LECTURE 18 (March 24th)

TODAY QMA(2)

RECAP Def $L \in QMA(2)$ if $\exists$ verifier s.t.

- if $x \in L \Rightarrow \exists$ a proof $|\pi\rangle \otimes |\psi\rangle$ s.t. Verifier accepts $x, |\pi\rangle \otimes |\psi\rangle$ with prob. $\geq 2/3$
- if $x \notin L \Rightarrow \forall$ proofs $|\pi\rangle \otimes |\psi\rangle$, Verifier accepts $x, |\pi\rangle \otimes |\psi\rangle$ with prob. $\leq 1/3$

Some Remarks

1. Amplification. Usual method of amplification, i.e., the majority trick does not work for QMA(2)

Suppose Verifier does 100 repetitions and takes the majority

Completeness case: Verifier recieves $|\psi_1\rangle^{\otimes 100} \otimes |\psi_2\rangle^{\otimes 100}$
$\mathbb{P}$[Verifier succeds] $\geq 1 - \exp(-100)$
since each trial is independent

Soundness case: Merlins could give proofs of the form

$$\left(\sum_i \alpha_i |\psi_{1,1}, \cdots \psi_{1,100}\rangle\right) \otimes \left(\sum_i \beta_i |\psi_{2,1} \cdots\cdots \psi_{2,100}\rangle\right)$$

Can we show that the maximum is achieved by product states ?

NOT CLEAR !

Suppose Verifier processes the register corresponding to the first copy of $|\psi_1\rangle \otimes |\psi_2\rangle$

The verifier makes a joint measurement which will entangle the two witnesses together and we have no guarantees on what the verifier does on entangled witnesses

This phenomena is called entanglement swapping

Despite this, Harrow and Montanaro used more sophisticated ideas to show that error reduction is possible :

With poly(n) repetitions, one can make the success probability $\geq 1 - 2^{-poly(n)}$

Note This requires many copies of the witnesses. There is no known analog of Marriott - Watrous single-copy error reduction for QMA(2)

$\boxed{2}$ $QMA(k) = QMA(2)$ $\forall$ $2 \le k \le poly(n)$ as shown by Harrow & Montanaro

Note: Size of proofs increase by poly(n) factor in transforming a QMA(k) protocol to QMA(2) protocol

$\boxed{3}$ Upper Bounds on QMA(2)

Exponential-sized witness & EXP Verifier

$QMA \subseteq QMA(2) \subseteq NEXP$

$QMA_{log} = BQP$ and it is unlikely that 3SAT or 3COL has a QMA witness of sublinear size because of the Exponential Time Hypothesis

Short QMA(2) proofs for NP

Theorem (Blier-Tapp) 3COL is in $QMA(2)_{log}$ with completeness 1 and soundness $1 - \frac{1}{n^6}$

Note that amplifying the gap to constant will increase the size of proofs by $O(n^6)$ factor

So, this does not say that $NP \subseteq QMA(2)_{log}$

A similar result was shown by Aaronson, Beigi, Drucker, Fefferman and Shor who showed

$3SAT \in QMA(2)_{\sqrt{n}\,polylog(n)}$ with completeness $\geq 2/3$ and soundness $\leq 1/3$

This is surprising because a similar result for QMA would imply a sub-exponential algorithm for 3SAT

QMA(2) proofs for 3 COLORING

3-COLOR Given a graph, can its vertices be colored with 3-colors so that end points of all edges have different colors?

Let G be the graph on n vertices

Arthur hopes that Merlin will provide $|\psi\rangle \otimes |\psi\rangle$ where

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{v \in V} \underbrace{|v\rangle}_{\text{vertex, } O(\log n) \text{ qubits}} \otimes \overbrace{|color(v)\rangle}^{O(1) \text{ qubits}}$$

Size of proof is $O(\log n)$

Now if Merlin provides 2 copies of this state $|\psi\rangle$ to Arthur

$$|\psi\rangle \otimes |\psi\rangle = \left(\frac{1}{\sqrt{n}} \sum_{v_1} |v_1\rangle |color(v_1)\rangle\right) \otimes \left(\frac{1}{\sqrt{n}} \sum_{v_2} |v_2\rangle |color(v_2)\rangle\right)$$

Arthur wants to check that the coloring is a valid 3COLORING
so, he measures the four registers and obtains

$$(v_1, color(v_1)) \quad , (v_2, color(v_2)) \text{ for}$$

vertices v_1 and v_2 sampled independently and uniformly

COLORING TEST

- If $v_1 \neq v_2$ are not neighbours, Arthur accepts.
- If v_1 & v_2 are neighbours, Arthur accepts if $color(v_1) \neq color(v_2)$ o/w rejects — happens with probability $\geq 1/n^2$
- If $v_1 = v_2$, Arthur accepts if $color(v_1) = color(v_2)$ ← will become relevant later for soundness

What is the completeness and soundness of this proof system ?

- If G was 3-colorable, then Merlin can use a valid 3-coloring and Arthur will accept with probability 1
- If G was not 3-colorable, then for any coloring there is at least one edge that violates the coloring constraint.

  If Merlin sends $|\psi\rangle \otimes |\psi\rangle$ where $|\psi\rangle$ is of the form we said, then the probability that Arthur samples a violated edge is at least $\frac{2}{n^2}$

  So, he will accept with probability at most $1 - \frac{2}{n^2}$

So, there is $\frac{1}{poly(n)}$ gap between completeness and soundness assuming Merlin provides state of the form we said

In general, Merlin could provide $|\varphi\rangle \otimes |\theta\rangle$ for arbitrary $|\varphi\rangle$ and $|\theta\rangle$ which need not be of the form $\frac{1}{\sqrt{n}} \sum_{v} |v\rangle |color(v)\rangle$

For example, a cheating Merlin could remove the vertices that correspond to improperly colored edges, which will cause Arthur to always accept

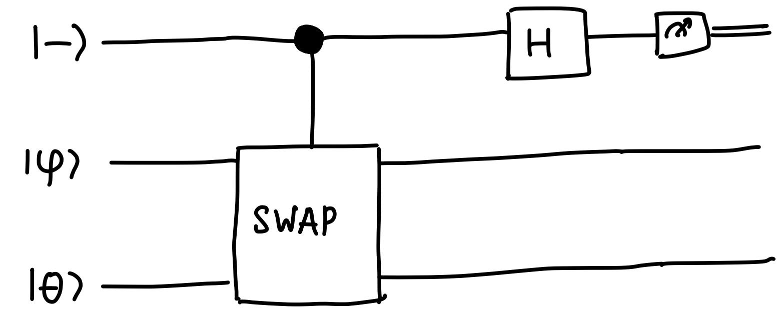
To handle this, we need to check that the proof given by Merlin satisfies

1. $|\varphi\rangle = |\theta\rangle$ — This will be checked by the SWAP test
2. $|\varphi\rangle = \frac{1}{\sqrt{n}} \sum_v |v\rangle |\beta_v\rangle$ — This will be checked by a uniformity test
3. COLORING test from before

Arthur can pick one of the 3 tests at random and apply it to the given witness $|\varphi\rangle \otimes |\theta\rangle$

If the test fails, Arthur will reject with an inverse polynomial gap

<u>SWAP Test</u>



State after controlled SWAP $= \dfrac{|0\rangle|\varphi\rangle|\theta\rangle - |1\rangle|\theta\rangle|\varphi\rangle}{\sqrt{2}}$

If we apply H, we get $= \dfrac{|+\rangle|\varphi\rangle|\theta\rangle - |-\rangle|\theta\rangle|\varphi\rangle}{\sqrt{2}}$

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

$$\mathbb{P}\left[\text{output qubit is } 1\right] = \frac{1}{4} \| |\varphi\rangle|\theta\rangle + |\theta\rangle|\varphi\rangle \|^2$$

$$= \frac{1}{4}\left(\| |\varphi\rangle|\theta\rangle\|^2 + \||\theta\rangle|\varphi\rangle\|^2 + 2|\langle\varphi|\theta\rangle|^2\right)$$

$$= \frac{1}{4}\left(2 + 2|\langle\varphi|\theta\rangle|^2\right)$$

$$= \frac{1}{2} + \frac{|\langle\varphi|\theta\rangle|^2}{2}$$

If $|\varphi\rangle = |\theta\rangle$, test always outputs 1

If $|\varphi\rangle$ and $|\theta\rangle$ are orthogonal, test outputs 1 with probability $\frac{1}{2}$

One can repeat this

Uniformity Test   We can assume that the state is (approximately) of the form $|\varphi\rangle \otimes |\varphi\rangle$ otherwise SWAP test would reject

Arthur now wants to check if $|\psi\rangle$ is of the form $\frac{1}{\sqrt{n}} \sum |v\rangle |color(v)\rangle$

First note that one can check if a state is an equal superposition or not by using the Quantum Fourier Transform over $\mathbb{Z}/\mathrm{mod}\, r\mathbb{Z}$

$$QFT_r |x\rangle \longrightarrow \frac{1}{\sqrt{r}} \sum_{y=0}^{r-1} \omega_r^{x \cdot y} |y\rangle$$ where $x, y \in [0, r-1]$ are integers and $\omega_r = e^{2\pi i/r}$ is the r^{th} root of unity

Note that $$QFT_r^{\dagger} \left(\frac{1}{\sqrt{r}} \sum_{y=0}^{r-1} |y\rangle \right) = |0\rangle$$

① Arthur applies QFT_3 to the second register and measures
If outcome is not $|0\rangle$, he accepts

② If outcome was $|0\rangle$, Arthur then applies QFT_n to the first register and measures
If outcome is $|0\rangle$, he accepts

Let's see what happens for a properly formatted state

$$\frac{1}{\sqrt{n}} \sum_v |v\rangle |color(v)\rangle \xrightarrow{\mathbb{I} \otimes QFT_3} \frac{1}{\sqrt{n}} \sum_v |v\rangle \otimes \left(\frac{1}{\sqrt{3}} |0\rangle + \frac{1}{\sqrt{3}} \omega_3^{color(v)} |1\rangle + \frac{1}{\sqrt{3}} \omega_3^{2color(v)} \right)$$

$$= \frac{1}{\sqrt{3n}} \sum_v |v\rangle |0\rangle + |\perp\rangle$$

↳ second register orthogonal to $|0\rangle$

If we measure the second register, w.p. $2/3$ we get non-zero and accept

If the outcome was $|0\rangle$, our state becomes $\frac{1}{\sqrt{n}} \sum_v |v\rangle \otimes |0\rangle$

Now applying QFT_n to the first register and measuring gives $|0\rangle$ always

If all three tests pass, then the state is of the right form approximately
(One can make this quantitative but we are not going to do it here)

IN-CLASS EXERCISE   What if Merlins give a superposition over colors ?

So, to cheat Merlins must use a state where one of the tests fail and choosing the tests at random, there is some chance for Arthur to detect it which creates a $1/\text{poly}(n)$ gap between completeness and soundness

<u>NEXT TIME</u> Detecting Entanglement and Complexity of Ground States