Lecture 18

31 MAR 2014

Focus on the complexity class QMA.

Quantum Merlin-Arthur

Formalizes the idea of a quantum proof

- a quantum state that plays the role of a certificate to a quantum computer that functions as a verification procedure.

Several interesting problems known to be QMA-complete or in QMA (but not in NP).

Definition: Let $A = (A_{yes}, A_{no})$ be a promise problem, let p be a poly-bounded function, & let $a, b : \mathbb{N} \to [0,1]$ be poly-time computable functions. Then $A \in QMA_p(a,b)$ iff $\exists$ a poly-time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$ where each Q_n accepts $n + p(n)$ input qubits & produces one output qubit, such that

1. Completeness: For all $x \in A_{yes}$, $\exists$ a $p(|x|)$-qubit state $|\psi\rangle$ such that

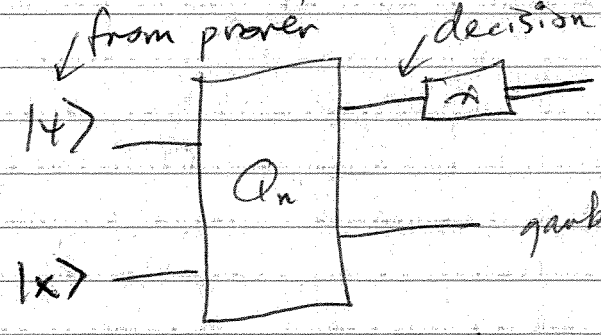
$$\Pr[\text{accept } (x,\psi)] = \left\| (\langle 1| \otimes I)\, Q_n\, |\psi\rangle |x\rangle \right\|_2^2 \geq a(|x|)$$

2. Soundness: For all $x \in A_{yes}$ & all $p(|x|)$-qubit states $|\psi\rangle$

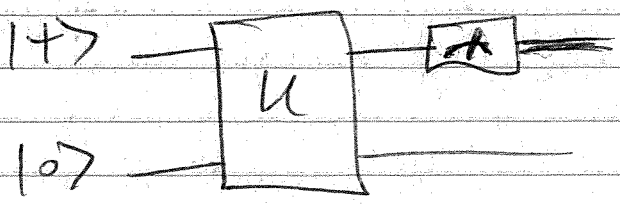
$$\left\| (\langle 1| \otimes I)\, Q_n\, |\psi\rangle |x\rangle \right\|_2^2 \leq b(|x|)$$

$$QMA = \bigcup_p QMA_p(2/3, 1/3)$$

Just picture this as



can think of it more simply as



Example of a problem not known to be in NP but in QMA:

Group Non-membership

Preliminary

Let G be a finite group whose elements can be represented uniquely by binary strings of a given length n.

Assume we can do multiplication & inverse efficiently

$$|g\rangle|h\rangle \to |g\rangle|gh\rangle$$

$$|g\rangle \to |g^{-1}\rangle$$

For example, could be $m \times m$ invertible matrices w/ entries in $\{0, \ldots, p-1\}$ for prime p w/ arithmetic mod p.

Group non-membership

Input: group elements $g_1, \ldots, g_k$ & h of G

Decide

1) $h \notin \langle g_1, \ldots, g_k \rangle$

2) $h \in \langle g_1, \ldots, g_k \rangle$

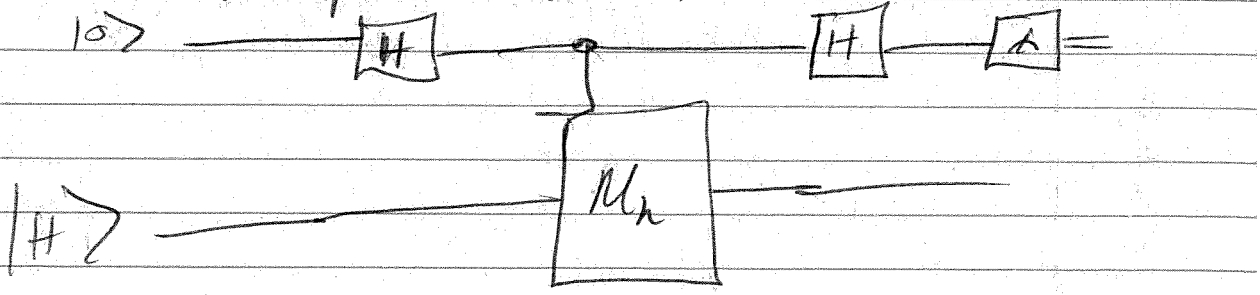
Simple idea to show this:

for $H = \langle g_1, \ldots, g_k \rangle$,
the quantum proof that $h \notin H$ is the state

$$|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{a \in H} |a\rangle$$

↑ state is hard to make for non-abelian groups

Quantum algorithm to put this in QMA is like phase estimation:



$C\text{-}M_h |0\rangle|a\rangle \rightarrow |0\rangle|a\rangle$

$C\text{-}M_h |1\rangle|a\rangle \rightarrow |1\rangle|h \cdot a\rangle$

Consider the case 2) where $h \in H$

Given that $h \in H$, we have

$$M_h|H\rangle = |h \cdot H\rangle = |H\rangle$$

so controlled multiplication has no effect.

$\Rightarrow$ measurement will result in

$|0\rangle$ w/ certainty

Now consider the case 1) where $h \notin H$

then $M_h|H\rangle = |hH\rangle$ which is orthogonal to $|H\rangle$

So evolution is

$$|0\rangle|H\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|H\rangle + |1\rangle|H\rangle\right)$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|H\rangle + |1\rangle|hH\rangle\right)$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(|+\rangle|H\rangle + |-\rangle|hH\rangle\right)$$

$$= \frac{1}{2}\left(\left(|0\rangle+|1\rangle\right)\left(|H\rangle\right) + \left(|0\rangle-|1\rangle\right)\left(|hH\rangle\right)\right)$$

$$= \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|H\rangle+|hH\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|H\rangle-|hH\rangle}{\sqrt{2}}\right)$$

Since $\frac{|H\rangle+|hH\rangle}{\sqrt{2}} \perp \frac{|H\rangle-|hH\rangle}{\sqrt{2}}$

are orthogonal,

outcome of measurement is a random bit.

Do this a few times & can conclude w/ enough statistical evidence that

$h \notin H$.

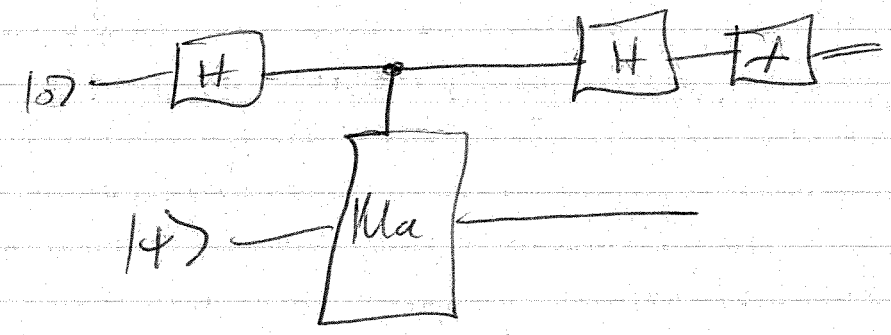
Problem needing to be resolved:

For case 2) the prover does not need to send the state $|H\rangle$ — we can actually send any state.

Idea to resolve this: Pick an element a of H at random & run test for this state

If it fails, then we reject b/c proof is bad.

After running one of these tests, if it passes, the state becomes



$$\alpha\,|\psi\rangle + M_a|\psi\rangle$$

After repeating w/ $a_1, \ldots, a_k$ the state becomes close to

$$\sum_{a \in H} M_a|\psi\rangle$$

This state will then be good for a membership test.

So this puts group non-membership in QMA (idea is very quantum)

Error Reduction for QMA

We defined QMA to be

$$\bigcup_p QMA_p(2/3, 1/3)$$ (could call this $QMA(2/3, 1/3)$)

but we would like to show that

$$QMA(2/3, 1/3) \subseteq QMA(1-2^{-r}, 2^{-r})$$

for every $r \in poly$

Idea to show this:

Let $a(n) - b(n) \geq \frac{1}{q(n)}$ for $q \in poly$

In the case of a YES instance,
$\exists$ a state $|\psi\rangle$ that prover can supply to verifier such that

$$Pr\{accept\} \geq a(n)$$

So prover can supply many copies of this & verifier accepts if the # of acceptances is larger than $\frac{a+b}{2}$

Recall Chernoff bound:

Prob for getting $\geq pk$ "heads" in k coin tosses, where each trial has success prob. p^* is

$$\Pr\{\geq pk \text{ heads}\} \leq \sum_{j \geq pk} \binom{k}{j} p^{*j} (1-p^*)^{k-j}$$

$$\Pr\{\geq pk \text{ heads}\} \leq \exp\{-2(p-p^*)^2 k\}$$

if $p > p^*$

$$\Pr\{\geq pk \text{ heads}\} \geq 1 - \exp\{-2(p-p^*)^2 k\}$$

if $p < p^*$

By setting threshold as $\frac{a+b}{2}$, we find that

$$p^* - p = a - \left(\frac{a+b}{2}\right) = \frac{a-b}{2} = \frac{1}{\text{poly}(n)}$$

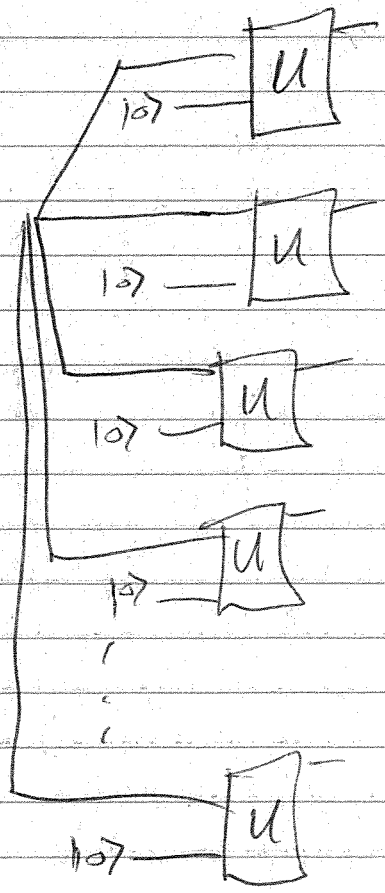
We can have $k \in poly(n)$

+ get acceptance probability

$$\geq 1 - 2^{-nr}$$

for $r \in poly$

For NO instances, prover can entangle the witness state in an attempt to make the verifier accept when he should not. So picture could look like this:



However, we know from QM that tracing over all other systems besides 1st leaves a density operator on 1st, which itself is a convex combination of pure states. And all of these have acceptance prob. $\leq b(n)$

So we can think of each test as being run sequentially, w/ all of them having success prob. $\leq b(n)$

Since $\frac{a(n)+b(n)}{2} > b(n)$

$$p - p^* = \frac{a(n)+b(n)}{2} - b(n)$$

$$= \frac{a(n)-b(n)}{2} \cdot \frac{1}{poly}$$

we can make this prob. $\leq 2^{-nr}$

for $r \in poly$ by choosing $k \in poly$