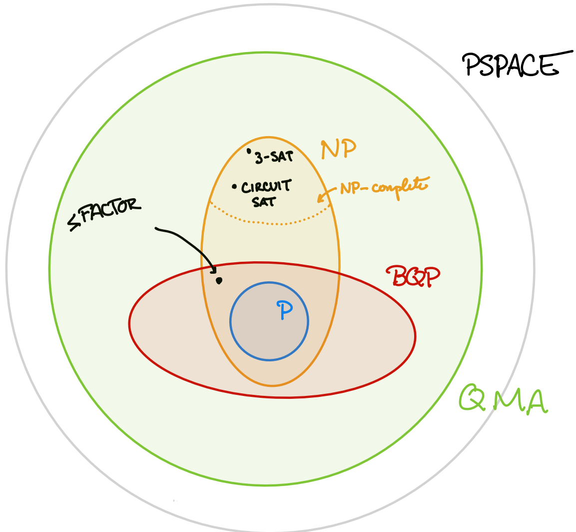
Lecture 16

Nov 17, 2025

Next: QMA "Quantum Merlin-Arthur"

Easiest to define by complete problem:

QCIRCUIT-SAT

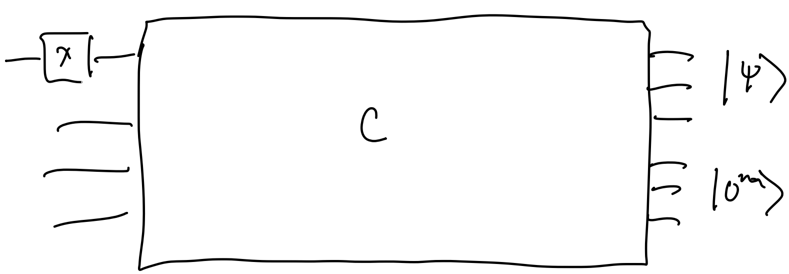


QCIRCUIT-SAT : $\langle C \rangle$ - q circuit with some inputs fixed to 0.

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

② $\forall\, |\psi\rangle$ $\| \langle 1 | C | \psi, 0^m \rangle \|^2 \leq \frac{1}{3}$.

witness



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 $C(|\psi\rangle, |0^m\rangle)$ the state $|\psi\rangle$ may be destroyed.

Easiest to switch to Prover & Verifier interaction perspective

Prover

$$\Big\downarrow |\psi\rangle$$

Verifier runs $C(|\psi\rangle|0^m\rangle)$
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 $A|v\rangle \in \mathrm{span}(|v\rangle)$, then $B|v\rangle \in \mathrm{span}(|v\rangle)$ and so

A and B preserve the block spanned by $|v\rangle$.

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

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

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

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

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

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. $= \max\limits_{|\bar{\Psi}\rangle} \| \Pi_1 \Pi_0 |\bar{\Psi}\rangle \|^2$

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.

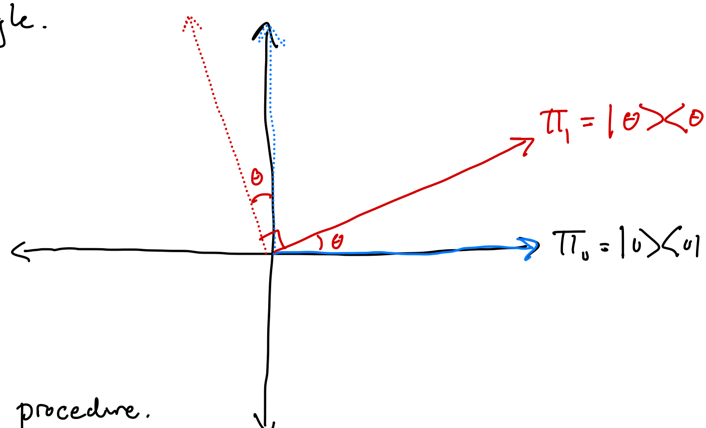
Consider the block of max eigenvalue.

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

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

Otherwise, let θ = angle.

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



Consider the following procedure.

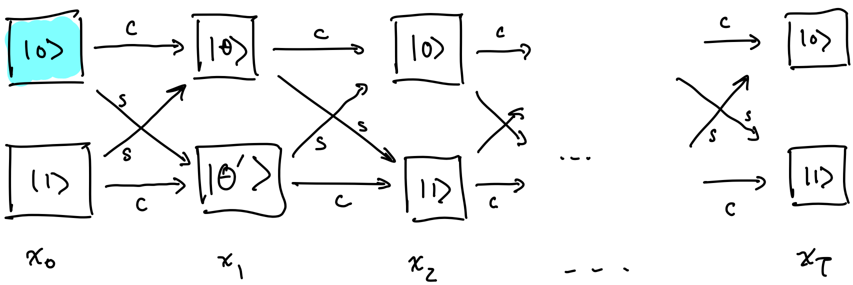
- Start with $|0\rangle$. Set $x_0 = 0$.
- Measure in $\{|\theta\rangle, |\theta + \frac{\pi}{2}\rangle\}$ basis. Set $x_1 = 0$ or 1, respectively.
- Measure in $\{|0\rangle, |1\rangle\}$ basis. Set $x_2 = 0$ or 1, respectively.

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

⋮

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

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



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 clause $x_1 \vee x_2 \vee \neg x_3 \implies$

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

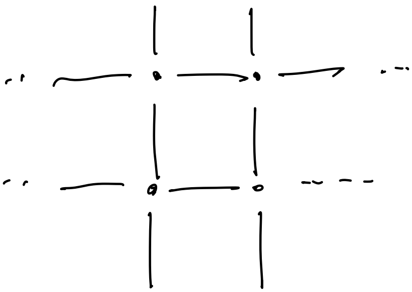
Each term checks a local energy stem.

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: $E \leq a$ so $\mathbb{E}X \leq \frac{a}{m}$.

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

Using $X \in [0,1]$, 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 $b - a \geq 1/\mathrm{poly}(n)$,

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