In order to compare problems & resources, we need a common language to describe problems.

Language: \( L \subseteq \{0,1\}^* \) (a language is a subset of the set of all binary strings)

Let \( f = \{f_n\}_{n=1}^\infty \) be a family of Boolean formulas

\[ f_n: \{0,1\}^n \to \{0,1\}. \text{ Then } x \in L_f \text{ if } f_n(x) = 1 \text{ for } x \in \{0,1\}^n \]

\( x \in L \) if \( x \) has a factor \( \leq K \)

Questions?

What is a language that corresponds to the problem of eigenvalue estimation?

Divide input \( x \) into 2 halves \( \rightarrow x \) \begin{tabular}{|c|c|}
\hline
\end{tabular} \text{ then } x \in L \text{ if } U(x) e^{i\lambda_1} = e^{i\lambda_1} x \]

description of a circuit that creates a unitary \( U \) description of a circuit that creates a state \( |\psi\rangle \)
Complexity Class: a set of languages.

**def:** \( L \subseteq P \) if for any input \( x \in \{0,1\}^* \), \( \exists \) a polynomial time classical algorithm \( A \) s.t. \( A(x) \) accepts iff \( x \in L \).

If input \( x \) has length \( n \), the time \(< c_0 n^{c_1} \) for constants \( c_0, c_1 \).

\( P \sim \) polynomial time

**def:** \( L \subseteq NP \) if for any input \( x \in \{0,1\}^* \), \( \exists \) a polynomial time classical algorithm \( A \) s.t.

- If \( x \in L \) \( \exists \) a string \( y \) s.t. \( A(x,y) \) accepts
- If \( x \not\in L \) for all strings \( y \), \( A(x,y) \) rejects

"witness" \( NP \sim \) non-deterministic polynomial time

Quantum version of \( P \):

**def:** \( L \subseteq BQP \) if for any input \( x \in \{0,1\}^* \), \( \exists \) a polynomial time quantum algorithm \( A \):

- If \( x \in L \), \( A(|x\rangle) \) accepts w/prob \( > \frac{2}{3} \)
- If \( x \not\in L \), \( A(|x\rangle) \) accepts w/prob \( < \frac{1}{3} \)

\( BQP \sim \) bounded error quantum polynomial time

Questions

What is the quantum version of \( NP \)?

\(|x\rangle \) is computational basis state. Circuit: \( |x\rangle \rightarrow U_A |y\rangle \rightarrow D \)
**def** Let $\text{QMA}$ if for any $x \in \{0,1\}^*$ there exists a polynomial-time quantum algorithm $A$ such that:

- If $x \in L$, there exists a state $|\psi\rangle$ such that $A(|x\rangle, |\psi\rangle)$ accepts with probability $\geq \frac{2}{3}$.
- If $x \notin L$, $A$ accepts $|\psi\rangle$ with probability $< \frac{1}{3}$.

$QMA \approx$ quantum Merlin Arthur (Merlin sends $|\psi\rangle$ to Arthur, who has a quantum computer)

<table>
<thead>
<tr>
<th>Class</th>
<th>Input State</th>
<th>Success Prob</th>
</tr>
</thead>
<tbody>
<tr>
<td>$QMA$</td>
<td>$</td>
<td>\psi\rangle$</td>
</tr>
<tr>
<td>QCMA</td>
<td>$</td>
<td>\psi\rangle$ (standard basis state)</td>
</tr>
<tr>
<td>$QMA_L$</td>
<td>$</td>
<td>\psi\rangle$</td>
</tr>
<tr>
<td>$QMA(2)$</td>
<td>$</td>
<td>\psi_1\rangle</td>
</tr>
<tr>
<td>QCMA$_L$</td>
<td>$</td>
<td>\psi\rangle$ (standard basis state)</td>
</tr>
</tbody>
</table>
Complete Problems:

**Def:** A language $L$ is complete for a complexity class $C$ if $L \in C$ and also $L$ is $C$-hard.

**Def:** $L$ is $C$-hard if for every $L' \in C$, $\exists$ a polynomial time algorithm to convert input $x' \rightarrow$ string $x$ s.t. $x \in L$ iff $x' \in L'$.

Why are complete problems important? Allow us to relate a specific problem to a specific resource.

**Ex:** Let $x \in \{0,1\}^*$ describe a classical circuit $\chi_x$.
Let $x \in L_x$ if $\chi_x(0...0)$ accepts.

$A_x$ is $P$-complete

$A_x \in P$ $\implies$ $L_x \in P$ $\implies$ $L_x$ is $P$-hard b/c any other language in $P$ has a poly time circuit to decide it, so encode that circuit as $A_x$ with pre-circuit to encode input $x$.

(If familiar with complexity, try to think of a complete problem for $BQP$)
**Thm:** k-local Hamiltonian problem is QMA-Complete [Kitaev]

A Hamiltonian \( H \) has form \( \sum \lambda_i |\psi_i \rangle \langle \psi_i| \).

\( \lambda_i \) real orthonormal basis \( |\psi_i \rangle \) s.t. \( \lambda_i \leq \lambda_j \ \forall \ j \) is called "groundstate".

**def:** [k-local Hamiltonian problem] Let a Hamiltonian \( H = \sum H_j \)

act on \( n \) qubits, where \( H_j \) are Hamiltonians acting non-trivially

on at most \( k \) qubits. Let \( \lambda \) be the smallest eigenvalue of \( H \), and let \( a, b \in \mathbb{R} : a < b, b - a \geq \frac{1}{\text{poly}(n)} \).

Then the problem is to determine if \( \lambda \leq a \) ("accept")
or \( \lambda > b \), promised one is the case.