Title: Entanglement can be made robust [Joint work with Aram Harrow]

Date: Oct 07, 2015 04:00 PM

URL: http://pirsa.org/15100027

Abstract: <p>The accumulated intuition from the last decades of research on quantum entanglement is that this phenomenon is highly non-robust, and very hard to maintain in the presence of de-cohering noise at non-zero temperatures. In recent years however, and motivated, in part, by a quest for a quantum analog of the PCP theorem researches have tried to establish, at least in theory, whether or not we can preserve quantum entanglement at "constant" temperatures that are independent of system size. This would imply that any quantum state with energy at most, say 0.05 of the total available energy of the Hamiltonian, would be highly-entangled.</p>

<p>A conjecture formalizing this notion was defined by Freedman and Hastings : called NLTS - it stipulates the existence of locally-defined quantum systems that retain long-range entanglement even at high temperatures. Such a conjecture does not only present a necessary condition for quantum PCP, but also poses a fundamental question on the nature of entanglement itself. To this date, no such systems were found, and moreover, it became evident that even embedding local Hamiltonians on robust, albeit "non-physical" topologies, namely expanders, does not guarantee entanglement robustness.</p>

<p>In this study, refute the intuition that entanglement is inherently fragile: we show that locally-defined quantum systems can, in fact, retain long-range entanglement at high temperatures. To do this, we construct an explicit family of 7-local Hamiltonians, and prove that for such local Hamiltonians ANY low-energy state is hard to even approximately simulate by low-depth quantum circuits of depth o(log(n)). In particular, this resolves the NLTS conjecture in the affirmative, and suggests the existence of quantum systems whose low-energy states are not only highly-entangled but also "usefully"-entangled, in the computational-theoretic sense. </p>

Expansion of a distribution

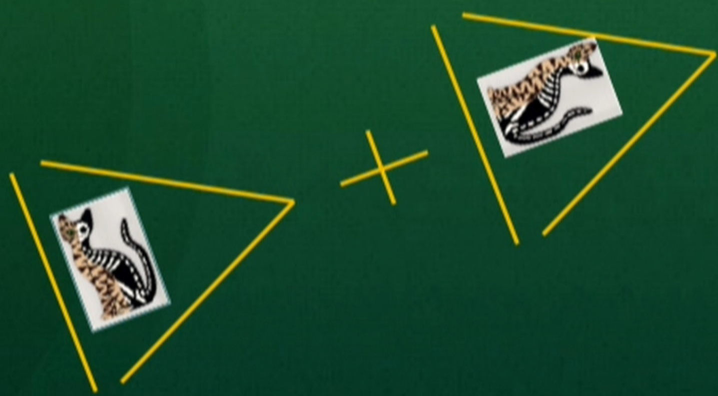
- D is some distribution.
- m is a parameter.
- Consider the graph on the boolean cube with edges of length m.
- Choose set S, of measure at most ½ according to D.
- Consider the boundary of S.

Expansion of a distribution

- D is some distribution.
- m is a parameter.
- Consider the graph on the boolean cube with edges of length m.
- Choose set S, of measure at most ½ according to D.
- Consider the boundary of S.
- Minimize over all such S.

Example of vertex expansion: CATs !

- Simple examples:
  - The CAT-state
  - Quantum code-states
  - Uniform super-positions over classical codes.



CAT state is hard

- Suppose U generates the cat state a=|00..0>+|11..1> in depth d, from the state |000..0>
- Consider the "negative" cat state b=|00..0>-|11…1>.
- Then U*b is supported on strings with Hamming weight at least 1.
- Write the local Hamiltonian \sum_j |1><1|_j, and conjugate by U.

CAT state is hard

- Suppose U generates the cat state a=|00..0>+|11..1> in depth d, from the state |000..0>
- Consider the “negative” cat state b=|00..0>-|11…1>.
- Then U*b is supported on strings with Hamming weight at least 1.
- Write the local Hamiltonian \sum_i |1><1|_i, and conjugate by U.
- It assigns 0 energy to (a) and non-zero energy to (b), so it distinguishes them.
- But H can only couple terms of Hamming distance at most 2^d,whereas (a),(b) differ only on terms |x><y|, where x,y differ by n.
- Therefore d is at least log(n).

Expansion of a distribution

- D is some distribution.
- m is a parameter.
- Consider the graph on the boolean cube with edges of length m.
- Choose set S, of measure at most ½ according to D.
- Consider the boundary of S.

Expansion of a distribution

- D is some distribution.
- m is a parameter.
- Consider the graph on the boolean cube with edges of length m.
- Choose set S, of measure at most ½ according to D.
- Consider the boundary of S.
- Minimize over all such S.

Claim: distributions of bounded-depth circuits expand well

- Start from a quantum-state generated by depth-d circuit U: $|\psi\rangle = U|0^{\otimes N}\rangle$
- Consider it's induced distribution on the first n qubits.

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

Claim: distributions of bounded-depth circuits expand well

- Start from a quantum-state generated by depth-d circuit U: $|\psi\rangle = U|0^{\otimes N}\rangle$
- Consider it's induced distribution on the first n qubits.

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

- It's expansion is lower bounded by 1/2, for m at least $2^d * \sqrt{n}$.

Lower-bounds
Proof

- Fix some set constant measure S, and its complement T :
  - Cat = |S> + |T>
  - Cat- = |S> - |T>.

Lower-bounds
Proof

- Fix some set constant measure S, and its complement T :
  - Cat = |S> + |T>
  - Cat- = |S> - |T>.
- Suppose |Cat> is generated by depth-d circuit U.
- Apply degree-$\sqrt{n}$ Chebyshev polynomials to the conjugated projections on 0, U |0><0| U*

Lower-bounds
Proof

- Fix some set constant measure S, and its complement T :
  - Cat = |S> + |T>
  - Cat- = |S> - |T>.
- Suppose |Cat> is generated by depth-d circuit U.
- Apply degree-$\sqrt{n}$ Chebyshev polynomials to the conjugated projections on 0, U |0><0| U*
- This LH distinguishes Cat, and Cat- states significantly:
  - It has a constant spectral gap.

Lower-bounds
Proof

- Fix some set constant measure S, and its complement T :
  - Cat = |S> + |T>
  - Cat- = |S> - |T>.
- Suppose |Cat> is generated by depth-d circuit U.
- Apply degree-$\sqrt{n}$ Chebyshev polynomials to the conjugated projections on 0, U |0><0| U*
- This LH distinguishes Cat, and Cat- states significantly:
  - It has a constant spectral gap.
- On the other hand, it is merely $2^d * \sqrt{n}$ –local.
- ➔S and T share a large boundary for m at most $2^d * \sqrt{n}$.

Locally-testable codes

Recap

- We know that low-expansion distributions (a la CAT) are hard.
- We want a quantum code, for which even high energy states have low-expansion.
- What can we do?

Locally-testable codes

Locally-testable codes

- Classical code C, with an extra property:
  - there exists a local tester T.
  - Given any word w, reads out O(1) position from w
  - Accepts/rejects w.p. porportional to dist(w,C).

Locally-testable codes

- Classical code C, with an extra property:
  - there exists a local tester T.
  - Given any word w, reads out O(1) position from w
  - Accepts/rejects w.p. porportional to dist(w,C).
- Check-out most updated survey by Goldreich.
- Tightly-connected to classical PCP.
  - Appears in almost all known PCP constructions.
  - Actual PCP theorems encode solution space into an LTC!

Example : Hadamard code

- Encoded space – any word of length n.
- Encode by writing all inner-products <w,x> for all x in $\{0,1\}^n$.
- Rate is log(n).
- It is locally testable [BLR] !
  - Sample x,y at random
  - Accept if and only if c(x) + c(y) = c(x+y).

Do LTCs enforce low expansion?

- We want: LTCs to enforce low expansion for distributions with “low-energy”.
- Consider the uniform distribution on codewords of an LTC.
- Suppose you add words that violate only few checks.

Do LTCs enforce low expansion?

- We want: LTCs to enforce low expansion for distributions with “low-energy”.
- Consider the uniform distribution on codewords of an LTC.
- Suppose you add words that violate only few checks.
- How does it look like ?

Is there a quantum analog?

- qLTC conjecture [AE'14]: quantum codes, with local check check matrix H, such that

$$\frac{1}{m}\langle\psi|H|\psi\rangle \propto dist(\psi, \mathcal{C})$$

- We show:
  - qLTC with linear distance is NLTS
  - Therefore, the qLTC conjecture is stronger !

Is there a quantum analog?

- qLTC conjecture [AE'14]: quantum codes, with local check check matrix H, such that

$$\frac{1}{m}\langle\psi|H|\psi\rangle \propto dist(\psi,\mathcal{C})$$

- We show:
  - qLTC with linear distance is NLTS
  - Therefore, the qLTC conjecture is stronger !
- Alas - Our construction is NOT a qLTC !

The hypergraph product code [Tillich-Zémor '09]

- Consider a classical parity-check code C
  - Parameterized by a bi-partite graph G(A,B).
- Generate two new linear codes:
  - Bits are A x A, B x B
  - Checks are A x B, B x A.
- Induces a quantum CSS code.
- Checks are commuting !
- Locality is the same as the maximal degree of G.

Hyper-graph product of the Hadamard code

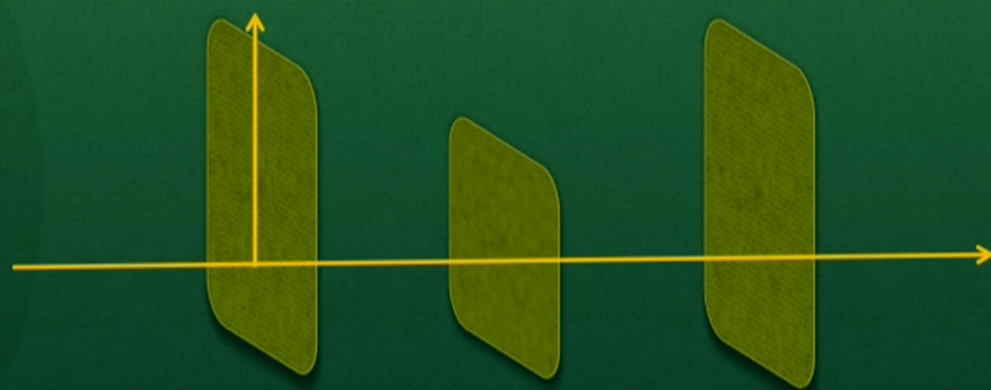
- It is not a qLTC.
- It has a “residual” property of local testability.
- A subset of the logical operators contains numerous copies of the original LTC.
- Any quantum state is a “CAT” state w.r.t. at least one such operator.

Hyper-graph product of the Hadamard code

- It is not a qLTC.
- It has a "residual" property of local testability.
- A subset of the logical operators contains numerous copies of the original LTC.
- Any quantum state is a "CAT" state w.r.t. at least one such operator.
- Measuring this state causes the string to cluster around this super-position.

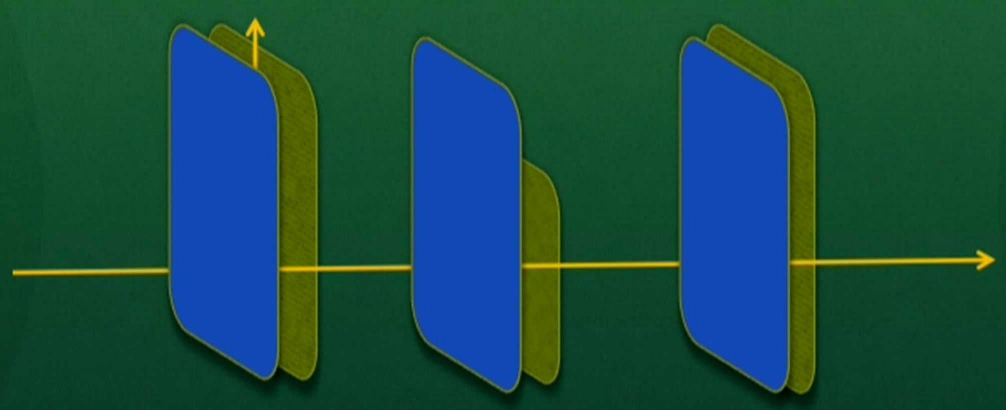
Clustering around affine spaces !

- Live "footage" from F_2^n



Clustering around affine spaces !

- Live "footage" from F_2^n



Final Proof !

- Fix a low-energy quantum state.
- It super-poses nontrivially on some (specially-chosen) affine spaces of the logical space.
- These spaces belong to a (classical) LTC
- Any other string clusters around them.
- Distribution is low-expansion
- So it is hard for bounded-depth circuits.

Results

- There are Hamiltonians with no low-energy trivial states.
- Local Hamiltonians don't have a problem with "rejecting" classical states even at high temperature.
- They need to have an expanding topology.
- Expansion per-se is not enough !
- You need an extra structure. What is it ?
  - Local testability !

Future directions

- Try to find such NLTS Hamiltonians that actually do something useful.
- If you can make it QMA-hard – it's the qPCP conjecture.

Future directions

- Try to find such NLTS Hamiltonians that actually do something useful.
- If you can make it QMA-hard – it's the qPCP conjecture.
- Try to find qLTCs – even with moderate locality.

Future directions

- Try to find such NLTS Hamiltonians that actually do something useful.
- If you can make it QMA-hard – it's the qPCP conjecture.
- Try to find qLTCs – even with moderate locality.
- Compromise on locality of qLTC, but not on the quality of the tester !