Proof: Define $|\alpha_k\rangle = (\alpha_{1k}, \alpha_{2k}, \dots, \alpha_{2^n k})$, $|\beta_k\rangle = (\beta_{1k}, \beta_{2k}, \dots, \beta_{2^n k})$.

So we can write: $P = \sum_{k=1}^{2^{2q-2}} |\alpha_k\rangle\langle\beta_k|$. Then:

$$\|P\|_{tr} = \left\| \sum_{k=1}^{2^{2q-2}} |\alpha_k\rangle \cdot \langle\beta_k| \right\|_{tr} = \sum_{k=1}^{2^{2q-2}} \| |\alpha_k\rangle \| \cdot \| |\beta_k\rangle \| \le \sum_{k=1}^{2^{2q-2}} \sqrt{2^n} \cdot \sqrt{2^n} = 2^{2q-2} \cdot 2^n$$

Taking log on both sides proves the corollary. □

Quantum Complexity

Def.: A language L is said to be in NP if exists verifier $V(x, \underset{\text{witness}}{y})$ such that if $x \in L \Rightarrow \exists y_0 \rightarrow V(x, y_0)$ accepts and if $x \notin L$ $\forall y \rightarrow V(x,y)$ rejects.

Def.: A language L is said to be in MA (Merlin & Arthur) if exists a randomized verifier $V(x,y)$ such that:

$x \in L \Rightarrow \exists y_0 \rightarrow \Pr[V(x,y_0) \text{ accepts}] \ge \frac{2}{3}$

$x \notin L \Rightarrow \forall y \rightarrow \Pr[V(x,y) \text{ accepts}] \le \frac{1}{3}$

Remark: It is obvious we can amplify the probabilities $2/3$ and $1/3$ to be exponentially close to 1,0 (respectively) by running V several times.

Def.: MA_1 – MA with one-sided error, that is $x \in L \Rightarrow \exists y_0 \rightarrow V(x, y_0) = \text{accepts}$

$x \notin L \Rightarrow \forall y \rightarrow \Pr[V(x,y) \text{ accepts}] \le \frac{1}{3}$

Remark: $MA_1 = MA$

Def: A language L is said to be in QMA if ~~thiste~~ is (efficiently generated) a family of quantum circuits V_n, $n = 1, 2, \dots$, such that V_n runs on input $\underset{\text{input}}{|x\rangle} \underset{\text{witness}}{|\psi\rangle} \underset{\text{auxiliary qubits}}{|0^k\rangle}$, $|x| = n$ and:

$|\psi| = poly(n)$, $k = poly(n)$

$x \in L \Rightarrow \exists |\psi_0\rangle$ s.t $\text{Prob}[V_n(x, \psi_0) \text{ accepts}] \ge 2/3$

$x \notin L \Rightarrow \forall |\psi\rangle$ $\text{Prob}[V_n(x, \psi) \text{ accepts}] \le \frac{1}{3}$

Def: QMA_1 – QMA with one sided error (as in MA_1).

Remark: Whether $QMA_1 = QMA$ or not is an open question.

Def: QCMA – class of languages with classical witness, quantum verifier.

Remark

$$NP \subseteq MA \subseteq \begin{array}{c} QCMA \subseteq \\ QMA_1 \subseteq \end{array} QMA$$

Def.: The language k-QSAT:

- There are n qubits $|\ell_1\rangle, \dots, |\ell_n\rangle$
- $M = \text{poly}(n)$ k-local projections $Q_i = \hat{Q}_i \otimes \mathbb{1}$ (k-qubits)

$|\psi\rangle$ satisfies $Q_i \iff Q_i|\psi\rangle = 0$

- Is there a state $|\psi\rangle$ that satisfies all Q_i's?

(Is the intersection of all null spaces $\neq \emptyset$)

Remark: This is a generalization of the classical k-SAT - we can describe constraints on classical variables - clauses - as k-local projections.

Example: $C_i = (X_k \vee \overline{X_\ell} \vee X_m)$. All satisfied, except $(0,1,0)$.

We will define a projection: $Q_i = |010\rangle\langle 010|$.

$|\psi\rangle$ satisfies $Q_i \iff Q_i|\psi\rangle = 0 \iff \langle\psi|Q_i|\psi\rangle = 0$

So: $|\psi\rangle$ satisfies $Q_i \; \forall i \iff \sum_i \langle\psi|Q_i|\psi\rangle = 0 \iff \langle\psi|\sum_i Q_i|\psi\rangle = 0$

$H = \sum_i Q_i$ is called a Hamiltonian, or Energy operator.

So we can redefine k-QSAT: Is there a state $|\psi\rangle$ s.t. $\langle\psi|H|\psi\rangle = 0$

$\iff$ The minimal eigenvalue of H, $\lambda(H)$ is 0. $\lambda(H)$ is also called (because of physical applications) Ground Energy.

Def.: k-QSAT problem: Given k-local QSAT system: $H = \sum_{i=1}^{M} Q_i$ ($M = \text{poly}(n)$)

We are promised that either: $-\ \lambda(H) = 0$ or $-\ \lambda(H) \geq b \geq \frac{1}{\text{poly}(n)}$

Decide which case is true.

Def.: k-local Hamiltonian problem: Given $H = \sum_{i=1}^{M} H_i$, $M = \text{poly}(n)$, H_i - k-local Hermitian operator, and given a, b, such that $b - a \geq \frac{1}{\text{poly}(n)}$, $\|H_i\| \leq K \sim O(1)$.

We are promised either $\lambda(H) \leq a$ or $\lambda(H) \geq b$.

Decide whether $\lambda(H) \leq a$ ("Yes-instance") or $\lambda(H) \geq b$ ("No-instance").

Theorem: (Kitaev 2000, "Quatum Cook-Levin") The k-LH problem for $k=5$ is QMA - complete.

Remark: We will first prove for $k = \log(n)$. There are impovements, for example one can put $k=2$

Proof:

k-LH$\in$QMA: Recall: $\langle\psi|H|\psi\rangle \geq \lambda(H)$. Assume WLOG H_i is positive (eigenvalues are positive) $\left(\begin{array}{l} H_i \leftarrow H_i + c_i \\ a \leftarrow a + \sum c_i \\ b \leftarrow b + \sum c_i \end{array}\right)$

H_i is Hermitian, so we can write: $H_i = \sum_\alpha \underset{\text{eigenvalue}}{\lambda_{i,\alpha}} \cdot \underset{\text{projection into the eigenspace of } \lambda_{i\alpha}}{P_{i,\alpha}}$.

We can do this classically, since H_i are small (k-local, k is small).

The total number of eigenvalues : # of $\lambda_{\alpha,i} \leq M \cdot 2^k = \text{poly}(n)$.

So we can compute $S = \sum_{\alpha,i} \lambda_{\alpha,i}$

$\frac{1}{S}\langle\psi|H|\psi\rangle = \sum_{i\alpha} \frac{\lambda_{i,\alpha}}{S} \langle\psi|P_{i\alpha}|\psi\rangle$. Denote $q_{i,\alpha} = \frac{\lambda_{i,\alpha}}{S}$

- Choose (i,α) according to probabilities $q_{i,\alpha}$.
- Then measure $P_{i,\alpha}$. We'll get 0 or 1.

The probability of getting 1 is $\mu = \frac{1}{S}\langle\psi|H|\psi\rangle$. So we want to decide either $\mu \geq \frac{b}{S}$ or $\mu \leq \frac{a}{S}$. Merlin will provide us with $|\psi\rangle$ (m copies), and we will approximate μ with:

Lemma (Chernoff - Hoelfding bound): Let $X_1, \dots, X_m$ be independent random variables over $\{0,1\}$, $\mu = \frac{1}{m}\sum_i \mathbb{E}(X_i)$. Then for every $\delta < \mu$ $\Pr(|X-\mu| > \delta) \leq e^{-2m\mu\cdot\delta^2}$ where $X = \frac{1}{m}\sum_i X_i$

k-LH $\in$ QMA-hard : Say we are given a verifier V to a language $L \in$ QMA.

Assume WLOG: - On input x, the verifier works as $V_x(|\psi\rangle, |0^k\rangle)$ (only needs x)

- V_x is made of 2-local gates (we can appoximate any unitary with 2-local gates)
- If $x \in L$: $\Pr(V_x(|\psi_0\rangle) \text{ accepts}) \geq 1 - 2^{-n} = 1 - \varepsilon$
- If $x \notin L$ $\Pr(V_x(|\psi\rangle) \text{ accepts}) \leq 2^{-n} = \varepsilon$

We work on register: $\underbrace{|\psi\rangle}_{\substack{n \text{ qubits} \\ \text{witness}}} \underbrace{|0^k\rangle}_{\substack{k \text{ qubits} \\ \text{auxiliary}}} \underbrace{|j\rangle}_{\substack{\log(n) \text{ qubits} \\ \text{clock}}}$

We will define a Hamiltonian: $H = H_{in} + H_{prop} + H_{out}$

H_{in}: check ancillas at $t=0$; H_{prop}: verify propogation; H_{out}: verify output

Write: $V_x = U_T U_{T-1} \dots U_1$. $U_j U_{j-1} \dots U_1 |\psi_0\rangle = |\psi_j\rangle$, $|\psi_0\rangle = |\psi\rangle \otimes |0^k\rangle$.

$\Rightarrow |\psi_j\rangle = |\psi\rangle \otimes |\varphi_j\rangle$

We want our Hamiltonian to verify the state: $\frac{1}{\sqrt{T+1}} \cancel{|\psi\rangle \otimes} \sum_{t=0}^{T} |\psi_t\rangle \otimes |t\rangle = |\varphi\rangle$ $(**)$

$H_{in} = \underbrace{|0\rangle\langle 0|}_{clock} \otimes \underbrace{|1\rangle\langle 1|}_{1st\ qubit} \otimes \mathbb{1}_{rest} + \underbrace{|0\rangle\langle 0|}_{clock} \otimes \underbrace{|1\rangle\langle 1|}_{2nd\ qubit} \otimes \mathbb{1}_{rest} + \dots$

A total of k projections. Verifies at $t=0$: $|\psi\rangle|0^k\rangle|0\rangle_{clock}$

$H_{prop} = \sum_{t=1}^{T} H_t$, H_t verifies propogation between time $t-1$ and t.

$H_t = \frac{1}{2}\left(\underbrace{|t\rangle\langle t|}_{clock} + \underbrace{|t-1\rangle\langle t-1|}_{clock} - U_t \otimes |t\rangle\langle t-1| - U_t^{\dagger} |t-1\rangle\langle t|\right)$

(notice: $|\psi_t\rangle|t\rangle + |\psi_{t-1}\rangle|t-1\rangle$ satisfies H_t).

$H_{out} = |0\rangle\langle 0| \otimes \underbrace{|T\rangle\langle T|}_{clock}$ (verifies output is 1).

<u>Completeness</u>: In Yes instance, Merlin sends $|\varphi\rangle$. (from $(**)$)

$\langle\varphi|H_{in}|\varphi\rangle = 0$, $\langle\varphi|H_{prop}|\varphi\rangle = 0$, ~~$\langle\varphi|H_{out}|\varphi\rangle =$~~

$\langle\varphi|H_{out}|\varphi\rangle = \frac{1}{T+1} \underbrace{\langle T|\langle\psi_T|P|\psi_T\rangle|T\rangle}_{\text{chance of failure (in a Yes instance)}} \leq \frac{\varepsilon}{T+1}$

$\rightarrow \langle\varphi|H|\varphi\rangle \leq \frac{\varepsilon}{T+1}$

So choose $a = \frac{\varepsilon}{T+1}$. Similarly (computation is ommited), choose $b = \frac{1}{(T+1)^3}$

We get a reduction from any $L \in QMA$ to $k\text{-}LH\left(H_{in} + H_{prop} + H_{out}, \frac{\varepsilon}{T+1}, \frac{1}{(T+1)^3}\right)$.

□

<u>Remark</u>: In order to combute b, such that $\langle\varphi|H_{in} + H_{prop} + H_{out}|\varphi\rangle \geq b$, where we are in a No-instance, we have to use the so-called <u>Geometrical Lemma</u>, ~~thats~~ which is providing a lower bound for $\lambda(H_1 + H_2)$.