} X & XU_2 & XU_3 \\ U_2X & U_2XU_2 & U_2XU_3 \\ U_3X & U_3XU_2 & U_3XU_3 \end{bmatrix} \tag{24}$$

with $X_{a,b} = x_a y_b$, for $|x\rangle = \sum_{a=1}^{D} x_a|a\rangle$ and $|y\rangle = \sum_{b=1}^{D} y_b|b\rangle$. The states in this clean form are the ground states of $H_L + H_R$, the abstract Hamiltonians of Section IV. We now know that any state $|c_{LR}\rangle$ that has an energy less than some E_{LR} for $H'_L + H'_R$, has a large overlap with the subspace spanned by (21), therefore as a matrix, this state is close to the form (11).

Second, we add the (positive semidefinite) Hamiltonian H_M (19) acting on the control registers. Its ground states (rewritten as a matrix in each block corresponding to some basis state of the ancilla registers) must be of the form

$$\begin{bmatrix} ? & Z & W \\ Z & ? & ? \\ W & ? & ? \end{bmatrix}. \tag{25}$$

Any state that has energy less than E_M for H_M has to be close to this form, as shown in Section IV.

Putting the conditions on low energy for both $H'_L + H'_R$ and H_M, we end up with $X = \frac{1}{\sqrt{D}}\mathbb{I}$, i.e. with a

low energy state

$$|g_{LMR}\rangle = \frac{1}{\sqrt{D}} \sum_{x=1}^{D} |\Phi_x\rangle|\Phi_x\rangle|w\rangle|w\rangle$$
$$= \frac{1}{3\sqrt{D}} \begin{bmatrix} \mathbb{I} & U_1 & U_2 \\ U_1 & U_1U_1 & U_1U_2 \\ U_2 & U_2U_1 & U_2U_2 \end{bmatrix}, \quad (26)$$

again writing the only nonzero block corresponding to the $|w\rangle|w\rangle$ state of the extra registers. Now any state that has energy less than a constant has to be close to this state. Therefore, the ground state of $H'_L + H'_R + H_M$ is unique, and the Hamiltonian has a constant gap.

Finally, we need to show that the ground state is entangled. This is straightforward, as the ground state is close to (26), which is itself close to the maximally entangled state, using the following lemma with $|\varphi\rangle = |g_{LMR}\rangle$ and $\langle\varphi|\phi_D\rangle = \frac{1}{3}$.

Lemma 8. *Any state $|\varphi\rangle$ that has a constant overlap c with a maximally entangled state $|\phi_D\rangle = \frac{1}{\sqrt{D}} \sum_{x=1}^{D} |x\rangle|x\rangle$ is close to maximally entangled.*

Proof: Let us look at the Schmidt decomposition $|\varphi\rangle = \sum_{k=1}^{\chi} \lambda_k |l_k\rangle|r_k\rangle$. Assuming $|\varphi\rangle$ has at least a constant overlap c with $|\phi_D\rangle$, we obtain

$$c \leq \langle\phi_D|\varphi\rangle = \frac{1}{\sqrt{D}} \sum_{x=1}^{D} \sum_{k=1}^{\chi} \lambda_k \langle x|l_k\rangle\langle x|r_k\rangle$$
$$= \frac{1}{\sqrt{D}} \sum_{k=1}^{\chi} \lambda_k \langle \tilde{r}_k|l_k\rangle \leq \frac{1}{\sqrt{D}} \sum_{k=1}^{\chi} \lambda_k, \quad (27)$$

where $\tilde{r_k}$ are vectors related to $|r_k\rangle$, obeying $\langle x|r_k\rangle = \langle\tilde{r}_k|x\rangle$. For a constant c, the entanglement of the state $|\varphi\rangle$ must be large, including $\Theta(D)$ terms of size $\Theta\left(D^{-\frac{1}{2}}\right)$, resulting in $-\sum_i \lambda_i \log \lambda_i = \Theta(\log D)$. When $D = 2^N$, this is $\Theta(N)$.

This concludes the proof of Claim 6.

C. Decomposing the Hamiltonian H'_L into $O(1)$-strength interaction terms

We now handle the problem of large interaction norm. The interactions in the Hamiltonian H_L^{clock} have norm $\mathrm{poly}(T)$. Each such term can be decomposed using the *strengthening quantum gadget construction* by Nagaj and Cao [10], into $\mathrm{poly}(T)$ interactions with $\mathrm{poly}(T)$ extra ancilla qubits. The gap of this new H'_L will remain a constant, while any state in its ground state will now be $1/\mathrm{poly}(T)$ close to some $|\Psi_x\rangle|0\cdots0\rangle_{\text{new ancillas}}$, with $|\Psi_x\rangle$ from (18). This also implies that each (less than a small constant energy) state of H'_L is $1/\mathrm{poly}(T)$ close to the state $|\Phi_x\rangle|w\rangle|0\cdots0\rangle_{\text{new ancillas}}$ for some x. However, this is just what we had in (13), with an expanded ancilla register state $|w'\rangle = |w\rangle|0\cdots0\rangle$.

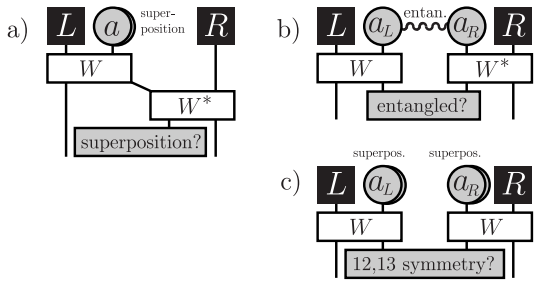

Figure 3. EPR testing procedures. a) The test from Section III-B. b) A modified test with two ancillas. c) The Hamiltonian from Section IV can be also easily recast as an EPR testing protocol.

Therefore, all of the arguments of Section V-B go through, and we have shown that

Theorem 9. *There exists a 2-body Hamiltonian on n qudits, whose terms are of $O(1)$ norm. The interaction graph is as in Figure I, where the two particles on the two sides of the cut are qutrits. All particles are involved in at most $\mathrm{poly}(n)$ interactions. Moreover, the Hamiltonian is gapped with a unique ground state, such that the entanglement entropy across the middle cut scales as $\Omega(n^c)$ for some $0 < c < 1$.*

VI. Entanglement testing and ground states of Hamiltonians

We now connect our two results more directly. Starting from the EPR testing protocol of Section III-B, we turn it into a Hamiltonian violating the generalized area law, using Kitaev's circuit-to-Hamiltonian construction. In fact, we use a slight variant of the protocol, which uses two ancillas (see Figure 3b), as it translates to a Hamiltonian more easily.

We first describe the modified EPR testing protocol. Alice has two registers, $L \otimes a_L$, and Bob has two registers denoted $a_R \otimes R$, where R, L are of large dimension D and a_R,a_L are of constant dimension d. They wish to check whether their joint state $|\psi\rangle_{LR}$ on registers $L \otimes R$ is maximally entangled. First, Alice and Bob pre-share a maximally entangled state on $a_L \otimes a_R$:

$$|\phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle_{a_L}|i\rangle_{a_R} \quad (28)$$

Second, Alice applies the unitary $W = \sum_{i=1}^{d} |i\rangle\langle i| \otimes U_i$ to $a_L \otimes L$, and Bob applies W^* to $a_R \otimes R$. Finally, they apply a projective measurement on $a_L \otimes a_R$ of the state $|\phi_d\rangle$ (28). It is not difficult to see that this too is an EPR testing protocol; the test passes with probability close to 1 if and only if the original state $|\psi\rangle_{LR}$ was very close to the maximally entangled state.

To encode this protocol into a Hamiltonian via the circuit-to-Hamiltonian construction, we use *two* independent, two-step clocks. (We will think of the circuit

W as well as W^* as applied in a single time step). The Hamiltonian will thus act on four registers, L, R and two enlarged registers, $A_L = a_L \otimes C_L$ and $A_R = a_R \otimes C_R$ with C_L, C_R being the two 2-dimensional spaces of the two clocks, respectively. We write the basis states of A_L, A_R as $|0,i\rangle$ and $|1,i\rangle$ for $i \in \{1,..,d\}$.

The Hamiltonian consists of the following terms. An "initialization" and "output" term on $A_L \otimes A_R$:

$$H_M = \sum_{s=0}^{1} \sum_{i,j=1}^{d} |s,i\rangle\langle s,i|_{A_L} \otimes |s,j\rangle\langle s,j|_{A_R} - \sum_{s=0}^{1} \sum_{i=1}^{d} |s,i\rangle\langle s,i|_{A_L} \otimes |s,i\rangle\langle s,i|_{A_R} \quad (29)$$

whose ground states have the form $|1,i\rangle|0,j\rangle$ and $|0,i\rangle|1,j\rangle$ for any i,j, but more importantly $\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|0,i\rangle|0,i\rangle$ and $\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|1,i\rangle|1,i\rangle$. These two states are maximally entangled states of the ancillas when the "clocks" are both 0 (initialization) or both 1 (output).

Second, we have the "left-computation-checking" Hamiltonian, which acts on the registers a_L and L:

$$H_L = \frac{1}{2}\sum_{i=1}^{d}\left(|0i\rangle\langle 0i| + |1i\rangle\langle 1i|\right)_{a_L} \otimes \mathbb{I}_L - \frac{1}{2}\sum_{i=1}^{d}|1i\rangle\langle 0i| \otimes W - \frac{1}{2}\sum_{i=1}^{d}\otimes|0i\rangle\langle 1i| \otimes W^\dagger. \quad (30)$$

We define H_R similarly, replacing W by W^* (and $W^\dagger$ by W^T). The final Hamiltonian, $H = H_M + H_L + H_R$ is our desired counterexample. We claim that its unique, frustration-free ground state is the "history" state

$$|\Psi\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}\left(|0,i\rangle_{a_L} + (W \otimes \mathbb{I})\,|1,i\rangle_{a_L}\right) \times \times \left(|0,i\rangle_{a_R} + (\mathbb{I} \otimes W^*)\,|1,i\rangle_{a_R}\right)|\phi_D\rangle_{LR}.$$

It is not difficult to check that this is a maximally entangled state of dimension dD, by observing that the Schmidt rank is dD and the coefficients are uniform.

VII. Discussion and Open Questions

What do our results imply regarding further progress on the area law problem? A crucial issue is the geometry of the underlying graph; of course, the 2D lattice case is wide open. A more modest goal would be to reduce the degree of the interconnection graph in our final construction to a constant. Such a step already seems to require significant progress in our understanding of related notions, e.g., parallel circuit-to-Hamiltonian constructions (see e.g.,[9]), and quantum expanders which are geometrically constrained.

We note that our intermediate construction (see Claim 6) violates the area law using very simple interconnection geometry – albeit with Hamiltonian local terms of polynomially large weights. Depending on the construction, the interaction graph consists either of a 1D lattice or two 2D lattices joined by a single edge. In each case, there is a cut edge such that the term of the Hamiltonian acting across that cut has unit norm, and the norms of all the terms acting to the left (right) of it have norm greater than 1 and bounded above by a polynomial in n. This can be viewed as a family of counterexamples to a different kind of generalized area law: one where the terms of the Hamiltonian acting across the cut are required to be of unit norm. The rationale of this condition is that large norm terms on each side of the cut should only increase the entanglement within the two regions on each side of the cut and therefore by monogamy of entanglement only *decrease* the entanglement across the cut. The fact that there are 1D and 2D counterexamples to this kind of an area law suggests that the intuition behind a 2D area law, if true, is more subtle.

The entanglement-testing problem and the area-law question appear to be closely related. Can any area-law-violating Hamiltonian be connected to an entanglement-testing protocol with communication pattern corresponding to the interaction graph of the Hamiltonian? More generally, in what ways can Hamiltonians be viewed as *testers* for their ground states? Making such an equivalence rigorous might open up a whole new set of tools to studying the area law question, and more generally, help develop better intuition for local Hamiltonians and their groundstates. A related question is whether EPR testing is in fact *equivalent* in some sense to the property of being a quantum expander.

VIII. Acknowledgements

The authors thank the Simons Institute (the Quantum Hamiltonian Complexity program) where part of this work was done. DA acknowledges the support of ERC grant 030-8301 and BSF grant 037-8574. AWH was funded by NSF grant CCF-1111382 and ARO contract W911NF-12-1-0486. ZL was supported by NSF Grants CCF-0905626 and CCF-1410022 and Templeton Grants 21674 and 52536. DN thanks the Slovak Research and Development Agency grant APVV-0808-12 QIMABOS. MS is supported by the NSF Grant No. CCF-0832787, "Understanding, Coping with, and Benefiting from, Intractability" and by CISE/MPS 1246641. UV was supported by ARO Grant W911NF-12-1-0541, NSF Grant CCF-0905626, and Templeton Grants 21674 and 52536.

References

[1] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. The power of quantum systems on a line. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, 0:373–383, 2007, 0705.4077.

[2] A. Ambainis and A. Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In K. Jansen, S. Khanna, J. Rolim, and D. Ron, editors, *APPROX-RANDOM*, volume 3122 of *Lecture Notes in Computer Science*, pages 249–260. Springer, 2004, quant-ph/0404075.

[3] I. Arad, A. Kitaev, Z. Landau, and U. Vazirani. An area law and sub-exponential algorithm for 1D systems. In *Proceedings of the 4th Innovations in Theoretical Computer Science (ITCS)*, 2013, 1301.1162.

[4] A. Barenco, B. André, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello. Stabilization of quantum computations by symmetrization. *SIAM J. Comput.*, 26:1541–1557, 1997, quant-ph/9604028.

[5] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, pages 449–458, 2002, quant-ph/0205128.

[6] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma. Quantum expanders and the entropy difference problem, 2007, quant-ph/0702129.

[7] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma. Quantum expanders: motivation and construction. In *CCC*, 2008, 0709.0911.

[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 52:3824–3851, 1996, quant-ph/9604024.

[9] N. P. Breuckmann and B. M. Terhal. Space-time circuit-to-hamiltonian construction and its applications. *Journal of Physics A: Mathematical and Theoretical*, 47(19):195304, 2014.

[10] Y. Cao and D. Nagaj. Perturbative gadgets without strong interactions, 2014. arXiv:1408:????

[11] D. Gross and J. Eisert. Quantum Margulis Expanders. *Q. Inf. Comp.*, 8(8/9):722–733, 2008, 0710.0651.

[12] S. Hallgren, D. Nagaj, and S. Narayanaswami. The local hamiltonian problem on a line with eight states is qma-complete. *Quantum Information & Computation*, 13(9-10):721–750, 2013.

[13] A. W. Harrow. Quantum expanders from any classical Cayley graph expander. *Quantum Inf. Comput.*, 8(8&9):715–721, 2008, 0709.1142.

[14] A. W. Harrow and D. W. Leung. A communication-efficient nonlocal measurement with application to communication complexity and bipartite gate capacities. *IEEE Trans. Inf. Theory*, 57(8):5504–5508, 2011, 0803.3066.

[15] M. B. Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2007(08):P08024, 2007, 0705.2024.

[16] M. B. Hastings. Entropy and entanglement in quantum ground states. *Phys. Rev. B*, 76:035114, 2007, cond-mat/0701055.

[17] M. B. Hastings. Random unitaries give quantum expanders. *Phys. Rev. A*, 76:032315, 2007, 0706.0556.

[18] M. B. Hastings and A. W. Harrow. Classical and quantum tensor product expanders. *Q. Inf. Comp.*, 9(3&4):336–360, 2009, 0804.0011.

[19] R. Jain, J. Radhakrishnan, and P. Sen. Optimal direct sum and privacy trade-off results for quantum and classical communication complexity, 2008, 0807.1267.

[20] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, Boston, MA, USA, 2002.

[21] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, J. Kelner, A. Hassidim, and P. Shor. Making and breaking quantum money. In *Innovations in Computer Science (ICS)*, pages 20–31, 2010, 0912.3825.

[22] I. Newman. Private vs. common random bits in communication complexity. *Inf. Process. Lett.*, 39(2):67–71, 1991.

[23] Y. Shi and Y. Zhu. Tensor norms and the classical communication complexity of nonlocal quantum measurement. *SIAM J. Comput.*, 38(3):753–766, 2008, quant-ph/0511071.

APPENDIX

Here we show a lemma about being close to two "independent" subspaces. It immediately implies that if $\phi \in H \otimes H'$ is a unit vector such that its projections on $\mathcal{S} \otimes H'$ and on $H \otimes \mathcal{T}$ have length close to one (i.e. ϕ is close to both subspaces), then ϕ is close to some unit vector $x \in \mathcal{S} \otimes \mathcal{T}$.

Lemma 10. *Let $\mathcal{S} \leq H$ and $\mathcal{T} \leq H'$ respective subspaces of Hilbert spaces H and H'. Let $s \in \mathcal{S} \otimes H'$ and $t \in H \otimes \mathcal{T}$ arbitrary. Then there is an $x \in \mathcal{S} \otimes \mathcal{T}$ such that $||s-x||^2 + ||t-x||^2 = ||s-t||^2$.*

Proof: We can decompose s as $s = s' + s''$ where $s' \in \mathcal{S} \otimes \mathcal{T}$ and $s'' \in \mathcal{S} \otimes \mathcal{T}^\perp$. Then $\langle s', s'' \rangle = 0$. We also have that $\langle t, s'' \rangle = 0$. Then $0 = \langle t - s', s'' \rangle = \langle t - s', s - s' \rangle$, or differently said, the $ss't$ triangle is a right triangle, where the right angle is at s'. Then by the Pythagorean theorem the Lemma holds with the choice $x = s'$.