Approximate low-weight check codes and circuit lower bounds for noisy ground states

Chinmay Nirkhe (UC Berkeley)
Umesh Vazirani (UC Berkeley)
Henry Yuen (U. Toronto)

arXiv:1802.07419
ICALP 2018, TQC 2018

Berkeley
UNIVERSITY OF CALIFORNIA

Robustness of proofs

How much of a classical proof does one need to read to ensure that it is correct?
For 100% confidence, the whole proof.

This notion was however shattered by the
Probabilistically checkable proofs (PCP) theorem [Arora et. al.98,Dinur07].

It states that if one writes the proof down in a special way, then
for 99% confidence, only a constant number of bits need to be read!

Does a quantum version of the PCP theorem hold?

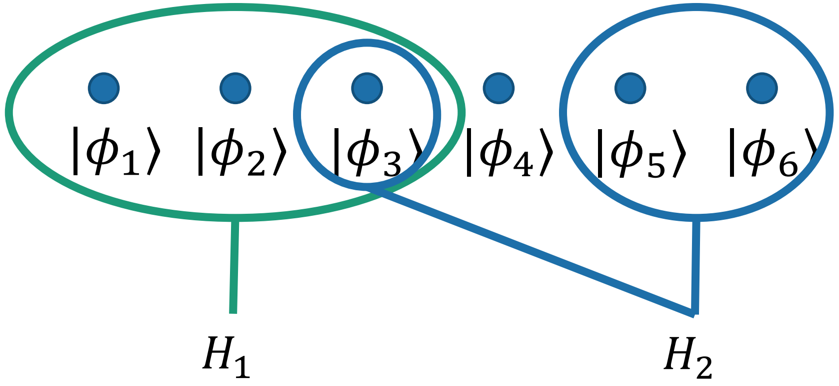
Can quantum computation be done at room- temperature?

Do quantum low-density parity-check codes exist?

These questions may share a common answer!

A quantum perspective on the classical PCP theorem

The Local Hamiltonian Problem



$|\phi_i\rangle \in \mathbb{C}^2$

Each H_j acts non-trivially on only a constant number of terms.

$\|H_j\| \leq 1$

$$H = \frac{1}{m}\sum_{j=1}^{m} H_j$$

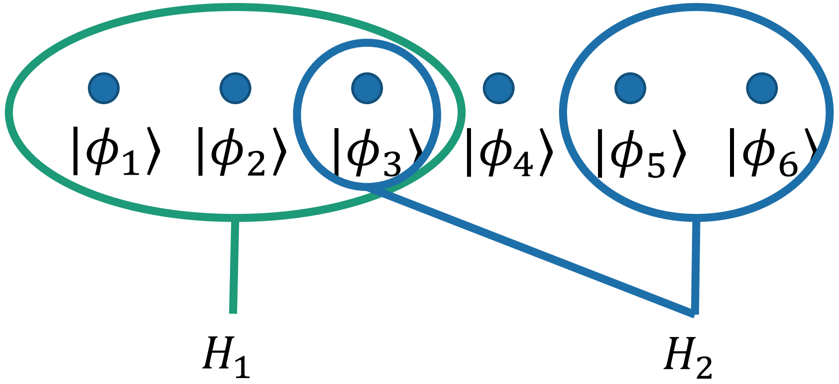
Minimum energy

$$\mathrm{E} = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \langle\phi|H|\phi\rangle = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \frac{1}{m}\sum_{j=1}^{m} \langle\phi|H_j|\phi\rangle$$

Given a local Hamiltonian H, decide if minimum energy $E \leq a$ or $E \geq b$.

A quantum perspective on the classical PCP theorem

Constraint Satisfaction Problems (CSPs)



$|\phi_i\rangle \in \mathbb{C}^2$

Each H_j acts non-trivially on only a constant number of terms.

$\|H_j\| \leq 1$

$$H = \frac{1}{m}\sum_{j=1}^{m} H_j$$

Minimum energy

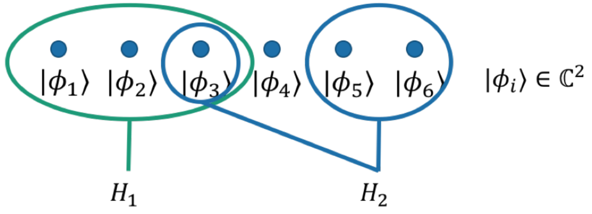
$$\mathrm{E} = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \langle\phi|H|\phi\rangle = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \frac{1}{m}\sum_{j=1}^{m} \langle\phi|H_j|\phi\rangle$$

H_j can be simultaneously expressed as diagonal matrices on the elements they act non-trivially on.

$\Longrightarrow$

The eigenvectors of H are the computational basis.

PCP theorem rephrased



NP-hardness of CSPs [Cook[71],Levin[73]].
It is NP-hard to estimate the energy E of a CSP to $\pm 1/m$.

Minimum energy

$$\mathrm{E} = \inf_{|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}} \frac{1}{m} \sum_{j=1}^{m} \langle \phi | H_j | \phi \rangle$$

PCP theorem [Arora et. al.[98],Dinur[07]].
It is NP-hard to estimate the energy E of a CSP to $\pm 1/4$.

Is there an analogous theorem about the hardness of estimating the energy of a local Hamiltonian problem?

Quantum hardness of LH

LH is QMA-hard [Kitaev99].

It is QMA-hard to estimate the energy of a local Hamiltonian H to $\pm\Omega(1/\mathrm{poly}(m))$.

qPCP conjecture [Aharanov-Naveh02,Aaronson06].

It is QMA-hard to estimate the energy of a local Hamiltonian H to $\pm\Omega(1)$.

$\mathrm{NP} \neq \mathrm{QMA}$

NLTS conjecture [Freedman-Hastings14].

There exist local Hamiltonians H such that $\forall|\xi\rangle$ with $\mathrm{E} = \langle\xi|H|\xi\rangle \leq \lambda_{\min}(H) + \epsilon$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

Complexity of quantum states

Depth of minimum generating circuit

Minimum depth of any circuit C with 2-qubit gates s.t. $|\psi\rangle = C|0\rangle^{\otimes n}$.

Purely quantum notion

Every classical state $x \in \{0,1\}^n$ can be generated by depth 1 circuit: X^x.

If NP $\neq$ QMA,...

Ground-states $|\xi\rangle$ of QMA-hard local Hamiltonians H cannot be generated by constant-depth circuits.

NLTS conjecture [Freedman-Hastings[14]].

There exists local Hamiltonians H such that $\forall|\xi\rangle$ with $\mathrm{E} = \langle\xi|H|\xi\rangle \leq \lambda_{\min}(H) + \epsilon$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

The goal of our paper is to understand more about the robustness of highly-complex entanglement.

1. Notions of robustness of entanglement

2. Approximate error correction
[Not covered in this talk]

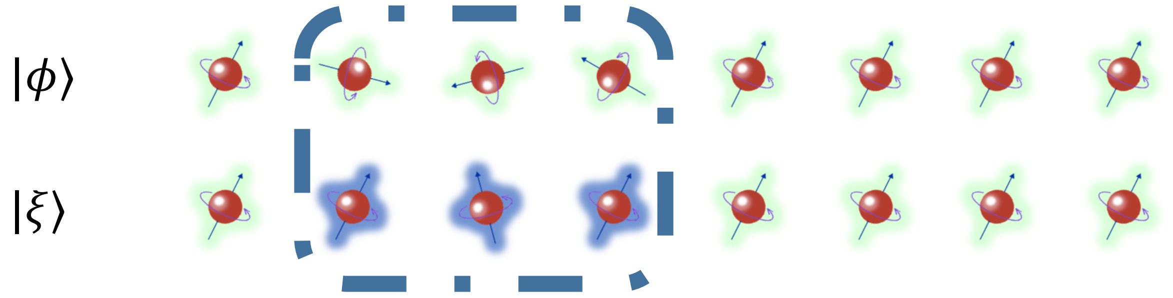
Part 1:
Notions of robustness of entanglement

Are these notions the same?

No low-energy trivial states (NLTS) conjecture [Freedman-Hastings[14]].
There exists local Hamiltonians H such that $\forall |\xi\rangle$ with $E \leq \lambda_{\min}(H) + \epsilon$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

No low-error trivial states (NLETS) theorem [Eldar-Harrow[17]].
There exists Hamiltonians H such that for all ϵ-low-error states $|\xi\rangle$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

Low-error state
A state $|\xi\rangle$ is a ϵ-low-error state for a local Hamiltonian H, if there exists a subset S of size $\leq \epsilon n$ of the particles and a groundstate $|\phi\rangle \in \mathcal{G}$ such that $\mathrm{Tr}_S\,(|\xi\rangle\langle\xi|) = \mathrm{Tr}_S\,(|\phi\rangle\langle\phi|)$.



Intuitively: The "Quantum Hamming Distance" between the two states is small.

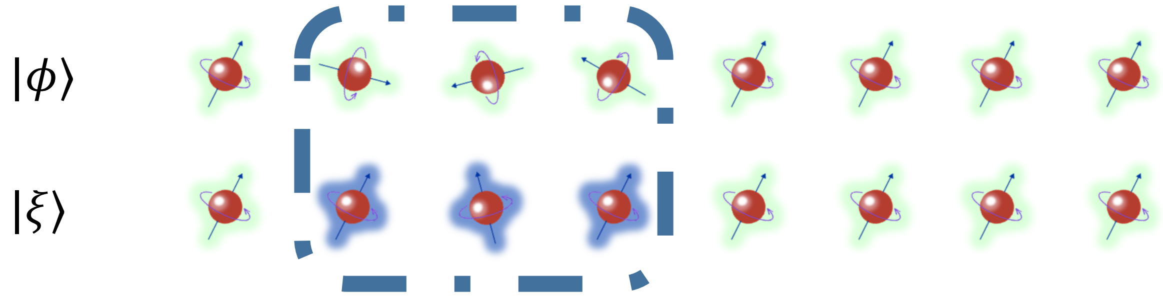
Are these notions the same?

No low-energy trivial states (NLTS) conjecture [Freedman-Hastings[14]].
There exists local Hamiltonians H such that $\forall |\xi\rangle$ with $E \leq \lambda_{\min}(H) + \epsilon$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

No low-error trivial states (NLETS) theorem [Eldar-Harrow[17]].
There exists Hamiltonians H such that for all ϵ-low-error states $|\xi\rangle$, $|\xi\rangle$ cannot be generated by a constant-depth circuit.

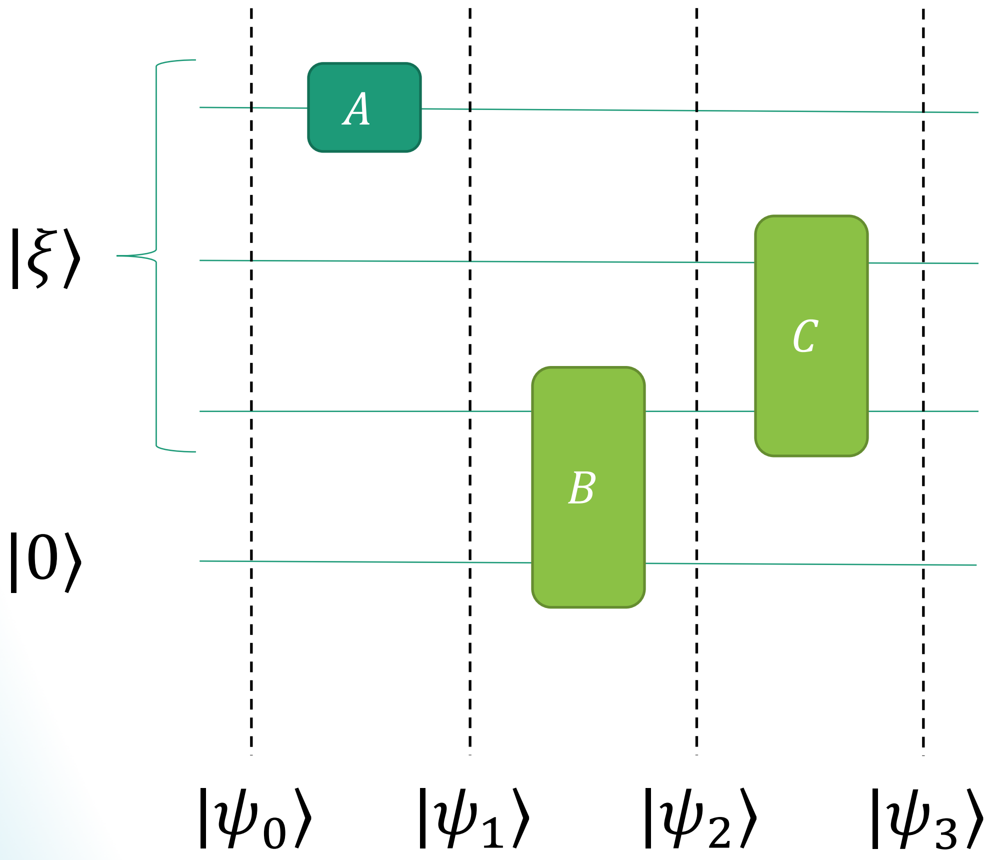
Our contribution [Informal]

A simpler construction of a NLETS Hamiltonian that shows low-error is not the same as low-energy.



Intuitively: The “Quantum Hamming Distance” between the two states is small.

Circuit-to-Hamiltonian construction



$$|\psi_0\rangle = |\xi\rangle|0\rangle$$
$$|\psi_1\rangle = A|\psi_0\rangle$$
$$|\psi_2\rangle = B|\psi_1\rangle$$
$$|\psi_3\rangle = C|\psi_2\rangle$$

Together, $\{|\psi_t\rangle\}$ are a "proof" that the circuit was executed correctly.

But, $|\widetilde{\Psi}\rangle = |\psi_0\rangle|\psi_1\rangle \ldots |\psi_T\rangle$ is not locally-checkable.

Instead, the following "clock" state* is:

$$|\Psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle|\psi_t\rangle$$

*Quantum analog of Cook[71]-Levin[73] Tableau.

Feynman-Kitaev Clock Hamiltonian

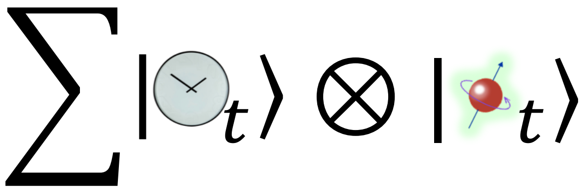
Express a computation as the groundstate of a 5-local Hamiltonian [Kitaev99]

Let $C = C_T C_{T-1} \dots C_1$ be a circuit with gates $\{C_i\}$ and let $|\psi_0\rangle = |\xi\rangle|0\rangle^{\otimes n-k}$ be an initial state for $|\xi\rangle \in (\mathbb{C}^2)^{\otimes k}$.

There is a local Hamiltonian with ground space of:

$$\mathcal{G} = \left\{ |\Psi_\xi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |\mathrm{unary}(t)\rangle \otimes |\psi_t\rangle : \begin{matrix} |\psi_t\rangle = C_t|\psi_{t-1}\rangle, \\ |\psi_0\rangle = |\xi\rangle|0\rangle^{\otimes(n-k)} \end{matrix} \right\}.$$

Used to prove that Local Hamiltonians is QMA-hard [Kitaev99].



Approximate $|🐈\rangle$ state

$$\left|🐈_n\right\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

Error states of cat states have $\Omega(\log n)$ circuit complexity

Let S be a subset of particles of size ϵn. Then,

$$\mathrm{Tr}_S\left(|🐈\rangle\langle🐈|\right) = \frac{|0 \ldots 0\rangle\langle 0 \ldots 0| + |1 \ldots 1\rangle\langle 1 \ldots 1|}{2}.$$

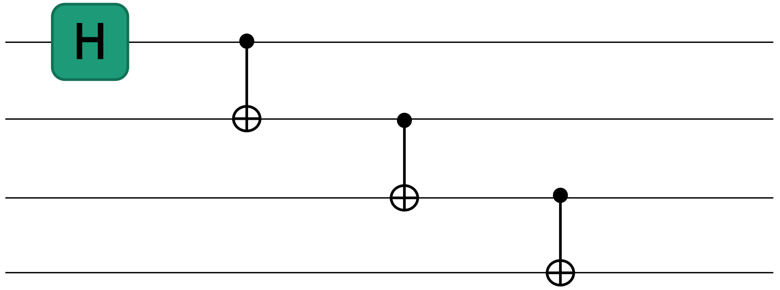
Information theoretic argument shows this state has $\Omega(\log n)$ circuit complexity.

But, cat states are not unique groundstates of local Hamiltonians…

💡 Create a Hamiltonian whose groundspace is almost a cat state. This will preserve the low-error property.

Approximate |🐈⟩ state

$$\left|🐈_n\right\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$



Generate the FK clock Hamiltonian for the circuit generating |🐈⟩. Has unique ground state if we restrict input to $|0\rangle^{\otimes n}$.

$$|\Psi\rangle = \frac{1}{\sqrt{n+1}} \sum_{t=0}^{n} |t\rangle \otimes \left|🐈_t\right\rangle |0\rangle^{\otimes(n-t)}$$

Intuition: For $t \geq \frac{n}{3}$, the first $\frac{n}{3}$ qubits form a cat state. Enough to prove that error states have $\Omega(\log n)$ circuit complexity.

Approximate |🐈⟩ state

$$\left|🐈_n\right\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}$$

NLETS Theorem [N-Vazirani-Yuen[18]]

$\exists$ a family of 3-local Hamiltonians $H^{(n)}$ *on a line*, such that for all $\epsilon < \frac{1}{48}$, the circuit depth of any ϵ-noisy ground state σ of $H^{(n)}$ is at least $\frac{1}{2}\log\left(\frac{n}{2}\right)$.

Superpolynomial Noisy Ground States [N-Vazirani-Yuen[18]]

If QCMA $\neq$ QMA, $\exists$ a family of 7-local Hamiltonians $H^{(n)}$, such that for an $\epsilon > 0$, the circuit depth of any ϵ-noisy ground state σ of $H^{(n)}$ *grows faster than any polynomial of* n.

states have $\Omega(\log n)$ circuit complexity.

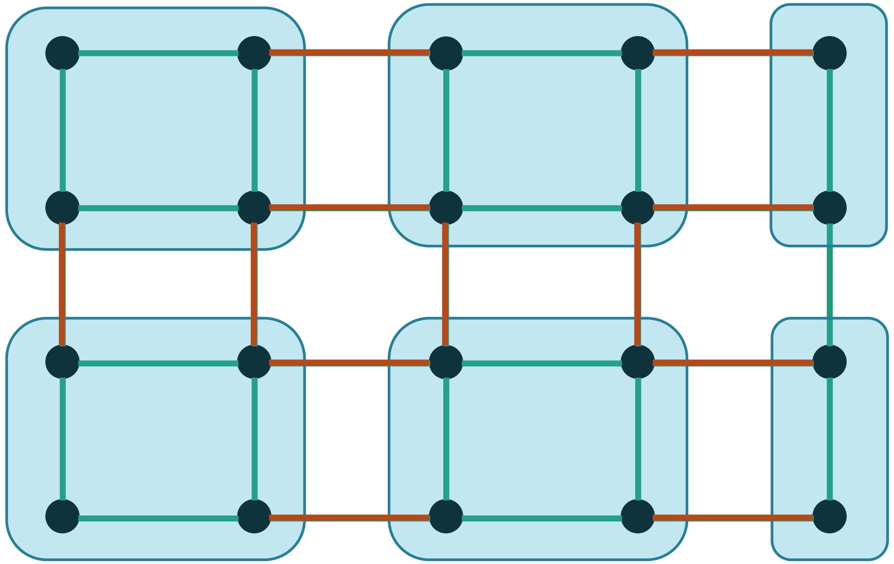
NLETS but not NLTS

With some additional technical details, can make construction 1-D geometrically local.

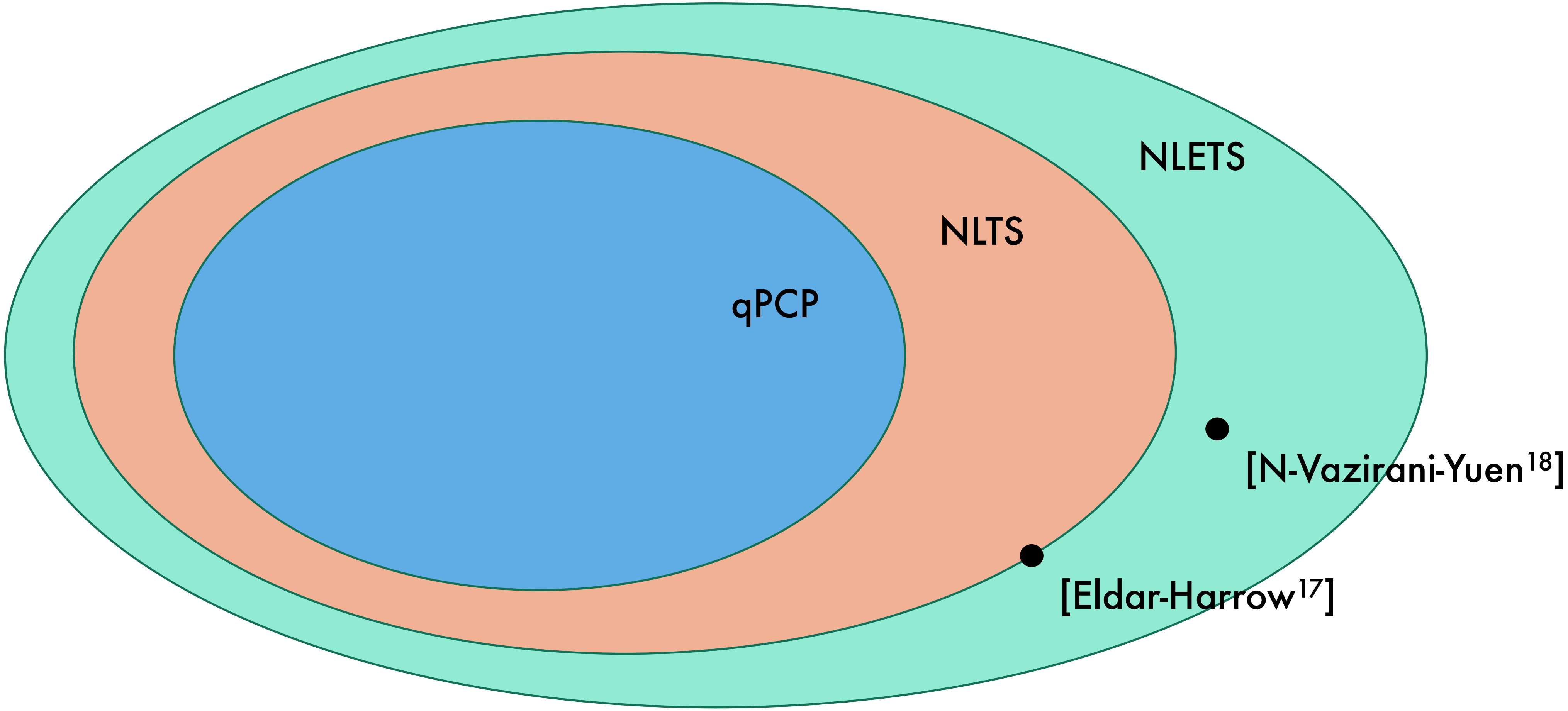
NLTS cannot be geometrically local.

Proof:

Smaller than constant fraction of terms will be violated. Can produce constant-depth states for subsection.



NLETS but not NLTS



Low-energy vs low-error

Low-energy

Correct definition for qPCP
Robustness of entanglement at room-temperature

Low-error

Errors attack specific particles
Reasonable model for physical processes, quantum fault-tolerance, noisy channels, noisy adiabatic quantum computation, etc.

$$\mathcal{M}(\rho) = \left((1-\epsilon)\mathcal{I} + \epsilon\mathcal{N}\right)^{\otimes n}(\rho) \approx \sum_{S:|S|\leq 2\epsilon n} (1-\epsilon)^{n-|S|}\epsilon^{|S|}\mathcal{N}^{S}(\rho)$$

Part 2:
Approximate low-weight check codes

The "conjectured" error-correcting zoo

Quantum low-weight check (qLWC) codes [N-Vazirani-Yuen[18]]

A local Hamiltonian $H = \sum H_j$ is a qLWC if the ground-space $\mathcal{G}$ forms a linear rate and distance code and each Hamiltonian term acts on $O(1)$ particles.

Conjectured: Quantum low-density parity-check codes (qLDPC) [Folklore]

Linear rate and distance codes with $O(1)$ row- and column-spare parity check matrices exist.

Conjectured: Quantum locally testable codes (qLTC) [Aharanov-Eldar[13]]

A local Hamiltonian $H = \sum H_j$ is a qLTC with soundness $R(\delta)$ if a state $|\psi\rangle$ distance δn from the groundspace $\mathcal{G}$ has energy $E = \langle\psi|H|\psi\rangle \geq R(\delta)\, m$.

The "conjectured" error-correcting zoo

Approximate quantum low-weight check (qLWC) codes [N-Vazirani-Yuen[18]]

A local Hamiltonian $H = \sum H_j$ is **an approximate** qLWC if the ground-space $\mathcal{G}$ forms a linear rate and distance code and each Hamiltonian term acts on $O(1)$ particles **and there is an approximate decoding algorithm.**

Conjectured: Quantum low-density parity-check codes (qLDPC) [Folklore]

Linear rate and distance codes with $O(1)$ row- and column-spare parity check matrices exist.

Conjectured: Quantum locally testable codes (qLTC) [Aharanov-Eldar[13]]

A local Hamiltonian $H = \sum H_j$ is a qLTC with soundness $R(\delta)$ if a state $|\psi\rangle$ distance δn from the groundspace $\mathcal{G}$ has energy $E = \langle\psi|H|\psi\rangle \geq R(\delta)\, m$.

Open Questions

- Can approximate qLWC codes be made geometrically local?
- Do super-positions of low-error states requires large circuit complexity? (vs convex combination)
- How do qLWC codes compare to qLTCs, qLDPCs? Do they offer progress towards the qPCP conjecture?
- Combinatorial NLTS vs standard NLTS

Thanks!

Error Correcting Codes

Approximate

A w-local Hamiltonian $H = H_1 + H_2 + \ldots + H_m$ acting on n qubits is a $[[n, k, d]]$ code if

A w-local Hamiltonian $H = H_1 + H_2 + \ldots + H_m$ acting on n qubits is a $[[n, k, d]]$ code with error δ if

1. each term H_i acts on at most w qubits
2. Maps $\mathrm{Enc}, \mathrm{Dec}$ s.t. $\langle\Psi|H|\Psi\rangle = 0$ iff $|\Psi\rangle\langle\Psi| = \mathrm{Enc}(|\xi\rangle\langle\xi|)$ for some $|\xi\rangle \in (\mathbb{C}^2)^{\otimes k}$
3. For all $|\phi\rangle \in (\mathbb{C}^2)^{\otimes k} \otimes \mathcal{R}$ for purify register $\mathcal{R}$, and CPTP error map $\mathcal{E}$ acting on $(d-1)/2$ qubits

$$\mathrm{Dec} \circ \mathcal{E} \circ \mathrm{Enc}(|\phi\rangle\langle\phi|) = |\phi\rangle\langle\phi|$$

$$\|\mathrm{Dec} \circ \mathcal{E} \circ \mathrm{Enc}(|\phi\rangle\langle\phi|) - |\phi\rangle\langle\phi|\| \leq \delta$$

Currently…

Code	Rate	Distance	Locality	Approximation Factor
CSS [Folklore]	$\Omega(n)$	$\Omega(n)$	$\Omega(n)$	0
qLDPC [Tillich-Zémor[13]]	$\Omega(n)$	$O(\sqrt{n})$	$O(1)$	0
Subsystem [Bacon-Flammia-Harrow-Shi[17]]	$\Omega(n)$	$O(n^{1-\epsilon})$	$O(1)$	0
Approx. qLWC [N-Vazirani-Yuen[18]]	$\boldsymbol{\Omega(n)}$	$\boldsymbol{\Omega(n)}$	$\boldsymbol{O(1)}$	$\mathbf{1/poly}(\boldsymbol{n})$