Lower bounds on the power of quantum systems

Chinmay Nirkhe

based on joint works with:

Anurag Anshu, Thom Bohdanowicz, Adam Bouland, Elizabeth Crosson, Bill Fefferman, Umesh Vazirani and Henry Yuen

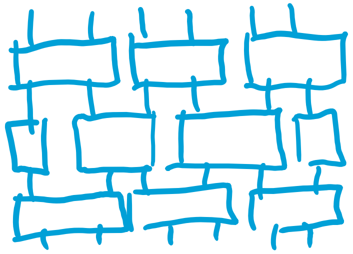
Berkeley
UNIVERSITY OF CALIFORNIA

Quantum systems are powerful...

$BQP^{\mathcal{O}} \not\subseteq PH^{\mathcal{O}}$ Factoring $\in$ BQP $MIP^* = RE$

...but often have great classical approximations

low-depth quantum circuits (decision)



low-depth 3D quantum circuits (sampling)

gapped 1D local Hamiltonian systems

Clifford circuits

tensor networks of low tree-width

noisy quantum circuits

Provable quantum speedups

For what problems is quantum computing/information useful?

For what problems are there (no) classical tractable approximations?

This thesis establishes techniques for lower bounding the complexity of classical approximations of quantum systems.

Provable quantum speedups

This thesis establishes techniques for lower bounding the complexity of classical approximations of quantum systems.

Prior Work:

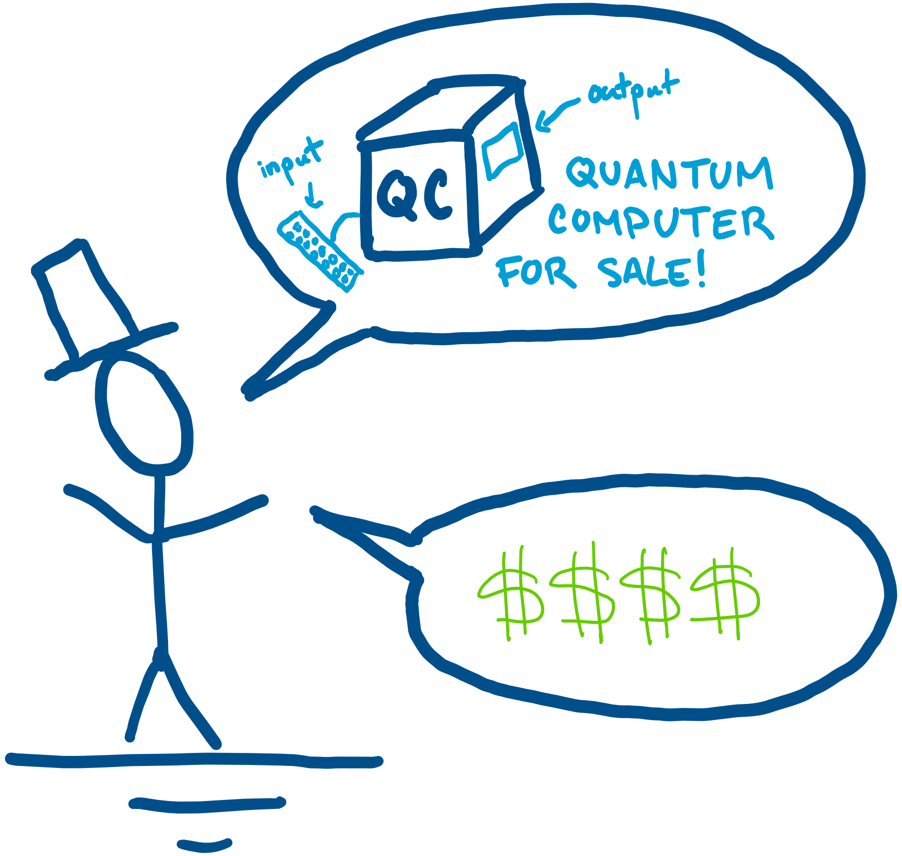
1. #P-hardness of quantum circuit sampling problems

   a.k.a. Quantum supremacy

2. Circuit lower bounds for approximations of quantum code Hamiltonians

   a.k.a. No low-energy trivial states conjecture, a precursor to the Quantum PCP conjecture.

Part I : Complexity of Random Circuit Sampling



How do you tell if the box is actually a quantum computer?

Requirement:

Have it run a task (theoretically) intractable for classical computers.

Quantum Supremacy Proposals

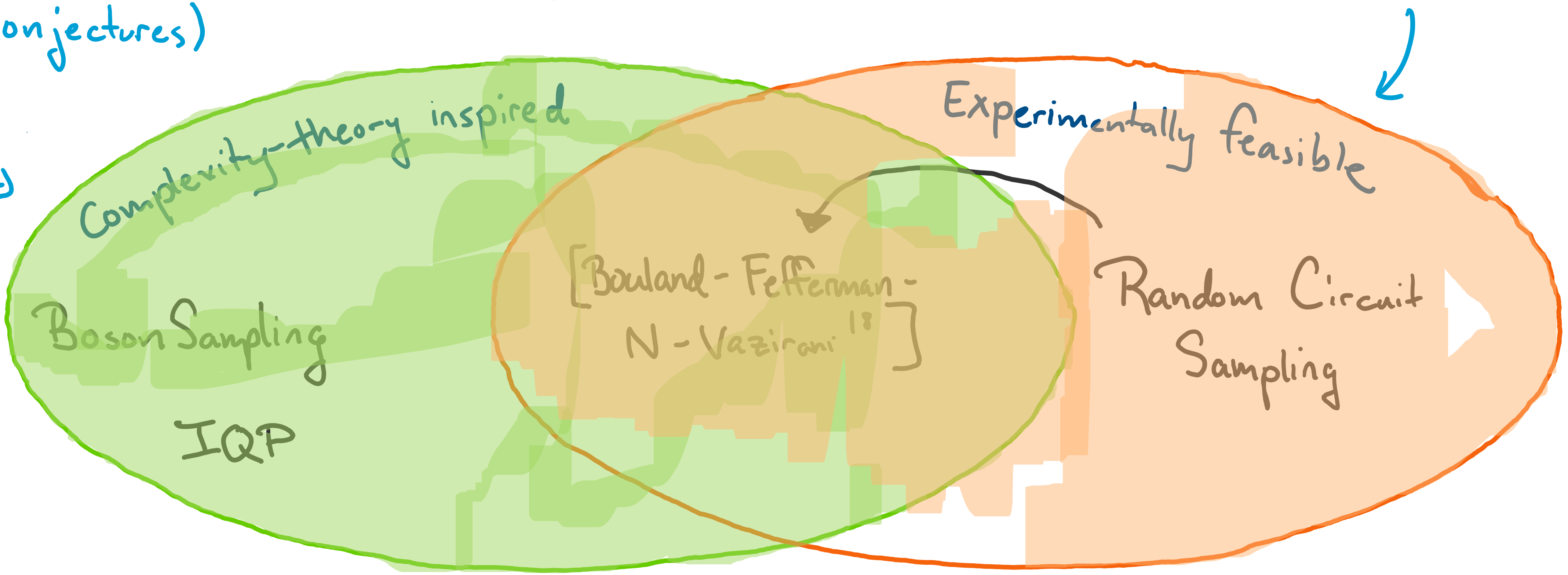
A practical demonstration of a quantum computation which is

1. Experimentally feasible
2. Has theoretical evidence of classical hardness
3. Verifiable

Supremacy proposals

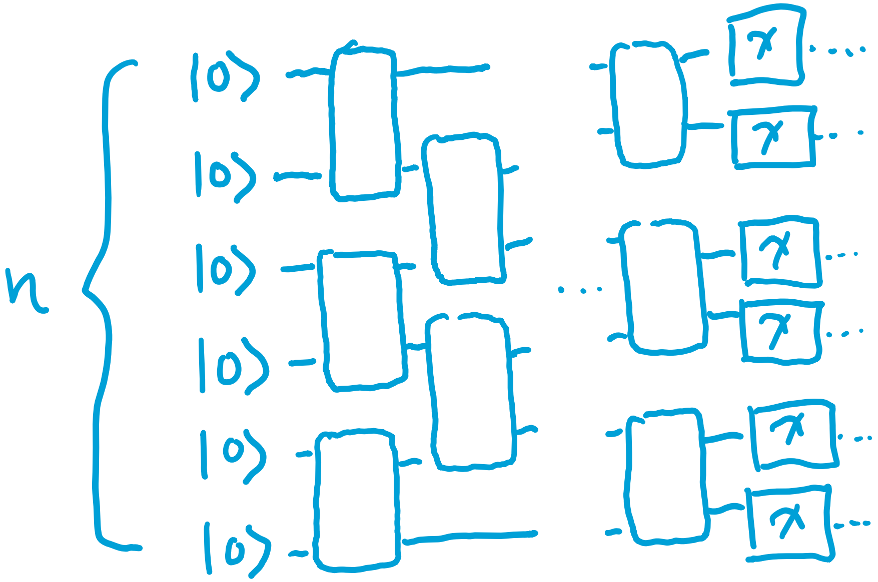
Problems for which no efficient classical algorithms exist (under complexity-theory conjectures)

Problems which we can experimentally test in the next ~5 years



Random Circuit Sampling

"canonical quantum problem"



Every quantum circuit has a classical probability distribution associated with it on $\{0,1\}^n$:

$$P_C(x) = |\langle x | C | 0^n \rangle|^2$$

Sampling from this distribution, is an easy task for an ideal quantum computer

Claim: If the gates are choosen Haar-randomly, then it is intractable for a classical device to output samples from P_C.

Establishing classical hardness

Goal: Show that sampling from the output distribution is #P-hard.

#P = { counting problems }.

examples:

# of solutions to a SAT problem

# of Hamiltonian cycles in a graph

# of 3-colourings of a graph

Idea: Show that if you had a sampler for the distribution, then you could calculate the probability $p_C(x)$ approximately.

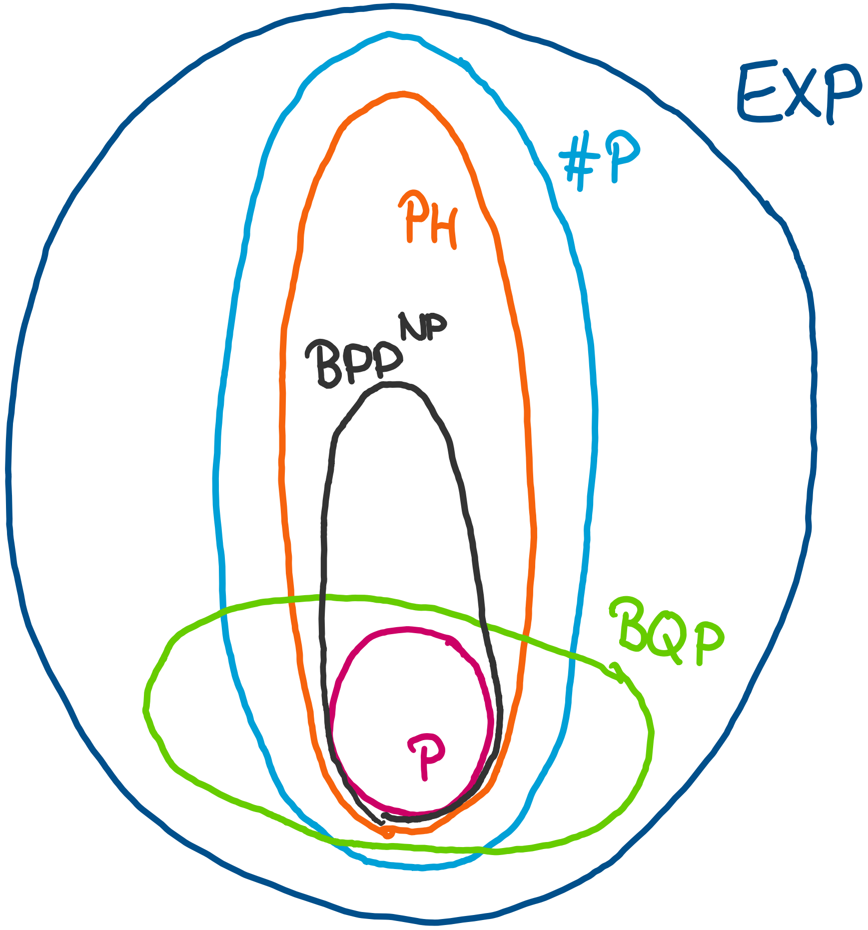
Second, show that approximating $p_C(x)$ is #P-hard.

Establishing classical hardness

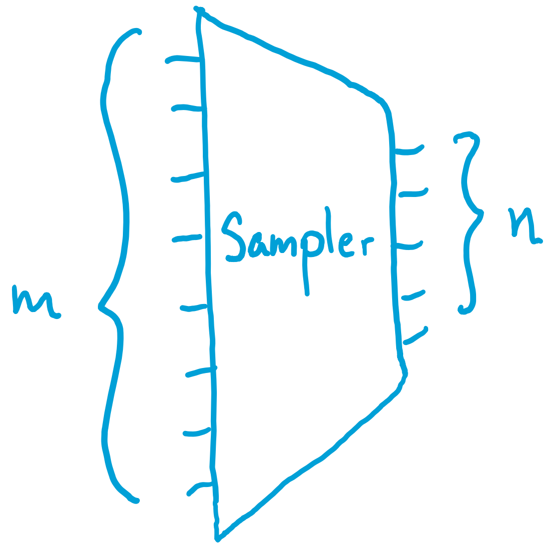
Idea: Show that if you had a sampler for the distribution, then you could calculate the probability $p_C(x)$ approximately.

We will establish a $BPP^{NP} \subseteq PH \subseteq \#P$ - reduction to show this statement.

A known result by Stockmeyer '85.



Stockmeyer's Theorem '85



$$\Pr(S \text{ outputs } x \in \{0,1\}^n) = \frac{\#\{y : S(y) = x\}}{2^m}$$

Let h be a random fn $\{0,1\}^m \to \{0,1\}^r$.

If $\#\{y : S(y) = x\} \geq 10 \cdot 2^r$, then w.h.p.

$\exists\, y$ s.t. $S(y) = x$ & $h(y) = 0^r$.

$\therefore$ $\mathrm{BPP}^{\mathrm{NP}^{\text{Sampler}}}$ can approximate

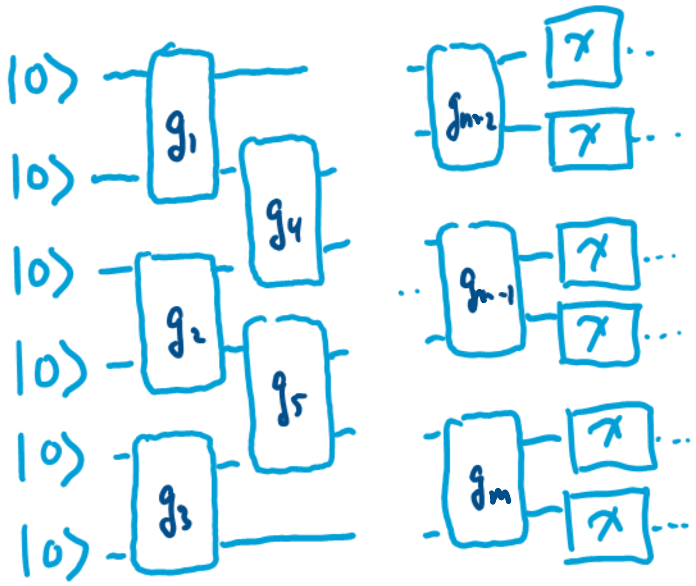
$\Pr(S \text{ outputs } x)$ to mult. 10.

Can be amplified to any ε using standard techniques.

Establishing classical hardness

Second, show that approximating $P_C(x)$ is #P-hard.

"Feynman Path Integral"



$$P_C(x) = \left|\langle x|C|0\rangle\right|^2 = \left|\langle x| g_m g_{m-1} \cdots g_1 |0\rangle\right|^2$$

$$= \left| \sum_{y_1,\dots,y_m \in \{0,1\}^n} \langle x|g_m|y_m\rangle\langle y_m|g_{m-1}|y_{m-1}\rangle \cdots \langle y_1|g_1|0\rangle \right|^2$$

$$= \left| \sum_{\substack{y_0,\dots,y_{m+1} \in \{0,1\}^n \\ y_0 = 0 \\ y_{m+1} = x}} \prod_{j=1}^{m+1} \langle y_j|g_j|y_{j-1}\rangle \right|^2$$

Establishing classical hardness

Second, show that approximating $p_c(x)$ is #P-hard.

$$p_c(x) = \left| \sum_{\substack{y_0, \dots, y_{m+1} \in \{0,1\}^n \\ y_0 = 0 \\ y_{m+1} = x}} \prod_{j=1}^{m+1} \langle y_j | g_j | y_{j-1} \rangle \right|^2$$

With a little work, it can be seen as the difference of two #P-hard quantities, or is therefore GapP-hard.

GapP-hard quantities are hard to multiplicatively approximate.

Putting it all together

Assume we can sample from the output distribution of a #P-hard circuit.

Then, using Stockmeyer's theorem, we can solve this #P-hard problem in BPP^{NP}.

Non-collapse of the Polynomial Heirarchy:

$$BPP^{NP} \subseteq \Sigma_3 \subsetneq PH \subseteq \#P$$

Contradiction!

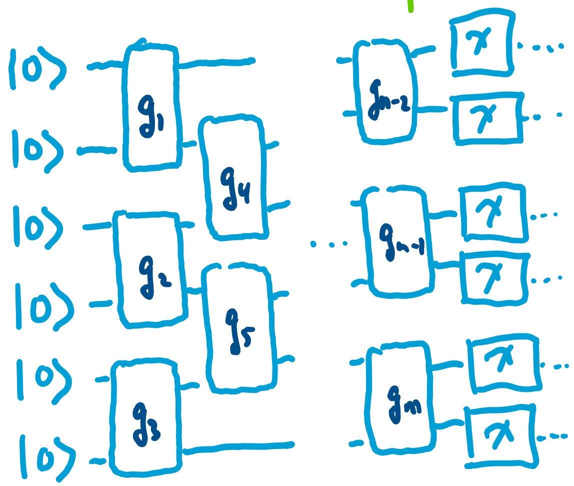
$\therefore$ Exact classical sampling of output distributions is intractable.

Close, but not quite there...

We have shown that exact sampling is #P-hard.

But exact sampling isn't feasible for near-term quantum devices.

Fix an architecture over quantum circuits.



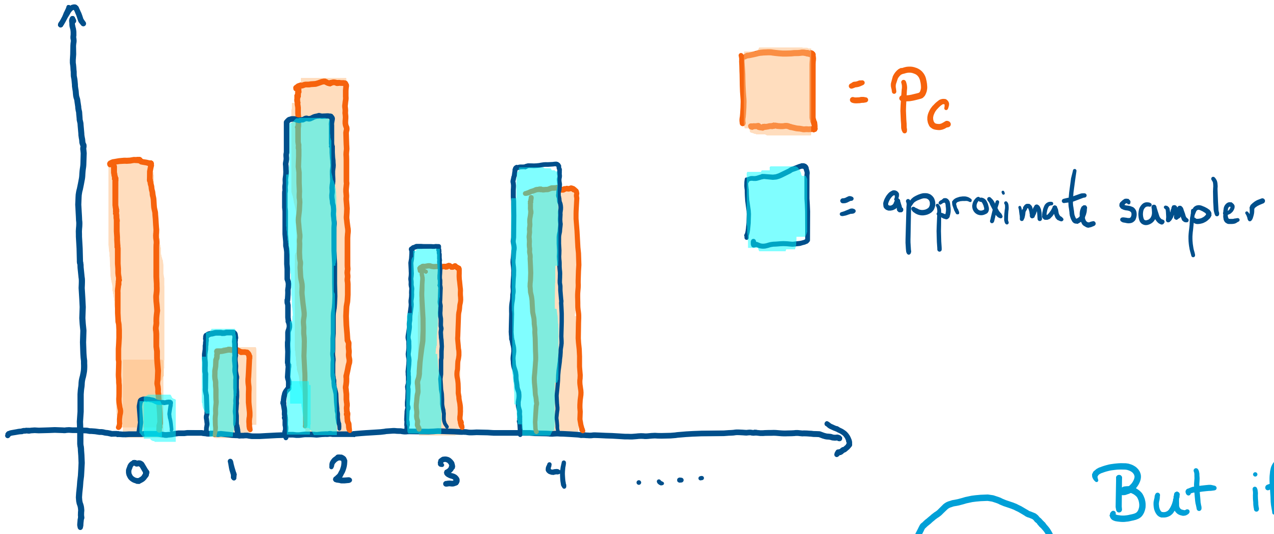
Choose gates $g_1, \dots, g_m \sim$ Haar.

Task:

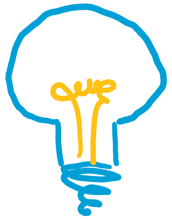
Output, whp over choice of gates, samples from a distribution near the canonical distribution of the circuit.

Showing that approximate sampling is also hard...

Let's assume that $p_c(0)$ is the GapP-hard quantity.



Even if $p_c(0)$ is hard to approximate, an ε-approximate sampler q may have $q(0)$ far from $p_c(0)$, so q may not be hard!



But if for most x, $p_c(x)$ is hard to approximate, then an approximate sampler will still be hard!

Equivalently, we need to show that the quantity $p_C(x)$ is average-case hard to approximate.

Currently, we don't know how to prove such a statement for any supremacy proposal including Boson Sampling or IQP.

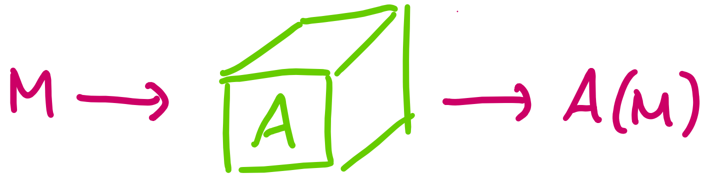
Due to a property called hiding, we need to show a statement like:

Calculating $p_C(0)$ for > 0.76 fraction of circuits w.r.t. the Haar-distribution is #P-hard.

average-to-worst-case reduction

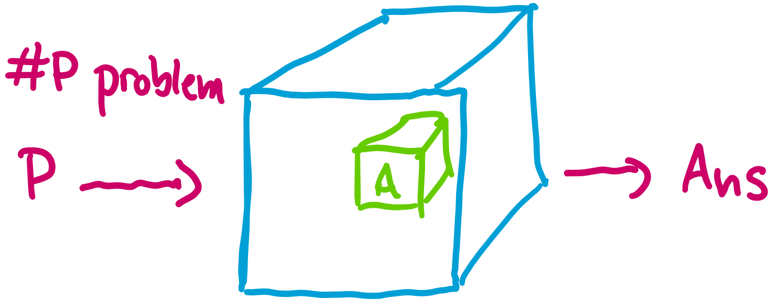
What known problems have avg-to-worst case reductions?

$$\text{perm}(M) = \sum_{\sigma \in S_n} \prod_{j=1}^{n} M_{j,\sigma(j)}$$



If $\Pr_M(A(M) = \text{perm}(M)) > 0.76$

then, $\exists$



in particular, can solve permanents on worst-case inputs.

Theorem (Lipton '91, GLR+ '91)

The following is #P-hard: For sufficiently large prime power q, given uniformly random matrix $M \in \mathbb{F}_q^{n \times n}$, calculating $\text{perm}(M)$ with prob. > 0.76.

Goal: Find a similar polynomial structure in the problem of Random Circuit Sampling

$$\mathrm{Perm}(M) = \sum_{\sigma \in S_n} \prod_{j=1}^{n} M_{j,\sigma(j)}$$

$$P_C(x) = \left| \sum_{\substack{y_0, \dots, y_{m+1} \in \{0,1\}^n \\ y_0 = 0 \\ y_{m+1} = x}} \prod_{j=1}^{m+1} \langle y_j | g_j | y_{j-1} \rangle \right|^2$$

Feynman
Path
Integral

$$P_C(x) = \left| \sum_{\substack{y_0, \ldots, y_{m+1} \in \{0,1\}^n \\ y_0 = 0 \\ y_{m+1} = x}} \prod_{j=1}^{m+1} \langle y_j | g_j | y_{j-1} \rangle \right|^2$$

Feynman Path Integral

$P_C(x)$ is a low-deg polynomial in the entries of $g_1, \ldots, g_m$. We can apply a similar interpolation technique to demonstrate that Random Circuit Sampling is worst-to-average case hard.

Exact vs approximate hardness

This proves (modulo technicalities) the #P-hardness of calculating

$p_C(x)$ to $\pm 2^{-\mathrm{poly}(n)}$ for over 76% of circuits.

However, in order to use the Stockmeyer argument, this would

need to be improved to $\pm 2^{-n}/\mathrm{poly}(n)$.

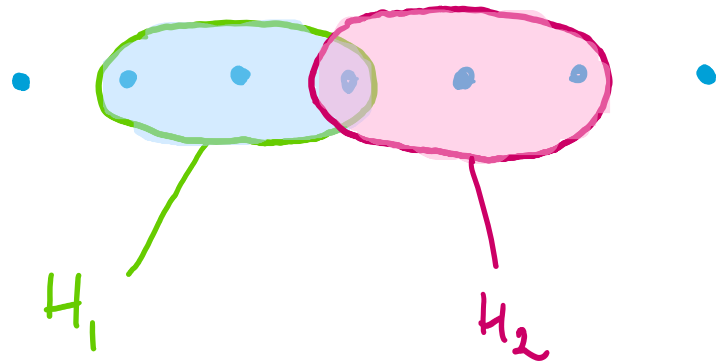
However, this is still very far from the noise achievable by

current quantum computers.

Part II : Circuit lowerbounds for low-energy states of code Hamiltonians

The QPCP Conjecture

n qubits:



Local Hamiltonian $H = \sum_{i=1}^{O(n)} H_i$

acting on n qubits.

$$E = \inf_{\phi} \operatorname{tr}(H\phi).$$

Given $\{H_i\}$, how hard is it to approximate E up to accuracy $\varepsilon(n)$?

Thm For $\varepsilon(n) = \frac{1}{n^2}$, its QMA-hard.

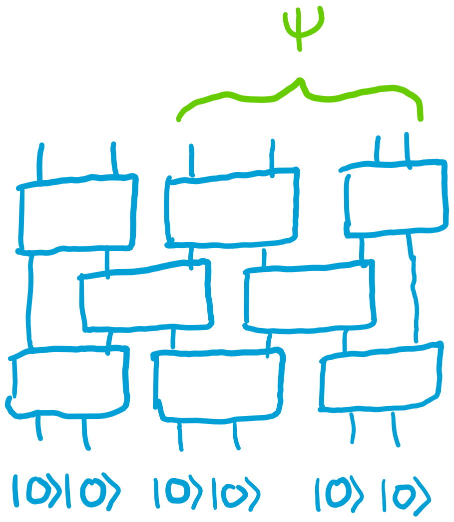
[Kitaev'03, Cahay, Landau, Nagaj'16, Bausch, Crosson'18]

QPCP Conjecture It is also QMA-hard for $\varepsilon(n) = \Omega(n)$.

[Aharonov, Naveh'02, Aharonov, Arad, Vidick'13]

Simplifying the problem : NLTS Conjecture [Freedman, Hastings '14]

(No low-energy trivial states conj.)



$cc(\psi)$

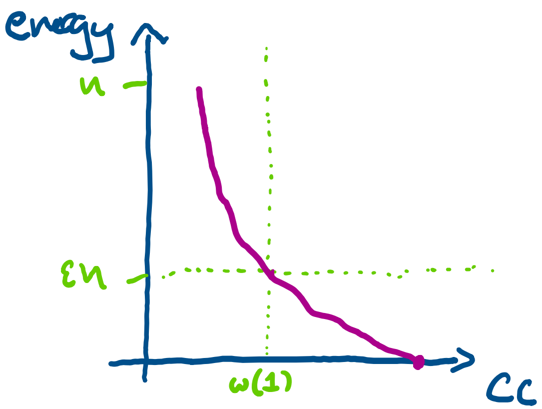
= min depth*

* : gates are any 2 qubit unitaries do not need to be on geometrically local circuits

NLTS Conj. $\exists$ a fixed constant $\varepsilon > 0$, and a fam of local Ham. $\{H^{(n)}\}_n$ on n qubits s.t.

$\forall\ \psi^{(n)}$ with $\mathrm{tr}(H^{(n)}\psi^{(n)}) < \varepsilon n$,

the $cc(\psi^{(n)}) = \omega(1)$ (superconstant).



The NLTS Conjecture [Freedman, Hastings '14]

① Necessary consequence of the QPCP conjecture

② Seperates the "robustness of entanglement" question from the "hardness of computation" aspect of QPCP

③ Asks about the ability to conduct quantum computation at room temperature

Our Results [Anshu-N 20]

Let $\mathcal{C}$ be a $[[n, k, d]]$ stabilizer error-correcting code of const. locality. (double sided LDPC)

n: # of physical qubits; k: # of logical qubits; d: erasure distance

Let $H_{\mathcal{C}}$ be the corresponding local Ham. $H_{\mathcal{C}} = \sum H_i$ with $H_i = \frac{\mathbb{I} - C_i}{2}$.

Let ρ be a mixed state s.t. $\mathrm{tr}(H_{\mathcal{C}}\rho) \leq \varepsilon n$. Then,

$$cc(\rho) \geq \Omega\left(\min\left\{\log d, \log\left(\frac{k}{n} \cdot \frac{1}{\varepsilon \log(1/\varepsilon)}\right)\right\}\right).$$

An almost linear NLTS Theorem. (dependence on ε).

Our Results

Let $\mathcal{C}$ be a $[[n, k, d]]$ stabilizer error-correcting code of const. locality.

Let ρ be a mixed state s.t. $\mathrm{tr}(H_{\mathcal{C}}\, \rho) \leq \varepsilon n$. Then,

$$cc(\rho) \geq \Omega\left(\min\left\{\log d,\ \log\left(\frac{k}{n} \cdot \frac{1}{\varepsilon \log(1/\varepsilon)}\right)\right\}\right).$$

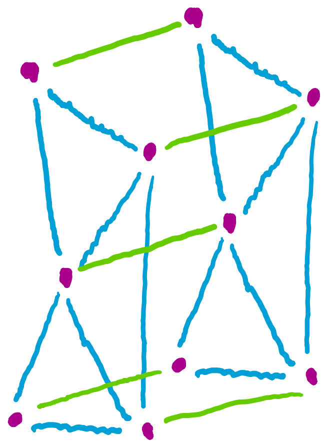
Cor If $k = \Omega(n)$ (linear rate) and $d = \Omega(n^c)$ (polynomial distance)

then for $\mathrm{tr}(H_{\mathcal{C}}\, \rho) \leq O(n^{0.99})$, | $\mathrm{tr}(H_{\mathcal{C}}\, \rho) \leq o(n)$

$cc(\rho) \geq \Omega(\log n)$ | $cc(\rho) \geq \omega(1)$.

Example codes

① Tillich-Zémor[09] hypergraph product codes

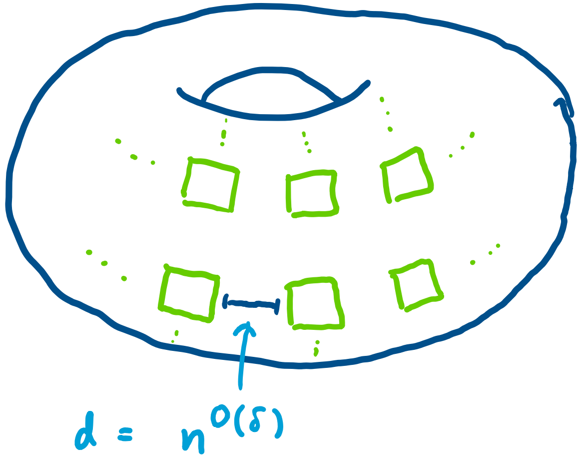


$k = \Theta(n)$

$d = \Theta(\sqrt{n})$

Possibly full NLTS.

② Punctured toric code with $\Omega(n^{1-\delta})$ holes.



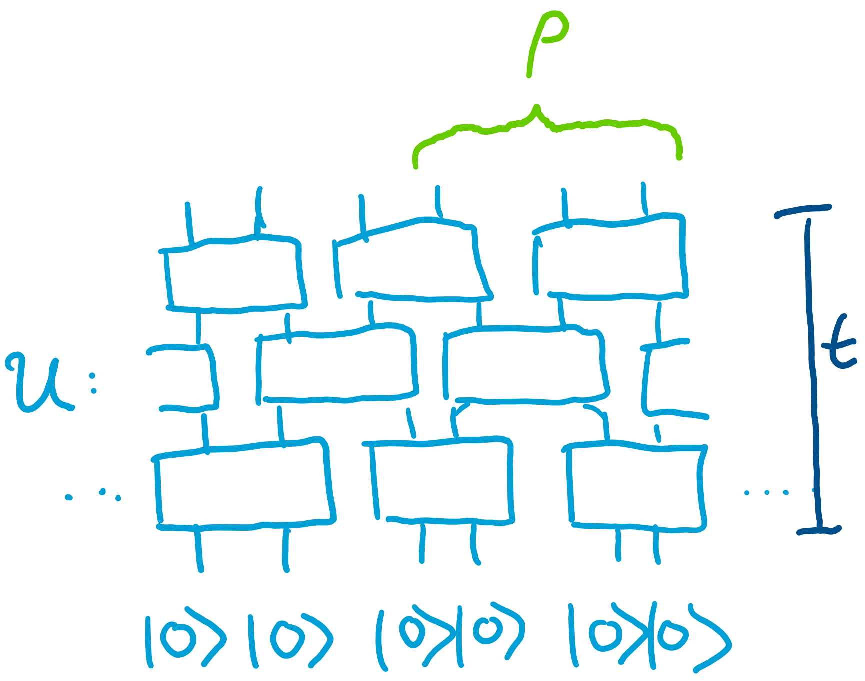
$k = \Theta(n^{1-\delta})$

$d = \Theta(n^{\delta})$

for $tr(H\rho) \leq O(n^{1-2\delta})$, $cc(\rho) \geq \Omega(\delta \log n)$.

Not full NLTS since 2D.

Circuit Complexity



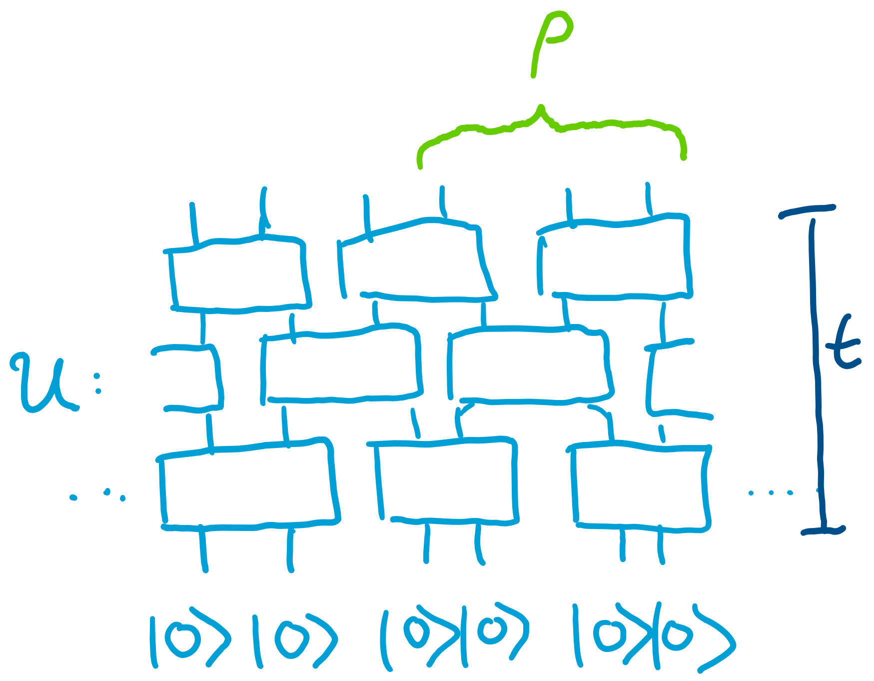
$cc(\rho)$ = min depth t of any ckt exactly producing ρ.

Fact A state has $cc \leq 1$ iff it is a tensor product state.

Fact Given a $O(1)$-local Ham. H and a state ρ of $cc(\rho) = t$, there is a classical alg. for computing $\mathrm{tr}(H\rho)$ (i.e. energy) in time $\mathrm{poly}(n) \cdot \exp(\exp(t))$.

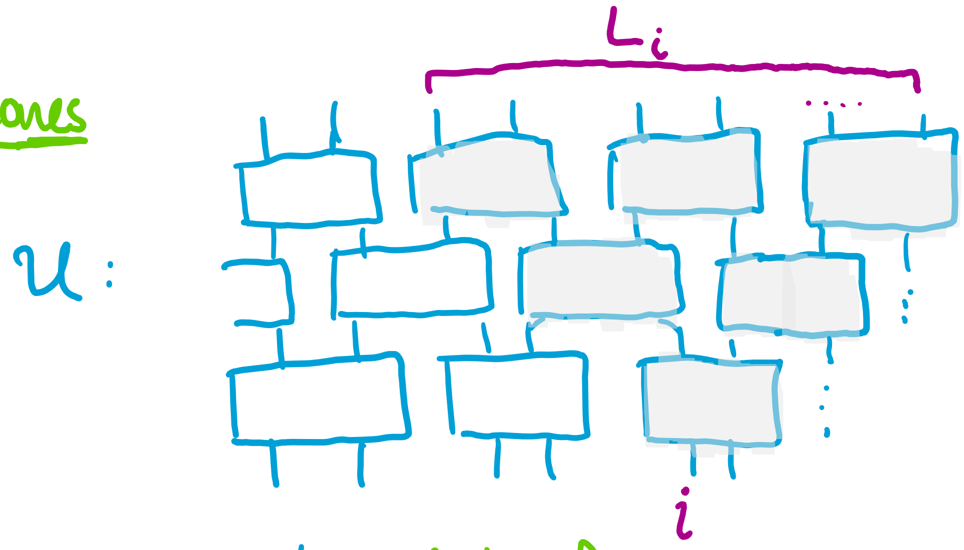
Pf. Each term $\mathrm{tr}(H_i \rho)$ depends on only the reduced computation on $O(2^t)$ qubits.

Circuit Complexity



cc(ρ) = min depth t of any ckt exactly producing ρ.

Lightcones



Fact 1 $|L_i| < 2^t$ ← depth of ckt.

reduced density matrix on L_i.

Fact 2 $\mathrm{tr}_{-i}(U \rho U^\dagger) = \mathrm{tr}_{-i}(U \rho_{L_i} U^\dagger)$

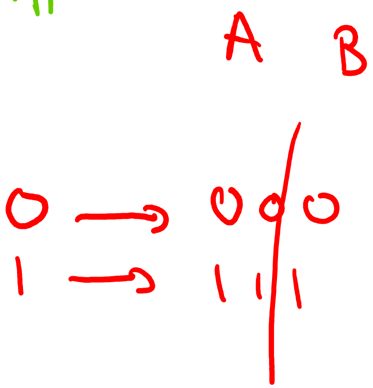
Error-correcting Codes

i.e. Local Indistinguishability.

Knill-Laflamme conditions:

Can correct an error E iff

$$\Pi E \underbrace{\Pi}_{\substack{\text{projector on} \\ \text{the codespace.}}} = \eta_E \Pi$$



Code has dist d, if it can correct all errors of size $< d$.

Let S be a set of qubits of $|S| < d$. (correctable region)

Then $\forall$ codestates ρ, $\rho_S = tr_{-S}(\rho)$ is an invariant.

Pf: E = any operator acting only on S.

$$tr(E\rho) = tr(E \Pi \rho \Pi)$$
$$= tr(\Pi E \Pi \rho)$$
$$= tr(\eta_E \Pi \rho)$$
$$= \eta_E. \leftarrow \rho \text{ independent.}$$

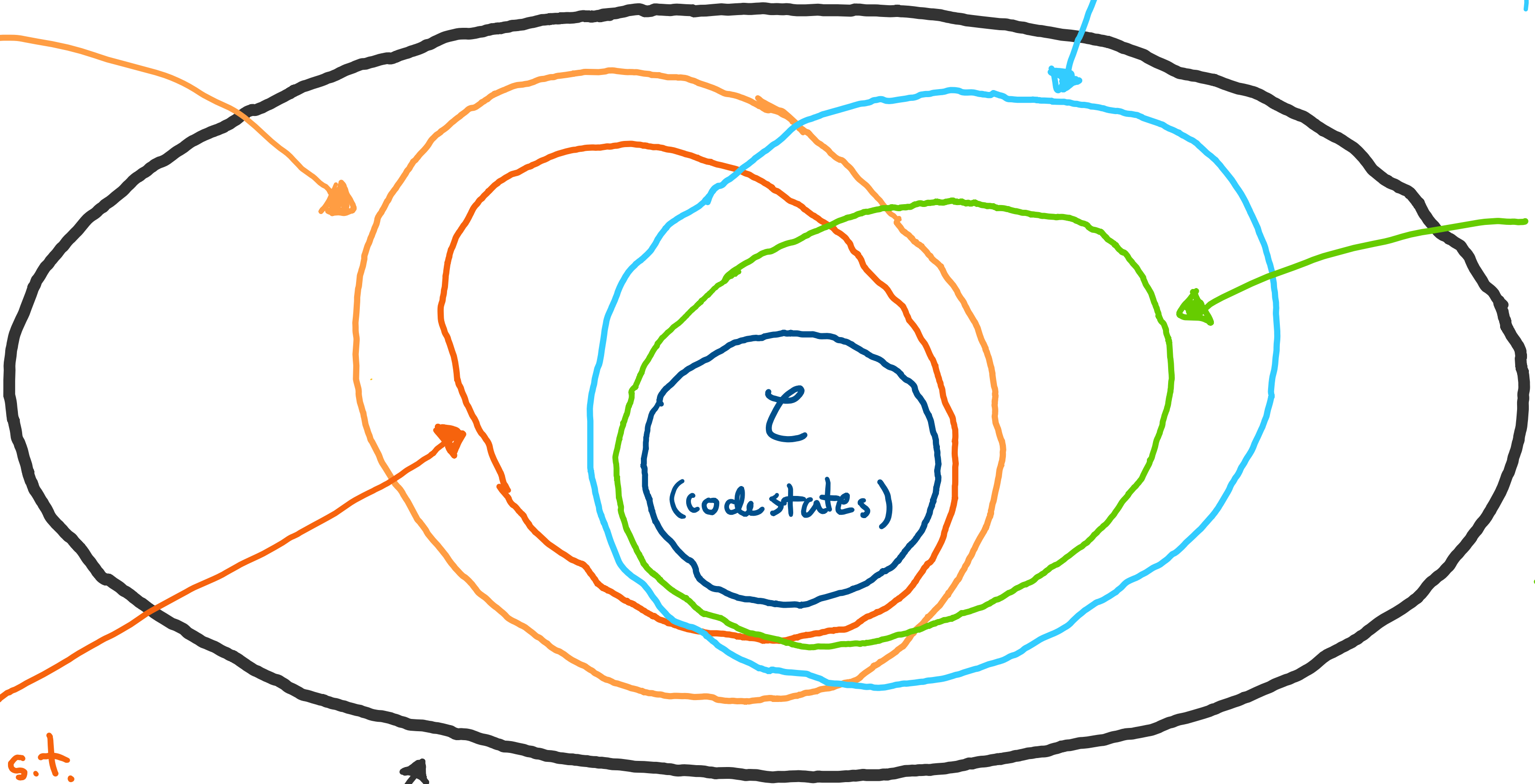
∎

The set of low-energy states

ε-smooth states: $\forall i$, $\mathrm{tr}(H_i \rho) \le \varepsilon$.

Combinatorial states: $\Pr_i\left(\mathrm{tr}(H_i \rho) \neq 0\right) \le \varepsilon$.

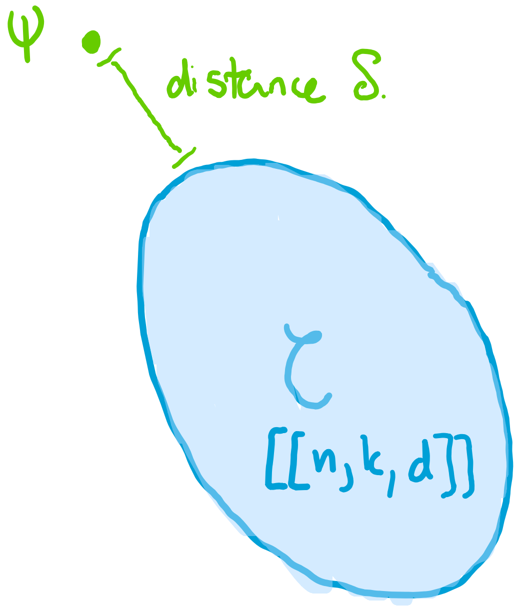
low-error states: take codestate ψ and change up to $O(\varepsilon n)$ qubits



ε-dist states: $\exists$ codestate ψ s.t. $\|\rho - \psi\|_1 \le \varepsilon$.

all low energy states: $\mathrm{tr}(H\rho) \le \varepsilon n$

Warmup: Circuit LBs for low-distance states



Let ψ be a state dist δ from $\mathcal{C}$. What is $cc(\psi)$?

Folklore: For any codestate ρ, $cc(\rho) = \Omega(\log d)$.

For simplicity, let's only consider pure states and circuits without ancillas.

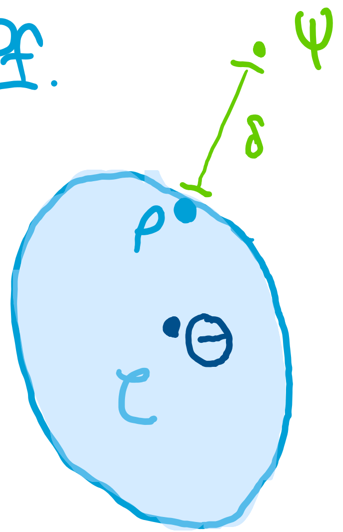
Thm: Let $\sqrt{\delta} < k/n$, for any state $|\psi\rangle$ of dist δ from $\mathcal{C}$.

$$\Rightarrow cc(\psi) \geq \Omega(\log d).$$

Warmup: Circuit LBs for low-distance states

Thm: Let $\sqrt{\delta} < k/n$, for any state $|\psi\rangle$ of dist δ from $\mathcal{C}$. $\Rightarrow cc(\psi) \geq \Omega(\log d)$.

Pf.



ρ be closest codestate to ψ. Θ be encoded maximally mixed state.

① Let R be a region of $|R| < d$.

$$\underbrace{\psi_R \approx_\delta}_{\text{distance}} \rho_R \underbrace{=}_{\text{local indistinguishability}} \Theta_R.$$

② Let $|\psi\rangle = \mathcal{U}|0\rangle^{\otimes n}$ for $\mathcal{U}$ of depth t s.t. $2^t < d$.

$|0\rangle\langle 0| = tr_{-i}(\mathcal{U}^\dagger \psi \mathcal{U})$.

③ $|0\rangle\langle 0| = tr_{-i}(\mathcal{U}^\dagger \psi \mathcal{U}) = tr_{-i}(\mathcal{U}^\dagger \psi_{L_i} \mathcal{U}) \underset{①}{\approx_\delta} tr_{-i}(\mathcal{U}^\dagger \Theta_{L_i} \mathcal{U}) = tr_{-i}(\mathcal{U}^\dagger \Theta \mathcal{U})$. [green ='s from the lightcone argument]

④ $S(tr_{-i}(\mathcal{U}^\dagger \Theta \mathcal{U})) \leq \sqrt{\delta}$. ⑤ $k = S(\Theta) = S(\mathcal{U}^\dagger \Theta \mathcal{U}) \leq \sum_{i=1}^{n} S(tr_{-i}(\mathcal{U}^\dagger \Theta \mathcal{U})) \leq \sqrt{\delta}\, n$. $\perp$.

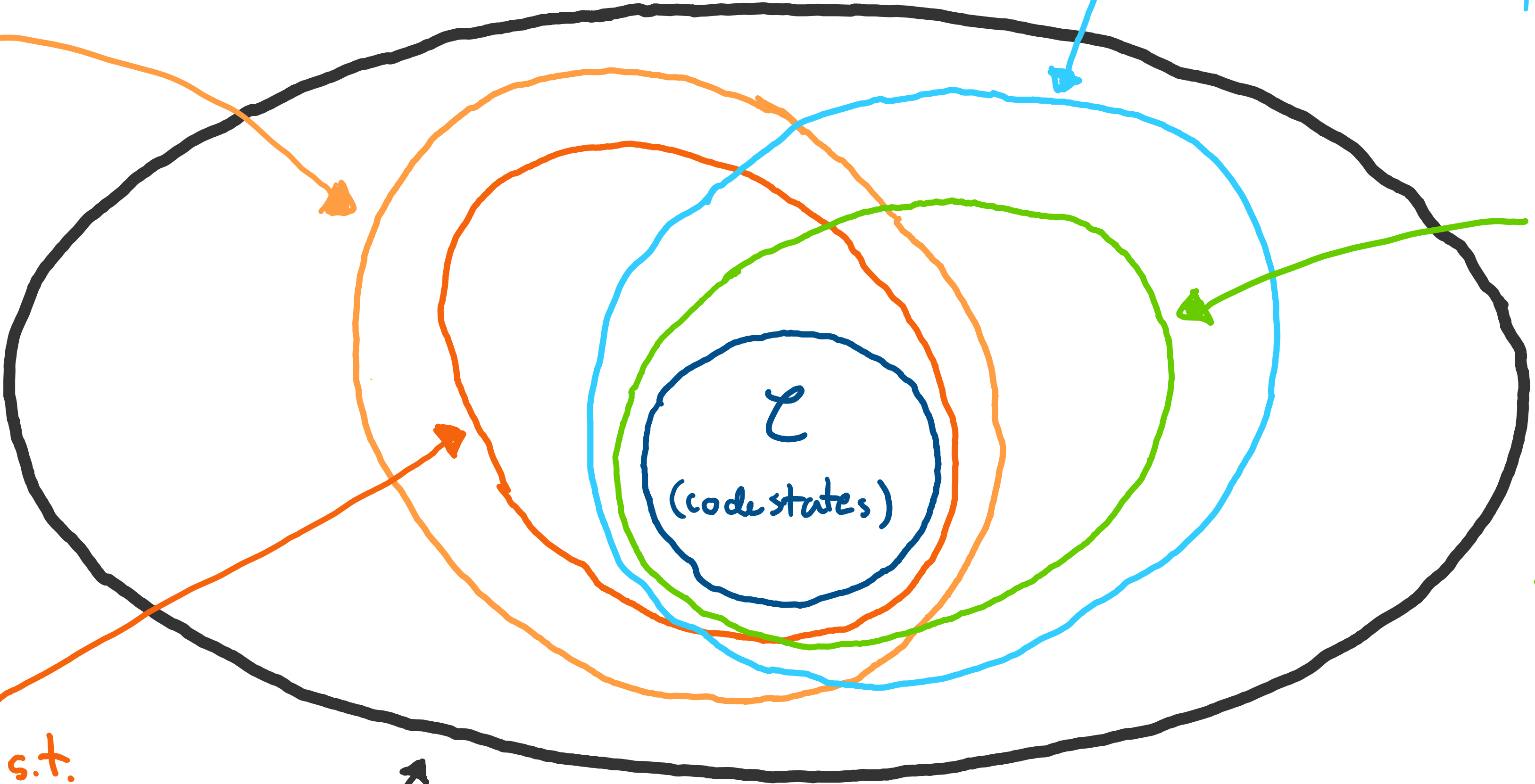
The set of low-energy states

Combinatorial states:

$\Pr_i(\mathrm{tr}(H_i\rho) \neq 0) \leq \varepsilon.$

ε-smooth states: $\forall i$, $\mathrm{tr}(H_i\rho) \leq \varepsilon.$

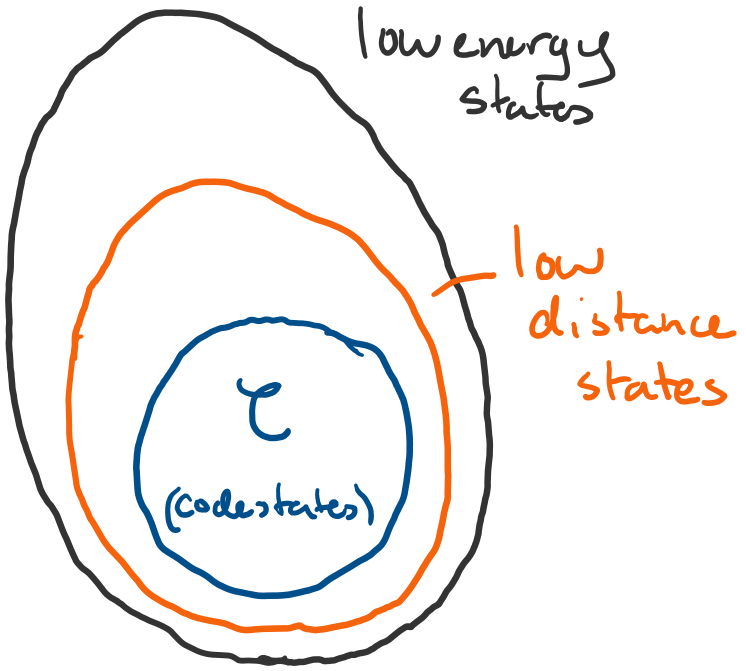
low-error states: take codestate ψ and change up to $O(\varepsilon n)$ qubits



ε-dist states: $\exists$ codestate ψ s.t. $\|\rho - \psi\|_1 \leq \varepsilon.$

all low energy states: $\mathrm{tr}(H\rho) \leq \varepsilon n$

Extending the argument to low-energy states



If $k = \Omega(n)$, then circuit LBs for all low-distance states.

LDPC Stabilizer Codes

All checks are tensor products of a few Paulis.

$$\mathcal{C} = \{ |\psi\rangle : C_i|\psi\rangle = |\psi\rangle \ \forall i \}.$$

$$D_s = \{ |\psi\rangle : C_i|\psi\rangle = (-1)^{s_i}|\psi\rangle \ \forall i \} \text{ for } s \in \{0,1\}^n.$$

Rmk: Local indistinguishability holds for each eigenspace D_s: Region R s.t. $|R| < d$. Then, ρ_R invariant over each D_s.
(but can depend on s).

Main Thm

Let $\mathcal{C}$ be a $[[n,k,d]]$ stabilizer LDPC code and ϕ a n qubit mixed state s.t. $\mathrm{tr}(H_{\mathcal{C}}\phi) \le \varepsilon n$. Then,

$$cc(\phi) \ge \Omega\left(\min\left\{\log d,\ \log\left(\frac{k}{n}\cdot\underbrace{\frac{1}{\varepsilon\log(1/\varepsilon)}}_{\ge \frac{1}{\sqrt{\varepsilon}}}\right)\right\}\right).$$

Sketch of low-energy argument: gentle measurement

Let ϕ be a n-qubit mixed state and $\mathcal{U}$ a depth t ckt on m qubits constructing ϕ.

Let $\varepsilon_i = \mathrm{tr}(H_i \phi)$ and $\sum_{i=1}^{N} \varepsilon_i \leq \varepsilon n$. Wlog can assume $m \leq n \cdot 2^t$.

Let ψ be ϕ after coherently measuring each stabilizer into $N = O(n)$ extra ancilla.

And Ψ be ϕ after incoherently measuring.

ancilla	code qubits	syndrome measurements

ψ has a constructing ckt W of depth $t + O(1)$. $\leftarrow$ due to LDPC.

① Let R be a region of the qubits.

$$F(\psi_R, \Psi_R) \geq 1 - \sum_{\text{syndrome} \ni \text{qubit } i \in R} \varepsilon_i .$$

Pf: Roughly gentle measurements from commuting measurements.

Sketch of low-energy argument : introducing entropy

Ψ = incoherently measured Φ, the low-depth low-energy state.

$$\mathcal{E}(\rho) := \frac{1}{4^k} \sum_{x,z \in \{0,1\}^k} (\bar{X}^x \bar{Z}^z)(\rho)(\bar{X}^x \bar{Z}^z)^\dagger$$ i.e. logical completely decohering channel

Define $\Theta = \mathcal{E}(\Psi)$. $\Rightarrow$ $S(\Theta) \geq k$.

② Let R be a region of qubits s.t. $|R| < d$.

Then $\Psi_R = \Theta_R$.

Pf: Local indistinguishability per eigenspace D_s. Both Ψ and Θ are CQ states with same dist.

Sketch of low-energy argument : Putting it together.

ψ = coherently measured ϕ. Θ = logically completely decohered ψ.

Ψ = incoherently measured ϕ.

① $F(\psi_R, \Psi_R) \geq 1 - \sum_{i \in R} \varepsilon_i$ ② $\Psi_R = \Theta_R$ when $|R| < d$.

syndrome measurement

③ For any qubit j,

$\mathrm{tr}_{-j}(W^\dagger \psi W) = |0\rangle\langle 0|$.

④ Assuming $2^{t+O(1)} < d$, then

$$F(\mathrm{tr}_{-j}(W^\dagger \psi W), \mathrm{tr}_{-j}(W^\dagger \Theta W))$$

$$\geq F(\mathrm{tr}_{-j}(W^\dagger \psi_{L_j} W), \mathrm{tr}_{-j}(W^\dagger \Theta_{L_j} W))$$

$$\geq 1 - \sum \varepsilon_i .$$ ⟵ by ① + ②.

Sketch of low-energy argument : Bounding the rate

④ $F\left(|0\rangle\langle 0|, \mathrm{tr}_{-j}(W^\dagger \Theta W)\right) \geq 1 - \sum_{i \in L_j} \varepsilon_i := 1 - \varepsilon_{L_j}$

$\mathbb{E}\ \varepsilon_{L_j} = O(2^t \varepsilon)$.

⑤ $S\left(\mathrm{tr}_{-j}(W^\dagger \Theta W)\right) \leq \varepsilon_{L_j} \log\left(\frac{1}{\varepsilon_{L_j}}\right)$.

⑥ $k \leq S(\Theta) = S(W^\dagger \Theta W)$

$\leq \sum_j S\left(\mathrm{tr}_{-j}(W^\dagger \Theta W)\right)$

$\vdots \qquad \vdots$

$\leq O\left[(m + O(n))\left(2^{t+O(1)} \varepsilon \log(1/\varepsilon)\right)\right]$

$= O\left(2^{2t} n \varepsilon \log(1/\varepsilon)\right)$.

$\therefore$ if Φ has depth t and energy $\leq \varepsilon n$,

$t \geq \Omega\left(\min\left\{\underbrace{\log d}_{\text{assumed for calculating fidelity.}}, \underbrace{\log\left(\frac{k}{n} \cdot \frac{1}{\varepsilon \log 1/\varepsilon}\right)}_{\text{due to bound on the rate.}}\right\}\right)$.

Part III: Future thesis work

Proving the NLTS Conjecture

① Conjecture: Linear rate & polynomial dist. stabilizer codes are NLTS.

consistent with prev no go results

potential for improving the analysis of almost NLTS result

② tree-NLTS, Clifford-NLTS, etc...

NLTS proves lower-bounds against one form of classical approximation

but QPCP proves lower-bounds against all forms of classical approximation

③ Improvements and ideas in quantum local testability

QPCP $\Rightarrow$ NLTS (modulo NP $\neq$ QMA)

QPCP: given Local Ham H is min energy $= 0$ or $\geq \frac{1}{10} n$ is QMA-hard.

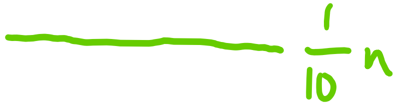
$+$

$\neg$NLTS: For every $\varepsilon > 0$, every Local Ham H, $\exists$ a state of $cc = O_\varepsilon(1)$ of energy $\leq \varepsilon n$.

$\Rightarrow$

QMA pf that min energy $= 0$ is a state ρ s.t. $\mathrm{tr}(H\rho) = 0$.

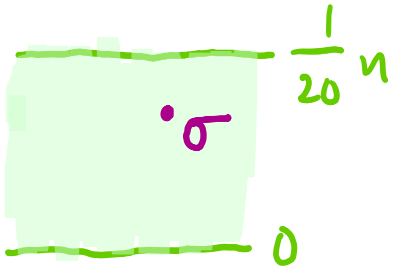
Instead, by $\neg$NLTS, $\exists$ a state σ with $cc = O(1)$ & $\mathrm{tr}(H\sigma) \leq \frac{1}{20} n$. Let $\mathcal{U}$ be defining ckt.



Claim: $\mathcal{U}$'s description is a classical witness for problem.

min energy $= 0 \Rightarrow$ classically check $\mathrm{tr}(H\sigma) \leq \frac{1}{20} n$

min energy $\geq \frac{1}{10} n \Rightarrow \forall\, \mathcal{U}$, $\mathrm{tr}(H\sigma) \geq \frac{1}{10} n$.



$\Rightarrow$ QMA $=$ NP.

because depth $\mathcal{U}$ is $O(1)$.

The Clifford NLTS Conjecture

Fact Given a state ψ generatable by Clifford circuit of poly(n) depth, one can compute $\mathrm{tr}(H\psi)$ for ℓ-local Ham. H in time $\mathrm{poly}(n)\cdot \exp(\ell)$.

Pf. Extended Gottesman-Knill Theorem.

Conj. $\exists$ a $\varepsilon > 0$ and a family of local Hamiltonians $\{H^{(n)}\}$ s.t. if $\psi^{(n)}$ is a Clifford state of poly(n) circuit complexity then $\mathrm{tr}\left(H^{(n)}\psi^{(n)}\right) > \varepsilon n$.

Also, a necessary consequence of the QPCP conjecture.

A bigger leap: QPCP Conjecture directly

Classically, PCP theorem $\Leftrightarrow$ games version of PCP.

Quantum games have come a long way

- $MIP^* = RE$
- locally testable code with quantum soundness

Although about bipartite entanglement power, can it be translated to multipartite entanglement case?

Classical progress on the connection between HDX and local testability.

What if NLTS is false?

$\Rightarrow$ Local Hamiltonian problem for promise gap $\Omega(n)$ is NP-complete.

Pf. Classical PCP for completeness and $\neg$NLTS gives classical verification.

What is the hardness of promise gap $\Omega(n^{1-\delta})$ for $\delta > 0$?

When gap $\Omega(n^{-2})$, its known to be QMA-complete.

Our almost NLTS result is consistent with gap $\Omega(n^{1-\delta})$ being QMA-hard.

Summary

Past research explores techniques for proving lower bounds on the power of quantum systems

Future goals are to continue this line of research ideally culminating in new understanding of the power of entanglement and more generally quantum hardness of approximation