NLTS Hamiltonians from good quantum codes

Anurag Anshu (Harvard)
Niko Breuckmann (Bristol)
Chinmay Nirkhe (IBM Quantum)
Understanding classical proofs
Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).
Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).

0 1 1 0 1 ... 0 1
**Understanding classical proofs**

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).

Local check: $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.

$C_i : \{0,1\}^3 \rightarrow \{0,1\}$.
**Understanding classical proofs**

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).

Local check $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.  

$$C_i : \{0, 1\}^3 \rightarrow \{0, 1\}.$$  

$C : \{0, 1\}^n \rightarrow [0, m]$ by $C(x) = \sum_{i=1}^{m} C_i(x)$.  

$C_{i}$ not necessarily geometrically local.
Understanding classical proofs

NP = the class of all efficiently (poly(n) time) checkable proofs.

NP has complete problems such as Constraint Satisfaction Problems (CSPs).

\[ C_i : \{0, 1\}^3 \rightarrow \{0, 1\} \]

local check \( C_i = x_1 \oplus x_2 \oplus x_3 = 0 \).

C : \{0, 1\}^n \rightarrow [0, m] by \( C(x) = \sum_{i=1}^{m} C_i(x) \)

 Decide if
1. \( \exists x, C(x) = 0 \).
2. \( \forall x, C(x) \geq 1 \).
Two extensions of the notion of proofs

NP \rightarrow \text{GMA}
Two extensions of the notion of proofs

NP \rightarrow \text{GMA}

\text{g. pf. so they require a g. verifier (BGP)}
Two extensions of the notion of proofs

NP \rightarrow \text{QMA}

Calculating ground energy of local Hamiltonians is a complete problem.

q. pf. so they require a q. verifier (BQP)
Two extensions of the notion of proofs

NP

\[ \text{GMA} \]

Calculating ground energy of local Hamiltonians is a complete problem

\[ h_i = \text{linear local operator calculating energy} \]

\[ \cdots 000\rangle\langle 000 | + 111\rangle\langle 111 | \]
Two extensions of the notion of proofs

NP → GMA

Calculating ground energy of local Hamiltonians is a complete problem

\[ h_i = \text{linear local operator calculating energy} \]

\[ H = \sum_{i=1}^{m} h_i \quad |\psi\rangle \rightarrow \langle \psi|H|\psi\rangle \text{ (energy)} \]
Two extensions of the notion of proofs

\[ h_i = \text{linear local operator calculating energy} \]

\[ H = \sum_{i=1}^{m} h_i \]

\[ \langle \psi | H | \psi \rangle \text{ (energy)} \]
Two extensions of the notion of proofs

\[ h_i = \text{linear local operator calculating energy} \]

\[ h_i = 1000\langle 000| + |111\rangle\langle 111| \]

\[ H = \sum_{i=1}^{m} h_i \quad |\psi\rangle \rightarrow \langle \psi|H|\psi\rangle \quad \text{(energy)} \]

ground energy \[ \lambda_{\min}(H) = \min_{|\psi\rangle} \langle \psi|H|\psi\rangle \]
Two extensions of the notion of proofs

\[ h_i = \text{linear local operator calculating energy} \]
\[ h_i = 1000|000\rangle + |111\rangle\langle 111| \]
\[ H = \sum_{i=1}^{m} h_i \]
\[ |\psi\rangle \rightarrow \langle \psi|H|\psi\rangle \text{ (energy)} \]

Ground energy \[ \lambda_{\min}(H) = \min_{|\psi\rangle} \langle \psi|H|\psi\rangle \]

QMA-hard to decide for \[ b - a = 1/\text{poly}(m), \]

1. \[ \lambda_{\min}(H) \leq a \iff \exists |\psi\rangle, \langle \psi|H|\psi\rangle \leq a \]
2. \[ \lambda_{\min}(H) \geq b \iff \forall |\psi\rangle, \langle \psi|H|\psi\rangle \geq b \]
Two extensions of the notion of proofs

QMA-hard to decide for $b-a = 1/\text{poly}(m)$,

1. $\lambda_{\min}(H) \leq a \iff \exists |\psi\rangle, \langle \psi|H|\psi\rangle \leq a$
2. $\lambda_{\min}(H) \geq b \iff \forall |\psi\rangle, \langle \psi|H|\psi\rangle \geq b$
Two extensions of the notion of proofs

QMA-hard to decide for $b-a = 1/ \text{poly}(m)$,

1. $\lambda_{\min}(H) \leq a \iff \exists \psi, \langle \psi | H | \psi \rangle \leq a$
2. $\lambda_{\min}(H) \geq b \iff \forall \psi, \langle \psi | H | \psi \rangle \geq b$

$\Rightarrow$ Groundstates of local Hamiltonians are a “canonical” form for all q. pts.
Two extensions of the notion of proofs

QMA-hard to decide for $b - a = 1 / \text{poly}(m)$,

1. $\lambda_{\min}(H) \leq a \iff \exists |\psi\rangle, \langle \psi | H | \psi \rangle \leq a$

2. $\lambda_{\min}(H) \geq b \iff \forall |\psi\rangle, \langle \psi | H | \psi \rangle \geq b$

$\Rightarrow$ groundstates of local Hamiltonians are a "canonical" form for all q. pfs.

It's widely believed that $NP \neq QMA$
Two extensions of the notion of proofs

QMA-hard to decide for \( b - a = 1 / \text{poly}(m) \),

1. \( \lambda_{\min}(H) \leq a \iff \exists |\psi\rangle, \langle \psi | H | \psi \rangle \leq a \)
2. \( \lambda_{\min}(H) \geq b \iff \forall |\psi\rangle, \langle \psi | H | \psi \rangle \geq b \)

\( \Rightarrow \) groundstates of local Hamiltonians are a "canonical" form for all q. pfs.

It's widely believed that \( \text{NP} \neq \text{QMA} \)

Therefore, not all groundstates of local Hamiltonians can be classically described (in an efficiently verifiable manner).
Two extensions of the notion of proofs

- NP
  - GMA
  - PCPs
Two extensions of the notion of proofs

we think of pfs as requiring step-by-step checking.
Two extensions of the notion of proofs

we think of proofs as requiring step-by-step checking.

PCP theorem: Every NP problem (i.e., every proof) can be converted into a form such that only O(1) bits need to be read to be 99% confident in validity.
Two extensions of the notion of proofs

we think of proofs as requiring step-by-step checking.

PCP theorem Every NP problem (i.e. every proof) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

NP-hard to decide if $[C(x) = \text{analog of } \langle \psi | H | \psi \rangle]$:

1. $\exists x, C(x) = 0$
2. $\forall x, C(x) \geq \frac{m}{2}$ (prev. 1)
Two extensions of the notion of proofs

we think of pf's as requiring step-by-step checking.

PCP theorem: Every NP problem (i.e., every pf) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

NP-hard to decide if

1. $\exists x, C(x) = 0$
2. $\forall x, C(x) \geq \frac{m}{2}$ (prev. 1)

Important consequence: Noisy pf's suffice!
Two extensions of the notion of proofs

we think of proofs as requiring step-by-step checking.

PCP theorem: Every NP problem (i.e., every proof!) can be converted into a form s.t. only $O(1)$ bits need to be read to be 99% confident in validity.

NP-hard to decide if

1. $\exists x, C(x) = 0$
2. $\forall x, C(x) \geq \frac{m}{2}$ (prev. 1)

Important consequence: Noisy proofs suffice!

Any $x$ s.t. $C(x) < \frac{m}{4}$ can be prob. verified with $O(1)$ queries.
The Quantum Prob. Checkable Pfs. Conjecture

NP \{ QMA \rightarrow QPCP_s \}

PCPs
The Quantum Prob. Checkable Probs. Conjecture

Conjecture: Every QMA problem (i.e. quantum pf.) can be converted into a form s.t. only $O(1)$ qubits need to be measured.
The Quantum Prob. Checkable Pfs. Conjecture

Conj. For $\varepsilon > 0$, it's QMA-hard to decide:

1. $\exists |\psi\rangle$ s.t. $\langle \psi | H | \psi \rangle = 0$ (morally)

2. $\forall |\psi\rangle$, $\langle \psi | H | \psi \rangle \geq \varepsilon m$
The Quantum Prob. Checkable Pts. Conjecture

Conj. For $\epsilon > 0$, it's QMA-hard to decide:

1. $\exists |\psi\rangle \text{ s.t. } \langle\psi|H|\psi\rangle = 0 \text{ (morally)}$

2. $\forall |\psi\rangle , \langle\psi|H|\psi\rangle \geq \epsilon m$

Conjecture: Every QMA problem (i.e. quantum pt.) can be converted into a form s.t. only $O(1)$ qubits need to be measured.

Similar to PCP theorem, every state of energy $\leq \frac{\epsilon}{2} m$ is a valid pt. for a QPCP local Hamiltonians.

Set of pts is much larger!
An important consequence of QPCPs

A (if $NP \neq QMA$) quantum pfs. cannot be classically described (in any efficiently checkable manner)

B low energy states of Q2PCP local Hamiltonians are also valid pfs. (since they are noisy pfs.)
An important consequence of QPCPs

A) (if \( \text{NP} \neq \text{QMA} \)) quantum states of QPCPs cannot be classically described (in any efficiently checkable manner)

B) low energy states of QPCPs are also valid local Hamiltonians (since they are noisy pfs.)

\[ \implies \] There exist local Hamiltonians with no succinct classical descriptions for any low-energy state of QPCPs.
An important consequence of QPCPs

A) (if $NP \neq QMA$) quantum local Hamiltonians are also valid pfs. (since they are noisy pfs.)

B) low energy states of Q2PCP ps. cannot be classically described (in any efficiently checkable manner)

$\Rightarrow$ There exist local Hamiltonians with no succinct classical descriptions for any low-energy state

Constant depth q. circuit descriptions are classically checkable pfs for output state
An important consequence of QPCPs

A. (if \(\text{NP} \neq \text{QMA}\)) quantum ps. cannot be classically described in any efficiently checkable manner.

B. Low energy states of Q2CP local Hamiltonians are also valid (since they are noisy ps.)

\[ \Rightarrow \] There exist local Hamiltonians with no succinct classical descriptions for any low-energy state.

Constant depth q. circuit descriptions are classically checkable ps. for output state.

No low energy trivial states. There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit.

[Freedman-Hastings 14]
No low energy trivial states. There exist local Hamiltonians such that no low-energy state is the output of a constant-depth circuit.

[Freedman-Hastings '14]
No low energy trivial states. There exist local Hamiltonians such that no low-energy state is the output of a constant depth circuit. [Freedman-Hastings 14]

- If it was false, then QPCP would have been trivially false.
- Makes a statement about physically realizable robust entanglement.
No low energy trivial states. There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit. [Freedman-Hastings 14]

- If it was false, then QPCP would have been trivially false.
- Makes a statement about physically realizable robust entanglement.

Theorem [Anurag Anshu, Niko Breuckmann, & C.N. ‘22]

Local Hamiltonians corresponding to most* linear-rate and -distance QLDPC error-correcting codes are NLTS Hamiltonians.
No low energy trivial states. There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit.

[Freedman-Hastings 14]

- If it was false, then QPCD would have been trivially false.
- Makes a statement about physically realizable robust entanglement.

Theorem [Anurag Anshu, Niko Breuckmann, & C.N. ‘22]

Local Hamiltonians corresponding to most* linear-rate and -distance QLDPC error-correcting codes are NLTS Hamiltonians. (Includes [leverrier-Zémor] construction).
No low energy trivial states. There exist local Hams. s.t. no low-energy state is the output of a constant depth circuit. [Freedman-Hastings 14]

- If it was false, then QPCP would have been trivially false.
- Makes a statement about physically realizable robust entanglement.

Theorem [Anurag Anshu, Niko Breuckmann, & C.N. '22]

Local Hamiltonians corresponding to most* linear-rate and -distance QLDPC error-correcting codes are NLTS Hamiltonians. (includes [Leverrier-Zémor] construction).

∃ ε > 0, and Hamiltonian family $H$ s.t. every state $ψ$ of energy $≤ εN$, the minimum depth circuit to generate $ψ$ is $Ω(\log n)$. 
Proof sketch of the NLTS theorem

1. Trivial states $\Rightarrow$ Local Hamiltonians $\Rightarrow$ Circuit depth lower bounds

Light cones for low depth circuits
Proof sketch of the NLTST theorem

1. Trivial states $\Rightarrow$ Local Hamiltonians
   $\Rightarrow$ Circuit depth lower bounds
   Lightcone for low depth circuits

2. Error Correction Codes (ECC)
   Low energy subspace of expanding codes.
Proof sketch of the NLTS theorem

1. Trivial states $\Rightarrow$ Local Hamiltonians $\Rightarrow$ Circuit depth lower bounds
   
   - Lightcombs for low depth circuits

2. Error Correction Codes (ECC)
   - Low energy subspace of expanding codes

3. Erasure errors for quantum codes
Proof sketch of the NLTS theorem

1. Trivial states $\Rightarrow$ Local Hamiltonians $\Rightarrow$ Circuit depth lower bounds

Lightcombs for low depth circuits

Error Correction Codes (ECC)

2. Low energy subspace of expanding codes

3. Erasure errors for quantum codes
Lightcones and quantum circuits
Lightcones and quantum circuits

Low-depth states are classical witnesses for energy
Lightcones and quantum circuits

If $A$ is a local operator and $U$ is a q. circuit of depth $t$, then $U^*AU$ is a $\leq 2^t \cdot |A|$ local operator.

Low-depth states are classical witnesses for energy.
Lightcones and quantum circuits

If $A$ is a local operator and $U$ is a q. circuit of depth $t$, then $U^\dagger AU$ is a $\leq 2^t \cdot |A|$ local operator.

Low-depth states are classical witnesses for energy.
Lightcones and quantum circuits

If $A$ is a local operator and $U$ is a $q$ circuit of depth $t$, then $U^t A U$ is a $\leq 2^t \cdot |A|$ local operator.

Low-depth states are classical witnesses for energy.
Lightcones and quantum circuits

If \( A \) is a local operator and \( \mathcal{U} \) is a q circuit of depth \( t \), then \( \mathcal{U}^\dagger A \mathcal{U} \) is a \( \leq 2^t \cdot |A| \) local operator.

Given a local Hamiltonian \( H = \sum_i h_i \) and a state \( |\psi\rangle = \mathcal{U}|0^n\rangle \), we can evaluate \( \langle \psi | H | \psi \rangle \) in classical time \( 2^{2t} \cdot \text{poly}(n) = \text{poly}(n) \) when \( t = O(1) \).

Low-depth states are classical witnesses for energy.
Lightcones and quantum circuits

If $A$ is a local operator and $U$ is a $q$ circuit of depth $t$, then $U^t A U$ is a $\leq 2^t |A|$ local operator.

Given a local Hamiltonian $H = \sum_i h_i$ and a state $|\psi\rangle = U |0^n\rangle$, we can evaluate $\langle \psi | H | \psi \rangle$ in classical time $2^{2t} \cdot \text{poly}(n) = \text{poly}(n)$ when $t = O(1)$.

$$\langle \psi | H | \psi \rangle = \sum_i \langle \psi | h_i | \psi \rangle = \sum_i \langle 0^n | U^t h_i U | 0^n \rangle$$
Lightcones and quantum circuits

If $A$ is a local operator and $U$ is a q circuit of depth $t$, then $U^\dagger A U$ is a $\leq 2^t \cdot |A|$ local operator.

Given a local Hamiltonian $H = \sum_i^m h_i$ and a state $|\psi\rangle = U|0^n\rangle$, we can evaluate $\langle \psi | H | \psi \rangle$ in classical time $2^{2t} \cdot \text{poly}(n) = \text{poly}(n)$ when $t = O(1)$.

$$\langle \psi | H | \psi \rangle = \sum_i^m \langle \psi | h_i | \psi \rangle$$

$$= \sum_i^m \langle 0^n | U^{\dagger} h_i U | 0^n \rangle$$

computation on $O(2^t)$ qubits
Lightcones and quantum circuits

If $A$ is a local operator and $U$ is a q. circuit of depth $t$, then $U^t A U$ is a $\leq 2^t |A|$ local operator.

Given a local Hamiltonian $H = \sum_i^m h_i$ and a state $|\psi\rangle = U |0^n\rangle$, we can evaluate $\langle \psi | H | \psi \rangle$ in classical time $2^{2t} \cdot \text{poly}(n) = \text{poly}(n)$ when $t = O(1)$.

$$\langle \psi | H | \psi \rangle = \sum_i^m \langle \psi | h_i | \psi \rangle = \sum_i^m \langle o^n | U^\dagger h_i U | o^n \rangle$$

Low-depth states are classical witnesses for energy computation on $O(2^t)$ qubits.
Trivial states $\Rightarrow$ Local Hamiltonians

The state $|0^n\rangle$ is the unique solution to a very simple local Hamiltonian.
Trivial states $\Rightarrow$ Local Hamiltonians

The state $|0^n\rangle$ is the unique solution to a very simple local Hamiltonian.

$$H_0 = \sum_{i=1}^{n'} |1angle\langle 1| \iff \text{qubit-wise projectors enforcing qubits equal } |0\rangle.$$
The state $|10^{n'}\rangle$ is the unique solution to a very simple local Hamiltonian.

$$H_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i \iff \text{qubit-wise projectors enforcing qubits equal } 10\rangle.$$  

$H_0$ is commuting and has a spectrum of $0, 1, 2, \ldots, n'$, with eigenvectors $|x\rangle$ of eigenvalue $|x\rangle$.  

**Trivial states $\Rightarrow$ Local Hamiltonians**
Trivial states $\Rightarrow$ Local Hamiltonians

The state $|0^n\rangle$ is the unique solution to a very simple local Hamiltonian.

$$H_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i \iff \text{qubit-wise projectors enforcing qubits equal } 10\rangle.$$  

$H_0$ is commuting and has a spectrum of $0, 1, 2, \ldots, n'$, with eigenvectors $|x\rangle$ of eigenvalue $|x\rangle$.

Let $H_u = U^\dagger H U$ for depth $t$ circuit $U$.  

Trivial states $\Rightarrow$ Local Hamiltonians

The state $|0^n\rangle$ is the unique solution to a very simple local Hamiltonian.

$$H_0 = \sum_{i=1}^{n'} |1\rangle\langle 1|_i \Leftarrow \text{qubit-wire projectors enforcing qubits equal } 10\rangle.$$

$H_0$ is commuting and has a spectrum of $0, 1, 2, \ldots, n'$, with eigenvectors $|x\rangle$ of eigenvalue $|x\rangle$.

Let $H_U = U^\dagger H U$ for depth $t$ circuit $U$.

$H_U$ is commuting and has a spectrum of $0, 1, 2, \ldots, n'$, with eigenvectors $U|x\rangle$ of eigenvalue $|x\rangle$.

And $H_U$ is a $2^t$-local Hamiltonian.
Local indistinguishability

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

\[ \Psi_s = \Psi'_s. \]
**Local indistinguishability**

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$, 

$$\Psi_S = \Psi'_S.$$ 

Ex. The states 

$$|\text{Q}{\pm}\rangle = \frac{10^n\rangle \pm |1^n\rangle}{\sqrt{2}}$$ 

are $(n-1)$ locally indistinguishable.
Local indistinguishability

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

$$|\Psi_S - \Psi'_S| = 0.$$ 

Ex. The states $|\psi_{\pm}\rangle = \frac{|0^n\rangle \pm |1^n\rangle}{\sqrt{2}}$ are $(n-1)$ locally indistinguishable.

Any strict reduced density matrix equals

$$|\psi_{\pm}\rangle_S = \frac{|0\times0|^{n-151} + |1\times1|^{n-151}}{2}.$$
Local indistinguishability

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

$$\Psi_{-S} = \Psi'_{-S}.$$
Local indistinguishability $\Rightarrow$ Ckt depth lower bounds

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$, $\Psi_S = \Psi'_S$. 

$\Psi_S$ and $\Psi'_S$ are the restrictions of $\Psi$ and $\Psi'$ to region $S$. 

This means that for any region $S$ that is $d$-local, the states are indistinguishable in that region.
Local indistinguishability $\Rightarrow$ Ckt depth lower bounds

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

$$|\Psi_S\rangle = |\Psi'_S\rangle.$$ 

Lemma (if $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable, then if $|\Psi\rangle = U|0^n\rangle$ for $U$ of depth $t$, then $2^t \geq d$. $\Rightarrow$ $t \geq \log d$.}
**Local indistinguishability** ⇒ Ckt depth lower bounds

Two states $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

$$\Psi_S = \Psi'_S.$$

**Lemma** (if $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable, then if $|\Psi\rangle = U|0^n\rangle$ for $U$ of depth $t$, then $2^t \geq d$. ⇒ $t \geq \log d$)

**Pt.**

$$\langle \Psi' | H_U | \Psi \rangle = \sum_i \langle \Psi' | h_i | \Psi \rangle = \sum_i \langle \Psi | h_i | \Psi \rangle$$

*since $H_U$ is $2^t$-local and are $d > 2^t$ locally indistinguishable*
Local indistinguishability $\Rightarrow$ Ckt depth lower bounds

Two states $|\psi\rangle$ and $|\psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

$$\psi_{-S} = \psi'_{-S}.$$

Lemma 4. If $|\psi\rangle$ and $|\psi'\rangle$ are $d$-locally indistinguishable, then if $|\psi\rangle = \mathbf{U}|0^n\rangle$ for $\mathbf{U}$ of depth $t$, then $2^t \geq d$. $\Rightarrow$ $t \geq \log d$.

Proof. $\langle \psi' | H_\mathbf{U} | \psi \rangle = \sum_i \langle \psi' | h_i | \psi \rangle$. Since $H_\mathbf{U}$ is $2^t$-local and are $d > 2^t$ locally indistinguishable,

$$= \sum_i \langle \psi | h_i | \psi \rangle = \langle \psi | H_\mathbf{U} | \psi \rangle = 0.$$
Local indistinguishability $\Rightarrow$ Ckt depth lower bounds

Two states $|\psi\rangle$ and $|\psi'\rangle$ are $d$-locally indistinguishable if for every region $S$ of size $\leq d$,

$\psi_{-S} = \psi'_{-S}$.

Lemma: If $|\psi\rangle$ and $|\psi'\rangle$ are $d$-locally indistinguishable, then if $|\psi\rangle = U|0^n\rangle$ for $U$ of depth $t$, then $2^t \geq d. \Rightarrow t \geq \log d$.

Proof.

$\langle \psi' | H_U | \psi \rangle = \sum_i \langle \psi' | h_i | \psi \rangle$ since $H_U$ is $2^t$-local and are $d > 2^t$ locally indistinguishable

$= \sum_i \langle \psi | h_i | \psi \rangle = \langle \psi | H_U | \psi \rangle = 0$

But groundstate $|\psi\rangle$ is unique! $\Rightarrow |\psi\rangle = |\psi'\rangle$, a contradiction!
Local indistinguishability

Lemma: If $|\Psi\rangle$ and $|\Psi'\rangle$ are $d$-locally indistinguishable, then if $|\Psi\rangle = U|0^n\rangle$ for $U$ of depth $t$, then $2^t \geq d$. \[ t \geq \log d. \]
Local indistinguishability

Lemma. If $|\psi\rangle$ and $|\psi'\rangle$ are $d$-locally indistinguishable, then if

$$|\psi\rangle = U|0^n\rangle$$

for $U$ of depth $t$, then $2^t \geq d$. \Rightarrow \boxed{t \geq \log d}$

Since, spectral gap of $H_U$ is 1, this argument is only robust to perturbations of $O(\frac{1}{n})$. 
Local indistinguishability

Lemma (14) and $|\Psi\rangle$ are $d$-locally indistinguishable, then if $|\Psi\rangle = U|0^n\rangle$ for $U$ of depth $t$, then $2^t \geq d$. $\Rightarrow t \geq \log d$.

Since, spectral gap of $H_U$ is 1, this argument is only robust to perturbations of $O(\frac{1}{n})$.

Using mathematics from Chebyshev polynomials, we can make l.b. robust.
Robust local indistinguishability
Robust local indistinguishability

\[ \Pi \overset{\text{def}}{=} \Pi - \frac{H_u}{n} \]
Robust local indistinguishability

\[ \Pi \overset{\text{def}}{=} \mathcal{I} - \frac{H_u}{n} \quad \Rightarrow \quad \| \Pi - |\psi\rangle \langle \psi| \|_\infty \leq 1 - \frac{1}{n} \]

a weak approximate projector.
Robust local indistinguishability

\[ T \triangleq I - \frac{H_n}{n} \implies \| T - |\psi\rangle\langle \psi| \|_\infty \leq 1 - \frac{1}{n} \]  

and a weak approximate projector.

\[ \exists \ p: \mathbb{R} \to \mathbb{R} \text{ of deg } O_n(\sqrt{n}) \text{ s.t. } \| p(H_n) - |\psi\rangle\langle \psi| \|_\infty \leq \mu \]
Robust local indistinguishability

$$\Pi \equiv \mathbb{I} - \frac{H_u}{n} \quad \Rightarrow \quad \| \Pi - |\psi\rangle\langle\psi| \|_\infty \leq 1 - \frac{1}{n}$$

a weak approximate projector.

\(\exists \ p : \mathbb{R} \to [0,1] \text{ of deg } O(\sqrt{n}) \text{ s.t. } \| p(H_u) - |\psi\rangle\langle\psi| \|_\infty \leq \mu \)

1-\(p\) is the Chebyshev poly. approx. of the OR function.

\(p(0) = 1, \ |p(\frac{i}{n})| \leq \mu \)
Robust local indistinguishability

\[ T \equiv \mathbb{I} - \frac{H_u}{n} \quad \Rightarrow \quad \| T - \psi \psi \|_\infty \leq 1 - \frac{1}{n} \]

\[ \exists \ p : \mathbb{R} \rightarrow \mathbb{R} \text{ of deg } O(\sqrt{n}) \text{ s.t. } \| p(H_u) - \psi \psi \|_\infty \leq \mu \]

1 - p is the Chebyshev poly. approx. of the OR function.

\[ p(0) = 1, |p(\frac{i}{n})| \leq \mu \]

\[ p(H_u) \text{ is a local Hamiltonian of } \mathcal{O}(2^t \sqrt{n}) \text{ locality} \]

\[ H_u \]
Robust local indistinguishability

\[ p(H_u) \] is a \( L := O(2^t \cdot \sqrt{n}) \)
local Ham. s.t.
\[ \| p(H_u) - |\psi \rangle \langle \psi| \|_\infty \leq \mu. \]
Robust local indistinguishability

Let $\mathcal{D}$ be the dist. on $\{0, 1\}^n$ formed by measuring $|\psi\rangle$.
Robust local indistinguishability

Let $D$ be the dist. on $\{0,1\}^n$ formed by measuring $|\Psi\rangle$.

Assume $D(S_1) > \mu$ & $D(S_2) > \mu$.

$p(H_u)$ is a $L = O(2^t \sqrt{n})$ local Ham. s.t.

$\| p(H_u) - |\psi\rangle \langle \psi | \|_\infty \leq \mu.$
Robust local indistinguishability

Let $D$ be the dist. on $\{0,1\}^n$ formed by measuring $|\psi\rangle$.

$p(H_u)$ is a $L := O(2^t \cdot \sqrt{n})$ local Ham. s.t.

$$\| P(H_u) - |\psi\rangle\langle\psi| \|_\infty \leq \mu.$$

Assume $D(S_1) > \mu$ & $D(S_2) > \mu$

Let $T{T}_{S_1}, T{T}_{S_2}$ be proj. onto the sets $S_1$ & $S_2$, respectively.
Robust local indistinguishability

Let $D$ be the dist. on $\{0,1\}^n$ formed by measuring $|\Psi\rangle$.

Assume $D(S_1) > \mu$ & $D(S_2) > \mu$

Let $T_{S_1}$ & $T_{S_2}$ be proj. onto the sets $S_1$ & $S_2$, respectively

$$\| T_{S_1} |\Psi\rangle \langle \Psi | T_{S_2} \|_\infty > \mu$$
Robust local indistinguishability

Let $D$ be the dist. on $\{0,1\}^n$ formed by measuring $|\Psi\rangle$.

Assume $D(S_1) > \mu$ & $D(S_2) > \mu$

Let $\Pi_{S_1}$, $\Pi_{S_2}$ be proj. onto the sets $S_1$ & $S_2$, respectively

$\|\Pi_{S_1}|\psi\rangle\langle\psi| \Pi_{S_2}\|_\infty > \mu$

$p(H_u)$ is a $L := O(2^t \sqrt{n})$

local Ham. s.t.

$\|p(H_u) - |\psi\rangle\langle\psi|\|_\infty \leq \mu.$
Robust local indistinguishability

Let $\mathcal{D}$ be the dist. on $\{0,1\}^n$ formed by measuring $|\Psi\rangle$. Assume $\mathcal{D}(S_1) > \mu$ & $\mathcal{D}(S_2) > \mu$

Let $\Pi_{S_1}, \Pi_{S_2}$ be proj. onto the sets $S_1$ & $S_2$, respectively

$\| \Pi_{S_1} |\Psi\rangle \langle \Psi| \Pi_{S_2} \|_\infty > \mu$

$\| \Pi_{S_1} p(H_u) \Pi_{S_2} \|_\infty = 0$

due to locality of $p(H_u)$ being small.

$p(H_u)$ is a $L := O(2^t \sqrt{n})$
local Ham. s.t.

$\| p(H_u) - |\Psi\rangle \langle \Psi| \|_\infty \leq \mu.$
Robust local indistinguishability

**Thm** Any dist. $D$ s.t. $D(S_1), D(S_2) > \mu$
cannot be generated by a quantum circuit
of depth $\leq \Omega(\log(\frac{L^2 \mu}{n}))$. 
Robust local indistinguishability

Thm Any dist. $D$ s.t. $D(S_1), D(S_2) > \mu$
cannot be generated by a quantum circuit
of depth $\leq \Omega(\log(\frac{L^2 \mu}{n}))$.

Cor. Any state $|\psi\rangle$ whose measurement dist is $D$
also has the same lower bound.
Robust local indistinguishability

Thm: Any dist. $D$ s.t. $D(S_1), D(S_2) > \mu$ cannot be generated by a quantum circuit of depth $\leq \Omega(\log(\frac{L^2 \mu}{n}))$.

Cor: Any state $|\psi\rangle$ whose measurement dist is $D$ also has the same lower bound.

If $L \geq \omega(\sqrt{n})$ and $\mu \geq \Omega(1)$, call $D$ a "well-spread" dist. well-spread dist. is a signature of quantum depth.
Proof sketch of the NLTS theorem

1. Trivial states $\Rightarrow$ Local Hamiltonians $\Rightarrow$ Circuit depth lower bounds

Lightcones for low depth circuits

2. Error Correction Codes (ECC)

Low energy subspace of expanding codes

3. Erasure errors for quantum codes
Expanding codes & Tanner codes

A linear code \( \mathcal{C} \subseteq \mathbb{F}_q^n \) can be expressed as \( \ker H \) for \( H \in \mathbb{F}_2^{m \times n} \).
Expanding codes & Tanner codes

\[
\begin{pmatrix}
H
\end{pmatrix}
\begin{pmatrix}
x
\end{pmatrix}
= \begin{pmatrix}
0
\end{pmatrix}
\]

A linear code \( \mathbb{F}_2^n \) can be expressed as \( \ker H \) for \( H \in \mathbb{F}_2^{m \times n} \).
Expanding codes & Tanner codes

\[ \left( \begin{array}{c} H \\ x \end{array} \right) = \left( \begin{array}{c} 0 \end{array} \right) \]

A linear code \( \subseteq \{0,1\}^n \) can be expressed as \( \ker H \) for \( H \in \mathbb{F}_2^{m \times n} \).

\( \{0,1\}^n \)

\( \mathcal{M}(n) \)

\( \bullet = \) code words
Expanding codes & Tanner codes

A linear code $\mathbb{C} \subseteq \{0,1\}^n$ can be expressed as $\ker H$ for $H \in \mathbb{F}_2^{m \times n}$

when $H$ is adj. matrix of

small-set expanding bipartite graph

$= \text{states that violate } \leq \text{ EM checks}$

$= \text{Codenwords}$
Expanding codes & Tanner codes

A linear code \( \mathbb{F}_2^n \) can be expressed as ker \( H \) for \( H \in \mathbb{F}_2^{m \times n} \) when \( H \) is adj. matrix of small-set expanding bipartite graph. The low-energy space of a code is a great support for a distribution that we hope to prove is well-spread.

\[
\begin{pmatrix}
H \\
\end{pmatrix}
\begin{pmatrix}
x \\
\end{pmatrix}
= \begin{pmatrix}
0 \\
\end{pmatrix}
\]

\( \{0,1\}^n \)

\( \bullet \) = code words  
\( \bullet \) = states that violate \( \leq \) EM checks  
\( \bullet \) = code words
Expanding codes & Tanner codes

A linear code \( \mathbb{F}_2^n \) can be expressed as \( \ker H \) for \( H \in \mathbb{F}_2^{m \times n} \) when \( H \) is adj. matrix of small-set expanding bipartite graph.

The low-energy space of a code is a great support for a distribution that we hope to prove is well-spread.

Only question is how to construct Hamiltonian with such property?
Proof sketch of the NLTS theorem

1. Trivial states $\rightarrow$ Local Hamiltonians $\rightarrow$ Circuit depth lower bounds

2. Error Correction Codes (ECC) $\rightarrow$ low energy subspace of expanding codes

3. Light cones for low depth circuits

Erasure errors for quantum codes
Quantum error correcting codes

Consider a state subject to an erasure error.
Quantum error correcting codes

Consider a state subject to an erasure error.
Consider a state subject to an erasure error.
Quantum error correcting codes

Consider a state subject to an erasure error.

If we could recover the original state then unless contains no information about the original state, this violates the no-cloning theorem.
Quantum error correcting codes

Consider a state subject to an erasure error.

If we could recover the original state then unless \( R \) contains no information about the original state, this violates the no-cloning theorem.

Erasure error-correction implies local indistinguishability for codes.
Quantum error correcting codes

Erasure error-correction implies local indistinguishability for codes.
Quantum error correcting codes

Erasure error-correction implies local indistinguishability for codes.

Exact codewords of codes of distance $d$ require circuits of depth $\Omega(\log d)$ to generate.
Quantum error correcting codes

Erasure error-correction implies local indistinguishability for codes.

Exact codewords of codes of distance $d$ require circuits of depth $\Omega(\log d)$ to generate.

Error-correcting codes that are LDPC naturally have a local Hamiltonian, one that applies every local check.
Quantum error correcting codes

Erasure error-correction implies local indistinguishability for codes.

Exact codewords of codes of distance $d$ require circuits of depth $\Omega(\log d)$ to generate.

Error-correcting codes that are LDPC naturally have a local Hamiltonian, one that applies every local check.

How do we prove circuit depth lower bounds for the low-energy subspace of these code Hamiltonians?
Optimal-parameter CSS codes

There is a class of q. codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.
Optimal-parameter CSS codes

There is a class of q. codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.

They are constructed from two classical codes $C_x, C_z$ (w. check-matrix $H_x, H_z$) s.t. $C_x^\perp \leq C_z$ (equiv. $C_z^\perp \leq C_x$).
Optimal-parameter CSS codes

There is a class of codes called Calderbank-Shor-Steane codes that correct for X-type (bit-flip) and Z-type (phase-flip) errors separately.

They are constructed from two classical codes \( C_x, C_z \) (w. check-matrix \( H_x, H_z \)) s.t. \( C_x^\perp \leq C_z \) (equiv. \( C_z^\perp \leq C_x \)).

\[
d_z = \min_{w \in C_z^\perp} |w|_{C_x^\perp}, \quad d_x = \min_{w \in C_x} |w|_{C_z^\perp}
\]

where \( |w|_S = \min_{w' \in S} |w + w'| \).

\[\{0,1\}^n\]

cluster of \( C_z \) related by adding \( C_x^\perp \).
Optimal-parameter CSS codes

There is a class of $q$ codes called Calderbank-Shor-Steane codes that correct for $X$-type (bit-flip) and $Z$-type (phase-flip) errors separately.

They are constructed from two classical codes $C_x, C_z$ (w. check-matrix $H_x, H_z$) s.t. $C_x^\perp \leq C_z$ (equiv. $C_z^\perp \leq C_x$).

\[ d_z = \min_{w \in C_z^\perp} |w|_{C_x^\perp}, \quad d_x = \min_{w \in C_z^\perp} |w|_{C_z^\perp} \]

where $|w|_S = \min_{w' \in S} |w + w'|$.

\[ d = \min \{ d_x, d_z \} \]

$\square$ = codewords of $C_z$. $\{0,1\}^n$

Cluster of $C_z$ related by adding $C_x^\perp$. 
Expanding CSS codes

Similar to classical example, we consider codes that have the property that if $|H_2 y| \leq 3m$ then either

1. $|y|_{c_x^+} \leq c_1 \epsilon n$ or
2. $|y|_{c_x^+} \geq c_2 n$.
Expanding CSS codes

Similar to classical example, we consider codes that have the property that if $|H_2 y| \leq \varepsilon m$ then either

1. $|y|_{c_x^+} \leq c_1 \varepsilon n$ or
2. $|y|_{c_x^-} \geq c_2 n$.

And, if we consider a $\frac{\varepsilon}{200}$-low-energy state of the code's local Hamiltonian, measuring in the $Z$-basis yields a dist. $99.5\%$ supported on $[0,1]^n$. 
The uncertainty principle

\[\{0,1\}^n\]
The uncertainty principle
The uncertainty principle

All that remains to show is that the distribution is not 99% concentrated on any cluster.
The uncertainty principle

All that remains to show is that the distribution is not 99% concentrated on any 1 cluster, ⇒ dist. is well-spread (μ = \frac{1}{400})
The uncertainty principle

All that remains to show is that the distribution is not 99\% concentrated on any 1 cluster. \( \Rightarrow \) dist. is well-spread \( (\mu = \frac{1}{400}) \)

\( \Rightarrow \) circuit depth lower bound.
The uncertainty principle

All that remains to show is that the distribution is not 99\% concentrated on any 1 cluster. \( \Rightarrow \) dist. is well-spread \( (\mu = \frac{1}{400}) \)

\( \Rightarrow \) circuit depth lower bound.

Uncertainty principle: For sets \( S, T \subseteq \{0,1\}^n \), any state \( \psi \) with dists. \( D_x, D_z \)

\[
D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{ \frac{|S| \cdot |T|}{2^n} }
\]
The uncertainty principle

All that remains to show is that the distribution is not 99% concentrated on any 1 cluster. \( \Rightarrow \) dist. is well-spread (\( \mu = \frac{1}{400} \))

\( \Rightarrow \) circuit depth lower bound.

Uncertainty principle: For sets \( \mathcal{S}, \mathcal{T} \subseteq \{0,1\}^n \), any state \( \psi \) with dists. \( D_x, D_z \)

\[
D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}
\]

Assume \( D_z \) is 99% concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \), \( D_x(T) < 0.99 \) \( \Rightarrow \) Either \( D_x \) or \( D_z \) is well-spread.
Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state $\Psi$ with dists. $D_x, D_z$

$$D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume $D_z$ is 29.99% concentrated on some Z-cluster $S$. Then for any X-cluster $T$, $D_x(T) < 0.99 \Rightarrow$ Either $D_x$ or $D_z$ is well-spread.
The uncertainty principle

\[ |S| \leq \left( \frac{n}{0(n)} \right) \cdot 2^r \]

Assume \( D_2 \) is 99.9% concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \), \( D_x(T) < 0.99 \Rightarrow \) Either \( D_x \) or \( D_2 \) is well-spread.
The uncertainty principle

\[ |S| \leq \binom{n}{(0, n)}, \quad 2^x \leq 2^x + O(\sqrt{2^n}) \]

Assume \( D_2 \) is 0.99% concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \), \( D_x(T) < 0.99 \) \( \Rightarrow \) Either \( D_x \) or \( D_2 \) is well-spread.
Uncertainty principle: For sets $S, T \subseteq \{0,1\}^n$, any state $\psi$ with dists. $D_x, D_z$

$$D_x(T) \leq 2 \sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}}$$

Assume $D_z$ is $99\%$ concentrated on some $Z$-cluster $S$. Then for any $X$-cluster $T$, $D_x(T) < 0.99 \Rightarrow$ Either $D_x$ or $D_z$ is well-spread.
The uncertainty principle

\[ |S| \leq \binom{n}{0(n^2)} \cdot 2^r \leq 2^r + O(\sqrt{\epsilon} n) \]

\( |T| \leq 2^r + O(\sqrt{\epsilon} n) \)

Uncertainty principle: For sets \( S, T \subseteq [0,1]^n \), any state \( \psi \) with dists. \( D_x, D_z \)

\[ D_x(T) \leq 2 \sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}} \]

Assume \( D_z \) is \( 99\% \) concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \), \( D_x(T) < 0.99 \Rightarrow \) Either \( D_x \) or \( D_z \) is well-spread.
The uncertainty principle

\[ |S| \leq \binom{n}{\text{\(O(n)\)}} \cdot 2^r_x \leq 2^r_x + O(\sqrt{\varepsilon} \cdot n) \]

\[ |T| \leq 2^r_z + O(\sqrt{\varepsilon} \cdot n) \]

Uncertainty principle: For sets \( S, T \subseteq \{0,1\}^n \), any state \( \psi \) with dists. \( D_x, D_z \)

\[ D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}} \]

Assume \( D_z \) is 999% concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \),

\[ D_x(T) < 0.99 \implies \text{Either } D_x \text{ or } D_z \text{ is well-spread.} \]
The uncertainty principle

\[ |S| \leq \left( \frac{n}{0(n)} \right)^2, \quad 2^{\frac{S^x}{0(n)}} \leq 2^{\frac{S^x + O(\sqrt{\varepsilon} n)}{0(n)}} \]

\[ |T| \leq 2^{\frac{S^z + O(\sqrt{\varepsilon} n)}{0(n)}} \]

Uncertainty principle: For sets \( S, T \subseteq \{0,1\}^n \), any state \( \Psi \) with dists. \( D_x, D_z \)

\[ D_x(T) \leq 2 \sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}} \]

Assume \( D_z \) is \( 0.99 \% \) concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \),

\[ D_x(T) < 0.99 \implies \text{Either } D_x \text{ or } D_z \text{ is well-spread.} \]
The uncertainty principle

\[ |S| \leq \binom{n}{o(n)} \cdot 2^r \leq 2^r + O(\sqrt{\varepsilon} n) \]

\[ |T| \leq 2^r + O(\sqrt{\varepsilon} n) \]

\[ D_x(T) \leq 2\sqrt{1 - D_z(S)} + \sqrt{\frac{|S| \cdot |T|}{2^n}} \]

Uncertainty principle: For sets \( S, T \subseteq \{0,1\}^n \), any state \( \psi \) with dists. \( D_x, D_z \)

\[ D_x(T) \leq 2\sqrt{1 - D_z(S)} + 2r_x + \frac{r_z}{2} + O(\sqrt{\varepsilon} n) - \frac{n}{2} \]

\[ = \frac{1}{5} + 2^{-k} + O(\sqrt{\varepsilon} n) \]

Code rate

so if \( \varepsilon < O\left(\frac{k^2}{n^2}\right) \), then \( D_x(T) < 0.99 \).

Assume \( D_z \) is \( 0.99 \) concentrated on some \( Z \)-cluster \( S \). Then for any \( X \)-cluster \( T \), \( D_x(T) < 0.99 \) \( \Rightarrow \) Either \( D_x \) or \( D_z \) is well-spread.
Conclusion of the proof

CSS code of linear-rate and linear-distance which are expanding are NCTS.

The [Levien et al. '21] construction can be shown by small modification of the distance bound of to satisfy these conditions.
Conclusion of the proof

CSS code of linear-rate and linear-distance which are expanding are NLTS.

The [Leverrier-Zémor '21] construction can be shown by small modification of the distance bound of $p_f$ to satisfy these conditions.

In progress: All linear-rate and distance codes are NLTS.
What's next after NLTS

NLTS is a necessary consequence of QPCP that isolated the problem of robust entanglement from the computational question.
What's next after NLTS

NLTS is a necessary consequence of QPCP that isolated the problem of robust entanglement from the computational question.

Next step: introduce computation, find NLTS Hamiltonians that capture NP (or MA) computations.
What’s next after NLTS

Constant-depth g. circuits are just one of many possible NP pls of the ground-energy.
What's next after NLTS

Constant-depth q. circuits are just one of many possible NP pls of the ground-energy.

Other examples include stab. circuits, some efficiently contractible tensors, etc. or samplable-queryable states ([Gharabian, Le Gall '21] MA witness)
What's next after NLTS

Constant-depth $g$. circuits are just one of many possible NPpls of the ground-energy.

Other examples include stab. circuits, some efficiently contractible tensors, etc. or samplable-queryable states ( [Gharabian, Le Gell '21] MA witness)

I think we need to prove lower bounds for the following ansatz: