Lecture 15

Nov 12, 2025

Finding a basis $\langle b_1, \ldots b_n \rangle$ for S_ψ s.t. only b_1 anticommutes:

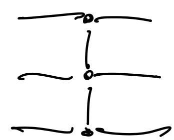
① Renumber bases s.t. b_1 anticommutes.

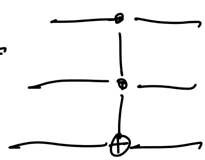
② If b_k anticommutes, replace b_k with $b_1 b_k$.

Next, computation with a few non-Clifford gates.

non-Clifford gate examples:

$$T = \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

CCZ 

CCX = 

(Toffoli)

Theorem (Solovay-Kitaev) Any 2-qubit unitary can be ϵ-approximated using $O(\text{polylog}(1/\epsilon))$ H, T, CNOT gates.

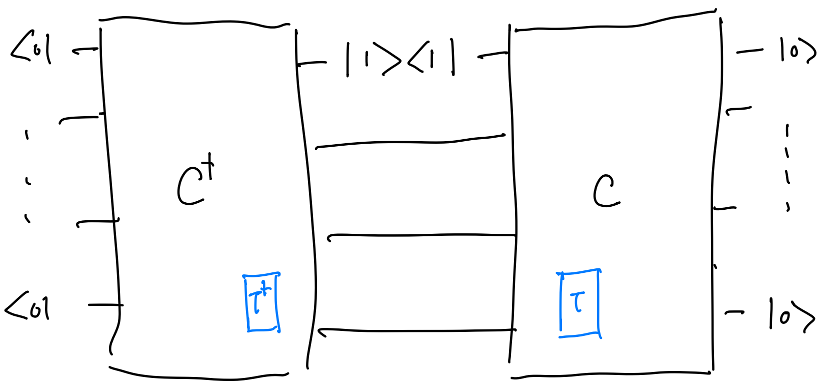
Solovay-Kitaev + Clifford simulation suggests that the number of T gates in a H, T, CNOT circuit should be a measure of the circuits complexity.

Thm $\exists$ a constant $\alpha > 0$, s.t. computing the output probability of a quantum circuit consisting of m Clifford gates, t T-gates on n qubits can be classically computed in time $O(2^{\alpha t} \cdot \mathrm{poly}(n, m))$.

Best: $\alpha < 0.4$ (Qassim-Pashayan-Gosset)

Today $2^{\alpha} = 3$, $\alpha < 1.6$.

Model of such a computation:



↑ one big matrix multiplication:

Replacement :

$$T^{\dagger} \otimes T = a\, \mathbb{1} \otimes \mathbb{1} + b\, S^{\dagger} \otimes S + c\, Z^{\dagger} \otimes Z.$$

$$\begin{pmatrix} 1 & & & \\ & e^{i\pi/4} & & \\ & & e^{-i\pi/4} & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} a & & & \\ & a & & \\ & & a & \\ & & & a \end{pmatrix} + \begin{pmatrix} b & & & \\ & bi & & \\ & & -bi & \\ & & & b \end{pmatrix} + \begin{pmatrix} c & & & \\ & -c & & \\ & & -c & \\ & & & c \end{pmatrix}$$

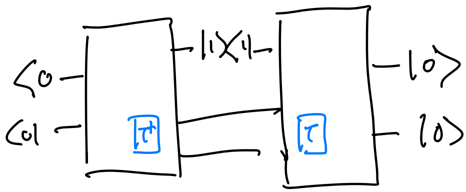
Solve

$$a + b + c = 1 \qquad a = 1/2$$

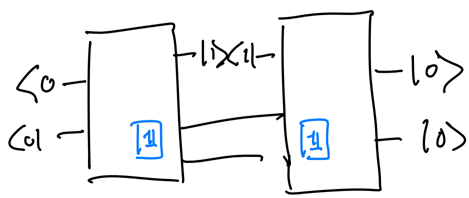
$$a + bi - c = e^{i\pi/4} \qquad b = 1/\sqrt{2}$$

$$a - bi - c = e^{-i\pi/4}. \qquad c = \frac{1}{2} - \frac{1}{\sqrt{2}}.$$

By linearity,

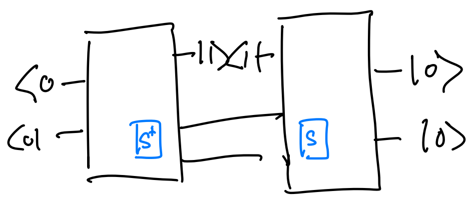


= a



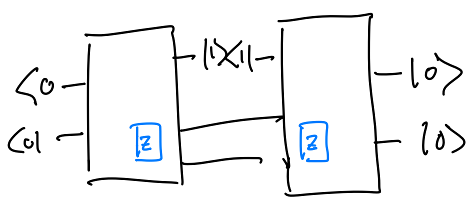
+

b



+

c



Apply this replacement recursively for every pair of T gates.
Yields 3^t calculations each of which was a only Clifford computation. So previous, subroutine gives an efficient poly(n,m) algorithm.

Quantum Complexity Theory

we define BQP - the class of decision problems decidable in poly-time by a family of uniform quantum circuits.

Other complexity classes.

P - decision problems solvable by deterministic classical polynomial time computation

BPP - decision problems solvable by randomized classical polynomial time computation

NP – decision problems solvable by non-deterministic classical polynomial time computation

also known as efficiently verifiable decision problems.

interaction-perspective:

Prover

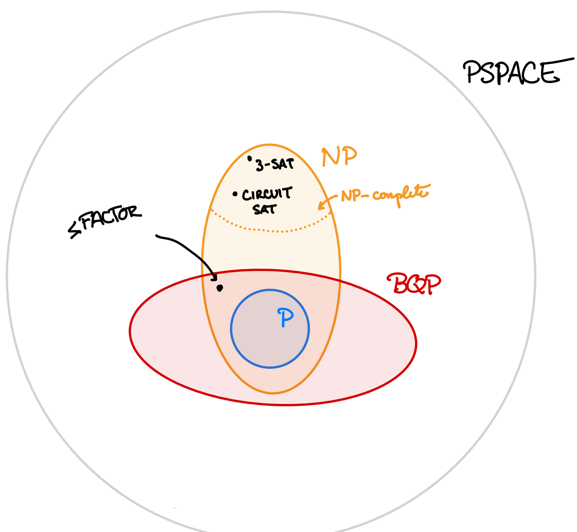
$\downarrow \pi \in \{0,1\}^{poly(n)}$

Verifier

$V(x, \pi)$ poly-time computation.

$x \in \mathcal{L}$ if $\exists\, \pi$ s.t. $V(x,\pi)$ accepts

$x \notin \mathcal{L}$ if $\forall\, \pi$, $V(x,\pi)$ rejects.



$$\leq\text{FACTOR} = \{ \underbrace{(N, K)}_{\text{as binary numbers}} : N \text{ has a factor } \leq K \}.$$

Useful to understand the notion of reductions.

<u>Def</u>. Promise lang $\mathcal{L}$ poly-time reduces to $\mathcal{L}'$ if

$\exists$ a poly-time algorithm $f : \{0,1\}^* \to \{0,1\}^*$ s.t.

(1) $x \in \mathcal{L}_{yes}$ iff $f(x) \in \mathcal{L}'_{yes}$

(2) $x \in \mathcal{L}_{no}$ iff $f(x) \in \mathcal{L}'_{no}$.

<u>Not</u>. $\mathcal{L} \leq \mathcal{L}'$.

"if we can solve $\mathcal{L}'$, then we can solve $\mathcal{L}$". $\mathcal{L}'$ is as hard as $\mathcal{L}$.

<u>Not</u>. A lang $\mathcal{L}'$ is hard for a comp. class C if

$\forall\ \mathcal{L} \in C,\ \mathcal{L} \leq \mathcal{L}'$.

$\mathcal{L}'$ is C-complete if $\mathcal{L}' \in C$ and $\mathcal{L}'$ is C-hard.

<u>Ex</u>. 3-SAT is NP-complete

Traveling Salesman is NP-complete.

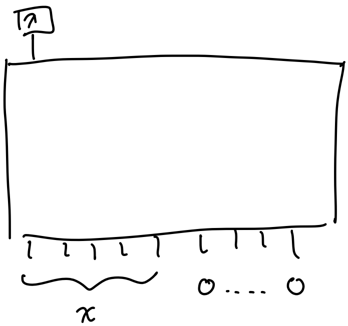
Ex. ($\leq$ FACTOR) $\leq$ ($\leq$ ORDER-FINDING)

Circuit-sat is NP-complete.

Input: $\langle C \rangle \leftarrow$ classical boolean reversible circuit

with some free wires and some fixed ancilla.

Decide if $\exists\, x$ s.t. $C(x)$ accepts.



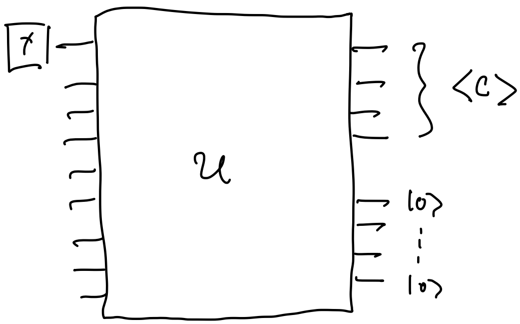
BQP-complete: Input $\langle C \rangle \leftarrow$ quantum circuit

Decide if ① yes: $\| \langle 1 | \otimes \mathbb{1} \, | C | 0^n \rangle \|^2 \geq \frac{2}{3}$

② no: $\_\_\_\_\_\_\_\_ \leq 1/3$.

"Canonical BQP-complete problem".

Containment $\in$ BQP is because of the notion of a universal quantum circuit.



s.t. pr measurement $= 1$ is equal to success prob. of C.

$\Rightarrow$ BQP $\subseteq$ PSPACE as we gave a PSPACE alg for this problem.

$$\mathcal{L}_{a,b} = \left\{ \langle C \rangle \text{ s.t. } \begin{array}{ll} p_C \geq a & (\text{yes}) \\ \text{or } p_C \leq b & (\text{no}) \end{array} \right\}$$

where $\| \langle 1 | C | 0^n \rangle \|^2 =: p_C$.

Claim $\mathcal{L}_{a,b} \in$ BQP for $\epsilon := a - b \geq$

Pf. Use Universal q.c. to run Circuit C T times getting outcomes $X_1, \ldots, X_T$. wlog assume $a \geq \frac{1}{2}$.

if $\langle C \rangle \in \mathcal{L}_{yes}$ (i.e. $p_C \geq a$), then

$\mathbb{E} X_t \geq a$. So $X = \sum X_t$.

$$\Pr\left[\mathbb{E}X \le b\right] = \Pr\left[X \le (aT) - (\epsilon T)\right]$$

$$= \Pr\left[aT - X \ge \epsilon T\right]$$

$$\le \Pr\left[aT - X \ge \epsilon a T\right]$$

$$\le \exp\left(-\frac{\epsilon^2 a T}{3}\right) \le \exp\left(-\frac{\epsilon^2 T}{6}\right)$$

only need error bound of $\le \frac{1}{3}$.

So $T \ge \Omega\left(\frac{1}{\epsilon^2}\right)$.

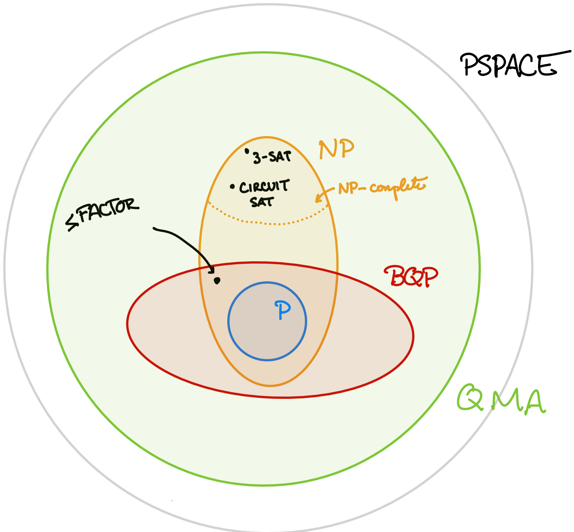
BQP can estimate p_c to accuracy $1/\text{poly}(n)$.

We can also boost success probability to $2^{-p(n)}$ of outputting correct answer by choosing $T \ge \Omega\left(\frac{p(n)}{\epsilon^2}\right)$.

Next: QMA "Quantum Merlin-Arthur"

Easiest to define by complete problem:

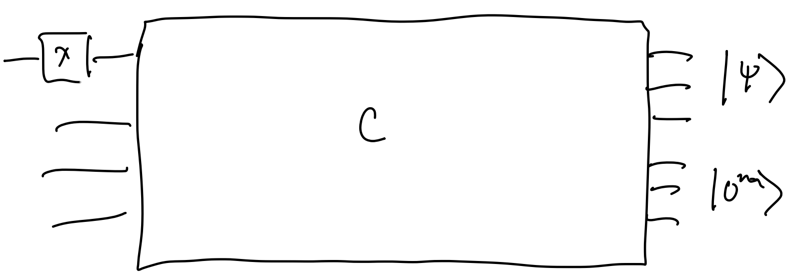
QCIRCUIT-SAT



QCIRCUIT-SAT : $\langle C \rangle$ – q circuit with some inputs fixed to 0.

Decide: if ① $\exists\, |\psi\rangle$ s.t. $\left\| \langle 1 | C | \psi, 0^m \rangle \right\|^2 \geq \frac{2}{3}$

② $\forall\, \underbrace{|\psi\rangle}_{\text{witness}}$ $\left\| \langle 1 | C | \psi, 0^m \rangle \right\|^2 \leq \frac{1}{3}$.



Generalizes circuit-sat & canonical BQP-complete problem.

Notion of non-deterministic q. computation.

Also of interest as it relates to major questions of interest in q. mechanics.

Does QMA have the same error-amplification properties of BQP?

<u>Yes</u>. But it is not as easy as repeat multiple times.

B.c. measurement is perturbative. After running $C(|\psi\rangle, |0^n\rangle)$ the state $|\psi\rangle$ may be destroyed.

Easiest to switch to Prover & Verifier interaction perspective

$$\text{Prover} \xrightarrow{\ |\psi\rangle\ } \text{Verifier}$$

Verifier runs $C(|\psi\rangle|0^n\rangle)$ and measures.

Goal. Come up with a better verifier which accepts with near certainty if $\exists$ an accepting witness and rejects with near certainty if $\nexists$ an accepting witness.

Idea: Have the (honest) prover send $|\psi\rangle^{\otimes T} \in (\mathbb{C}^2)^{\otimes nT}$

Issue: Prover may cheat and send a different entangled state $|\varphi\rangle \in (\mathbb{C}^2)^{\otimes nT}$.

Resolution: One can show that best strategy for the prover is to send an unentangled state

But in fact, $\exists$ a verification algorithm with better acceptance and rejection probabilities that only needs 1 copy.

Requires Jordan's lemma.

The story of a QMA verification circuit C is a tale of two projectors.

$$\Pi_0 = \mathbb{1}_{2^n} \otimes |0\rangle\langle 0|^m$$

$$\Pi_1 = C^\dagger \left(|1\rangle\langle 1| \otimes \mathbb{1}_{2^{n+m-1}} \right) C.$$

$\Pi_0 |\bar{\psi}\rangle = |\bar{\psi}\rangle$ where $|\bar{\psi}\rangle = |\psi\rangle \otimes |0^m\rangle$.

Π_0 checks input has correct ancilla.

Π_1 checks computation + measurement accepts.

<u>Jordan's lemma</u> Given two projectors $A, B \in \mathbb{C}^{D \times D}$, $\exists$ a change of basis s.t. A, B are block-diagonal with 1- or 2-dim blocks.

<u>Pf</u>. Let $|v\rangle$ be λ- eigenvector $(\lambda \neq 0)$ of $A+B$. Then,

$$A|v\rangle + B|v\rangle = \lambda |v\rangle.$$

if $A|v\rangle \in \text{span}(|v\rangle)$, then $B|v\rangle \in \text{span}(|v\rangle)$ and so A and B preserve the block spanned by $|v\rangle$.

if $A|v\rangle \notin \mathrm{span}(|v\rangle)$, then

$$B|v\rangle \in \mathrm{span}\big(A|v\rangle, |v\rangle\big) =: S$$

Then, $A\big(\alpha A|v\rangle + \beta|v\rangle\big) = \alpha A|v\rangle + \beta A|v\rangle \in S.$

& $B\big(\alpha A|v\rangle + \beta|v\rangle\big) = B\Big(\alpha\big(\lambda|v\rangle - B|v\rangle\big) + \beta|v\rangle\Big)$

$$\propto B|v\rangle \in S.$$

So, S is preserved by both A and B. Recursion finishes decomposition.

Applying Jordan's lemma to QMA verifiers.

Decompose Π_0, Π_1 using Jordan's lemma.

<u>Claim</u> Acceptance prob. $= \max_{|\bar{\Psi}\rangle} \| \Pi_1 \Pi_0 |\bar{\Psi}\rangle \|^2$

Pf. when $|\bar{\Psi}\rangle = |\psi\rangle \otimes |0^m\rangle$ for optimal $|\psi\rangle$, then

LHS $\leq$ RHS.

To show LHS $\geq$ RHS, use witness $|\psi\rangle = \Pi_0 |\bar{\Psi}\rangle$. $\boxtimes$

Equiv. acceptance prob $= \lambda_{max}\left(\Pi_0 \Pi_1 \Pi_0 \right)$

needed for Hermiticity.

$\Pi_0 \Pi_1 \Pi_0$ is also block-diagonal

so λ_{max} is max eigenvalue over blocks.

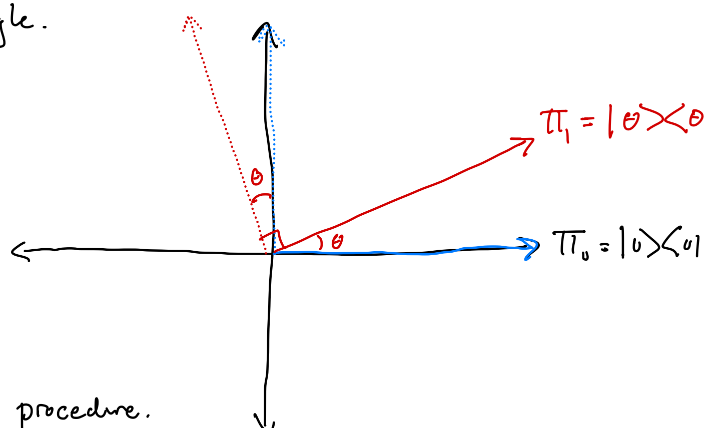
Consider the block of max eigenvalue.

If either Π_0 or $\Pi_1 = \mathbb{1}$, then easy as max eigenvalue $= 1$.

So, $\exists$ a $|\bar{\Psi}\rangle$ s.t. $\Pi_0 \Pi_1 \Pi_0 |\bar{\Psi}\rangle = |\bar{\Psi}\rangle$.

Otherwise, let θ = angle.

$\lambda_{max} = \cos^2 \theta$.



Consider the following procedure.

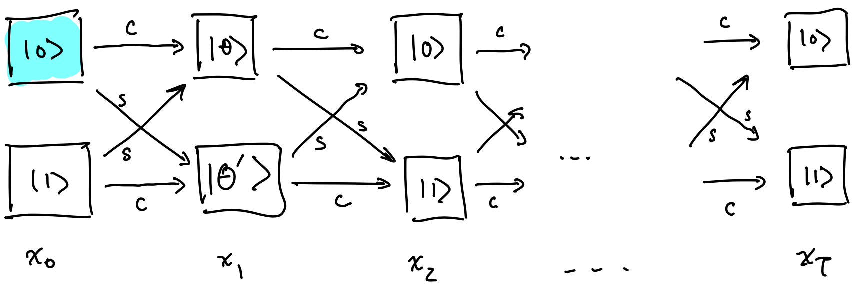
- Start with $|0\rangle$. Set $x_0 = 0$.
- Measure in $\{|\theta\rangle, |\theta + \frac{\pi}{2}\rangle\}$ basis. Set $x_1 = 0$ or 1, respectively.
- Measure in $\{|0\rangle, |1\rangle\}$ basis. Set $x_2 = 0$ or 1, respectively.

— Measure in $\{|\theta\rangle, |\theta + \frac{\pi}{2}\rangle\}$ basis. Set $x_3 = 0$ or 1, respectively.

$\vdots$

— Measure in $\{|0\rangle, |1\rangle\}$ basis. Set $x_T = 0$ or 1, respectively.

$c = \cos^2\theta,\ s = \sin^2\theta \qquad c + s = 1.$



Let $y_t = x_t \oplus x_{t-1}$. Change in t-th step.

$$\mathbb{E}\, y_t = s.$$

Use Chernoff bound argument on y_t to estimate s. And therefore c.

Lifted to original problem.

Algorithm$(|\psi\rangle)$:

(0) Start with $|\bar{\psi}\rangle = |\psi\rangle \otimes |0^m\rangle$. Set $x_0 = 0$.

(1) Apply C. Measure output and record as x_1. Appl $C^\dagger$.

(2) Measure POVM $\{\Pi_0, \mathbb{1} - \Pi_0\}$. Record as x_2.

(Not the same as measuring all ancilla, similar to Grover reflection operator)

(3) Apply C. Measure output and record as x_3. Apply $C^\dagger$.

$\vdots$

(T) Measure POVM $\{\Pi_0, \mathbb{1} - \Pi_0\}$. Record as x_T.

(T+1) Compute $y_t = x_t \oplus x_{t-1}$ for $t = 1, \dots T$.

Accept if $\sum y_t \leq \frac{1}{3} T$.

By Chernoff analysis + Jordan's lemma,

if $\langle C \rangle \in L_{yes}$ and prover gave valid $|\psi\rangle$, then we accept with prob. $1 - \exp\left(-\Omega(T)\right)$.

if $\langle C \rangle \in L_{no}$, $\forall\ |\psi\rangle$, we accept with prob. $\leq \exp\left(-\Omega(T)\right)$.

The local Hamiltonian problem

Why study QMA?

- Quantum generalization of NP
- Has a complete problem that is very interesting for physics.

LH problem:

A k-local Hamiltonian term is a matrix $h_i = h_i^\dagger \in \mathbb{C}^{2^k}$ (wlog $1 \geq h_i \geq 0$) and a site $S_i \subseteq [n]$ with $|S_i| = k$.

The Ham. term can also be seen as $(h_i)_{S_i} \otimes \mathbb{1}_{[n]\setminus S_i}$ as an operator on $(\mathbb{C}^2)^{\otimes n}$.

A k-local Hamiltonian (system) is a collection of k-local Hamiltonian terms and we define

$$H = \sum_{i=1}^{m} h_i \in \mathbb{C}^{2^n \times 2^n}.$$

$\lambda_{min}(H)$ = ground energy.

Problem $(\langle H \rangle, a, b)$:

Decide if $\underbrace{\lambda_{min}(H) \leq a}_{\text{yes}}$ or $\underbrace{\lambda_{min}(H) \geq b}_{\text{No}}$.

Note: $\langle H \rangle$ is the succinct $O\left(m\left(2^k + k \log n\right)\right)$ size description given by describing each h_i.

① LH is a generalization of CSPs.

3-SAT clase $\quad x_1 \vee x_2 \vee \neg x_3 \implies$

$$h_i = \text{diag}\left(0, 0, 0, 0, 0, 0, \underset{\substack{\uparrow \\ (0,0,1) \\ \text{site.}}}{1}, 0\right)$$

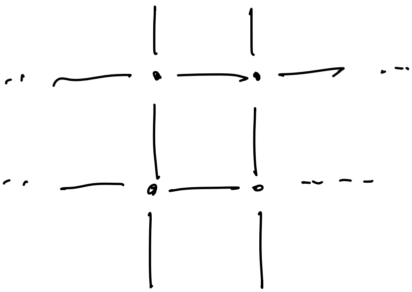
Each term checks a local energy stem.

When h_i are <u>all</u> diagonal, $\lambda_{min}(H)$ occurs at a basis vector.

Corresponds to the classical optimal solution to the CSP.

LHs are the Hermitian generalizations of CSPs.

(2) LHs capture Physical systems of interest:



$$H = -J\left(\sum_{i \sim j} Z_i Z_j + g \sum_j X_j \right)$$

transverse field Ising model.

Describes particle interactions in many-body q. mechanics.

Calculating groundstates of LHs is of critical interest in physics.

Calculating groundenergy is the decision version of the search problem.

<u>Claim</u> LH $\in$ QMA.

Say prover sends you witness $|\psi\rangle \in \mathbb{C}^{2^n}$.

<u>Algorithm</u> $(|\psi\rangle)$:

Pick a random Ham term h_i, acting on S_i.

Write $h_i = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ $\leftarrow$ spectral decomposition

Measure $|\psi\rangle$ with POVM P_i

$$\{ |\psi_j\rangle\langle\psi_j| \}_{S_i} \otimes \mathbb{1}_{-S_i}.$$

For measurement outcome j, accept if $\lambda_j < \frac{b}{m}$.

Proof.

Let's compute the expectation over λ_j output:

By construction, measuring the POVM P_i gives us expected outcome

$$\sum_j \lambda_j \langle\psi| \left(|\psi_j\rangle\langle\psi_j| \otimes \mathbb{1} \right) |\psi\rangle$$

$$= \langle\psi| h_i |\psi\rangle.$$

Expectation over i gives output $\langle\psi| \mathbb{E} h_i |\psi\rangle = \frac{1}{m} \underbrace{\langle\psi|H|\psi\rangle}_{E}.$

Let $X \in [0,1]$ be the outcome of λ_j.

$$\mathbb{E}X = \frac{E}{m}$$

If yes instance: $E \le a$ so $\mathbb{E}X \le \frac{a}{m}$.

If no instance: $E \ge b$ so $\mathbb{E}X \ge \frac{b}{m}$.

Using $X \in [0, I]$, we can show (exercise) that

$$\Pr[\text{accept} \mid \text{yes}] \geq 1 - \frac{a}{m} \quad \text{and} \quad \Pr[\text{accept} \mid \text{no}] \leq 1 - \frac{b}{m}.$$

gap between completeness and soundness $= \dfrac{b-a}{m}$.

Since $m \leq n^k$, as long as $b - a \geq 1/\text{poly}(n)$,

$LH_{a,b}$ is in QMA.

Proving local Hamiltonian is QMA-hard:

Given input circuit $C = g_T \cdots g_1$ acting on n qubit input, m ancilla.

Construct a local Ham H and quantities (a,b),

① $\exists |\psi\rangle$ s.t. $C(|\psi\rangle)$ accepts w pr $\geq 1-\epsilon$,

then $\exists |\varphi\rangle$ s.t. $\langle\varphi|H|\varphi\rangle \leq a$

② $\forall |\psi\rangle$, $C(|\psi\rangle)$ accepts w pr $\leq \epsilon$,

then $\forall |\varphi\rangle$, $\langle\varphi|H|\varphi\rangle \geq b$.

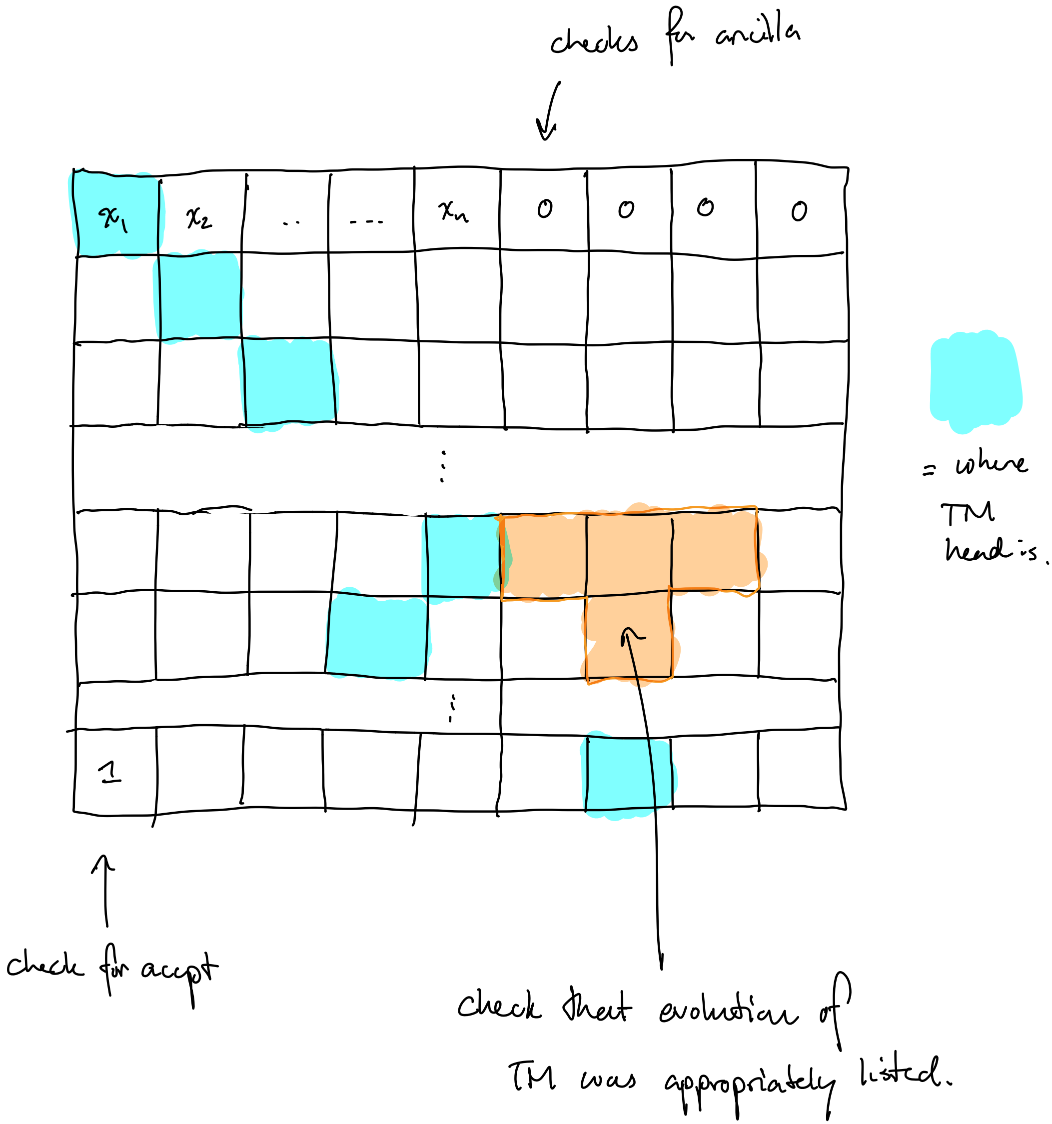
In class, we will only prove that $\underbrace{O(\log n)}_{\sim k}$-LH is QMA-hard.

HW will include problem for proving 5-local hardness.

Quantum analog of the Cook-Levin theorem proving that 3-SAT is NP-complete.

Cook-Levin Tableau Review:

given classical computation of T time steps using total space S, write a $T \cdot S$ tableau with the state of the machine at time t in row t.



Can we construct the same for quantum comp.?

Consider a circuit $C = g_T \cdots g_1$. Can we create a table with rows

$$|\psi_0\rangle = |\psi_{witness}\rangle \otimes |0^m\rangle$$

$$|\psi_1\rangle = g_1|\psi_0\rangle$$

$$|\psi_2\rangle = g_2 g_1|\psi_0\rangle = g_2|\psi_1\rangle$$

$$\vdots$$

$$|\psi_T\rangle = C|\psi_0\rangle.$$

Why does this not work? Local checks cannot verify the evolutions.

<u>Ex</u>. $|\psi_t\rangle = \frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$ and $g_{t+1} = Z_1$.

Then $|\psi_{t+1}\rangle = \frac{|0^n\rangle - |1^n\rangle}{\sqrt{2}}$.

Whereas if $g_{t+1} = \mathbb{1}$, then $|\psi_{t+1}\rangle = \frac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$.

<u>Claim</u> Any $k \leq (n-1)$ reduced density matrix of $\frac{|0^n\rangle \pm |1^n\rangle}{\sqrt{2}}$ is

$$\frac{1}{2}\left(|0^k\rangle\langle 0^k| + |1^k\rangle\langle 1^k|\right).$$

So a check differentiating if $g_{t+1} = Z_1$ vs. $\mathbb{1}$ must be non-local if it can distinguish

$$\underbrace{|\psi_t\rangle \otimes |\psi_{t+1}\rangle}_{g_t = Z_1} \quad \text{from} \quad \underbrace{|\psi_t\rangle \otimes |\psi_t\rangle}_{g_t = \mathbb{1}}$$

We need a better solution that can detect global changes that occur from local gates.

Let's create a $O(\log n)$-local Hamiltonian whose ground states are of the form

$$\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_t\rangle \quad \longleftarrow \text{state register}$$

time register

t expressed in $\lceil \log(T+1) \rceil$ bits

and $|\psi_t\rangle = g_t \cdots g_1 |\psi_0\rangle$ (all related).

In order to write out the Ham. let's first understand

$$h = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes U - |0\rangle\langle 1| \otimes U^\dagger + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$h = \frac{1}{2}\begin{pmatrix} \mathbb{1} & -\mathcal{U}^{\dagger} \\ -\mathcal{U} & \mathbb{1} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -\mathcal{U}^{\dagger} \\ \mathbb{1} \end{pmatrix}\begin{pmatrix} -\mathcal{U} & \mathbb{1} \end{pmatrix}$$

Then $\langle\psi|h|\psi\rangle$ for $h = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle \leftarrow$ unnormalized eqns.

$$\frac{1}{2}\begin{pmatrix} \langle\psi_0| & \langle\psi_1| \end{pmatrix}\begin{pmatrix} \mathbb{1} & -\mathcal{U}^{\dagger} \\ -\mathcal{U} & \mathbb{1} \end{pmatrix}\begin{pmatrix} |\psi_0\rangle \\ |\psi_1\rangle \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} \langle\psi_0| & \langle\psi_1| \end{pmatrix}\begin{pmatrix} |\psi_0\rangle - \mathcal{U}^{\dagger}|\psi_1\rangle \\ -\mathcal{U}|\psi_0\rangle + |\psi_1\rangle \end{pmatrix}$$

$$= \frac{1}{2}\left(\langle\psi_0|\psi_0\rangle - \langle\psi_0|\mathcal{U}^{\dagger}|\psi_1\rangle - \langle\psi_1|\mathcal{U}^{\dagger}|\psi_0\rangle + \langle\psi_1|\psi_1\rangle\right)$$

$$= \frac{1}{2}\left\| |\psi_1\rangle - \mathcal{U}|\psi_0\rangle \right\|^2.$$

h measures distance from states of the form

$$\frac{1}{\sqrt{2}}|0\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle\mathcal{U}|\psi_0\rangle.$$

where $|\psi_0\rangle$ is of norm 1.

Alternate proof of fact:

Let $V = |1\rangle\langle 1| \otimes U + |0\rangle\langle 0| \otimes \mathbb{1}$

$V^\dagger = |1\rangle\langle 1| \otimes U^\dagger + |0\rangle\langle 0| \otimes \mathbb{1}$

$$V^\dagger h V = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes \mathbb{1} - |0\rangle\langle 1| \otimes \mathbb{1} + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$= |-\rangle\langle -| \otimes \mathbb{1}.$$

So groundstates of $V^\dagger h V$ are states of the form

$|+\rangle \otimes |\psi_0\rangle$.

and $V^\dagger h V$ is a projector. So groundstates of h

are states of the form $V|+\rangle \otimes |\psi_0\rangle$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle U|\psi_0\rangle\right).$$

Apply this intuition to general Hamiltonian circuit

$$h_t = \frac{1}{2}\left(|t\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes g_t - |t-1\rangle\langle t| \otimes g_t^\dagger + |t-1\rangle\langle t-1| \otimes \mathbb{1}\right)$$

Each term h_t acts on time register + 2 extra qubits def. by g_t.

Same calculation will tell us that for $|\psi\rangle = \sum_t |t\rangle|\psi_t\rangle$

that

$$\langle\psi|h_t|\psi\rangle = \left\| \,|\psi_t\rangle - g_t|\psi_{t-1}\rangle \right\|^2 .$$

But how do all the pieces act together? Analyze a rotation.

$$V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1$$

$$V^\dagger = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_1^\dagger \cdots g_t^\dagger .$$

$$V^\dagger h_t V = \frac{1}{2}\Big(|t\rangle\langle t| \otimes \mathbb{1} - |t-1\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes \mathbb{1} + |t-1\rangle\langle t-1| \otimes \mathbb{1} \Big)$$

$$= \frac{1}{\sqrt{2}}\big(|t\rangle - |t-1\rangle\big) \frac{1}{\sqrt{2}}\big(\langle t| - \langle t-1|\big) \otimes \mathbb{1} .$$

So, $V^\dagger\left(\sum_{t=1}^{T} h_t\right)V =$

$$\frac{1}{2}\begin{pmatrix} 1 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & \ddots & \ddots & \ddots & & \\ & & \ddots & \ddots & -1 & \\ & & & \ddots & 2 & -1 \\ & & & & -1 & 1 \end{pmatrix} \otimes \mathbb{1} .$$

This is a special matrix. It is the Laplacian of a line graph and also a circulant matrix. (also tri-diagonal)

$\lambda_0 = 0$, eigenvector $|\Psi_0\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_0\rangle$ ← for any $|\psi_0\rangle$

$\lambda_1 \geq \frac{c}{T^2}$ ← exercise / intuition from graph mixing time.

So, removing rotation by V:

$H_{prop} = \sum_{t=0}^{T} h_t$ is a Hamiltonian with

ground-energy $= 0$, groundstates of the form $\underbrace{\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi_0\rangle}_{\text{known as a history state}}$

for any state $|\psi_0\rangle$

highly degenerate groundspace.

and first non-zero energy of $\geq c/T^2$.

Therefore, $H_{prop} \geq \frac{c}{T^2}(\mathbb{1} - \Pi_{prop})$

Projector onto span of history states

Next: Adding checks for ancilla and output and computing overall eigenvalues to make sure cheating provers are detected.

History states just check evolution of the computation

To check output of computation, we want a term that checks that when the time register is set to T, the first qubit is in the $|1\rangle$ state.

$$H_{out} = |T\rangle\langle T|_{time} \otimes |0\rangle\langle 0|_1$$

Penalizes being time T and first qubit = 0.

To check input, we need to make sure that all the ancilla registers of the computation were set to $|0\rangle$.

$$H_{in} = \sum_{j=1}^{m} |0\rangle\langle 0|_{time} \otimes |1\rangle\langle 1|_{ancilla(j)}$$

$H_{out} + H_{in}$ is a commuting Hamiltonian meaning every pair of local terms commute.

Each local term is a projector. So $H_{out} + H_{in}$ has an integer spectrum.

$$H_{out} + H_{in} \geq \left(\mathbb{1} - \Pi_{inout}\right)$$

projector onto passing all in & out checks.

<u>Claim</u> $H = H_{prop} + H_{out} + H_{in}$ suffices as a Ham.

Intuition: Let $|\psi\rangle = \sum_{t=0}^{T} |t\rangle|\varphi_t\rangle$ unnormalized.

so $\||\psi\rangle\| = 1 \Rightarrow \sum_{t=0}^{T} \||\varphi_t\rangle\|^2$

h_t gives energy $\||\varphi_t\rangle - g_t|\varphi_{t-1}\rangle\|^2$

H_{in} gives energy $\sum_{j=1}^{m} \|\langle 1|_{ancilla(j)}|\varphi_0\rangle\|^2$

H_{out} gives energy $\|\langle 0|_1 |\varphi_T\rangle\|^2$

Recall $V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1$.

Let $|\mu\rangle = V^{\dagger}|\psi\rangle = \sum_t |t\rangle|\mu_t\rangle$

where $|\mu_t\rangle = g_1^{\dagger} \cdots g_t^{\dagger} |\psi_t\rangle$.

Then

h_t gives energy $\| |\mu_t\rangle - |\mu_{t-1}\rangle \|^2$

H_{in} gives energy $\sum_{j=1}^{m} \| \langle 1|_{\text{ancilla}(j)} |\mu_0\rangle \|^2$

H_{out} gives energy $\| \langle 0|_1 C |\mu_T\rangle \|^2$

If satisfiable then $\exists$ good choice $|\mu\rangle$ for all $|\mu_0\rangle \ldots |\mu_T\rangle$.

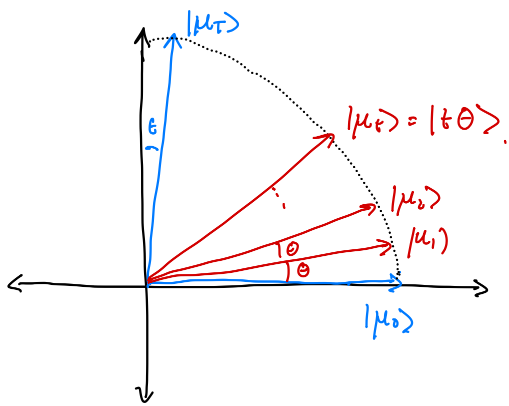
When unsatisfiable, in order for H_{in} and H_{out} energy to be small... $|\mu_0\rangle$ and $|\mu_T\rangle$ are orthogonal.

For intuition only: The following is not the lowest energy state.

Cartoon: $|\mu_0\rangle = |0\rangle$ and $|\mu_1\rangle \approx |1\rangle$ in some 2D space

(can be formal due to Jordan's lemma)

Then ideal $|\mu_t\rangle$ would be $|t\theta\rangle$ for $\theta = \frac{\pi}{2T}$ to minimize H_{prop} energy.



Then $\langle\psi|H|\psi\rangle$

$$= \langle\mu|V^\dagger H V|\mu\rangle$$

$$\leq \langle\mu|V^\dagger h_t V|\mu\rangle$$

$$= T \cdot \sin^2\theta$$

$$= O\left(\frac{1}{T}\right).$$

We will prove a lower bound of $\Omega\left(\frac{1}{T^3}\right)$ in the next class.