LECTURE 14 (March 4th)

TODAY Properties of QMA & Error Reduction

RECAP **QMA** L is in QMA if $\exists$ poly-size uniform quantum circuit family $\{V_n\}_n$ (Verifier) s.t.

$x \in L \implies \exists$ proof $|\pi\rangle \in \{0,1\}^{poly(|x|)}$, $\mathbb{P}[V \text{ accepts } |x\rangle|\pi\rangle] \geq \frac{2}{3}$ (completeness)

$x \notin L \implies \forall$ proofs $|\pi\rangle \in \{0,1\}^{poly(|x|)}$, $\mathbb{P}[V \text{ accepts } |x\rangle|\pi\rangle] \leq \frac{1}{3}$ (soundness)

If the proof $|\pi\rangle$ is classical (i.e. a computational basis state) the class is QCMA

POVM A POVM $M_1, \ldots, M_k$ is a set of operators satisfying

$$M_i \geq 0 \quad \text{and} \quad \sum_{i=1}^{k} M_i = I$$

$$\mathbb{P}[\text{Measuring } i^{th} \text{ operator on } |\pi\rangle] = \mathrm{Tr}[M_i |\pi\rangle\langle\pi|] = \langle\pi|M_i|\pi\rangle$$

A special case of POVM $\{M, I-M\}$ $\rightarrow$ Note that they sum to I

Any eigenvector $|v\rangle$ of M with eigenvalue λ
is also an eigenvector of $I-M$ with eigenvalue $1-\lambda$

So, one can diagonalize M and $I-M$ in the same basis

$$M = \sum_i \lambda_i |v_i\rangle\langle v_i|$$

$$\text{Then } I - M = \sum_i (1-\lambda_i) |v_i\rangle\langle v_i|$$

Naimark's Dilation Theorem Every POVM can be expressed as a projective measurement (i.e. projection on subspaces) on a system tensored with some ancillary space.

For instance, Measure $|\pi\rangle$ with POVM $\{M, I-M\}$

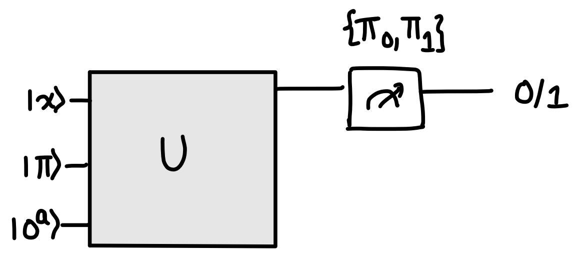
or

Measure $|\pi\rangle \otimes |0^a\rangle$ with projectors $\{\Pi_1, \Pi_0\}$ where

$$\left.\begin{array}{l} \Pi_1 = |1\rangle\langle 1| \otimes \mathbb{I} \\ \Pi_0 = |0\rangle\langle 0| \otimes \mathbb{I} \end{array}\right\} \text{ measures if the } 1^{st} \text{ qubit is } 1 \text{ or } 0$$

Let us revist QMA and reframe the problem of decinding if an input is in a QMA language in terms of POVMs

QMA and POVMs



QMA verifier

For example, $\mathbb{P}[\text{Verifier accepts } |\pi\rangle \text{ on input } x] = \| \Pi_1 U (|\pi\rangle |0\rangle^{\otimes a}) \|^2$

$$= \langle \pi | \langle 0^a | \underbrace{\left(U^\dagger \Pi_1 U \right) | 0^a \rangle}_{M_1 \,=\, \text{POVM element}} | \pi \rangle$$

$$= \text{Tr}\left[M_1 |\pi\rangle\langle\pi| \right] = \langle \pi | M_1 | \pi \rangle$$

Suppose that Merlin wanted Arthur to accept

What would be the best proof $|\pi\rangle$ for Merlin to choose ?

$\mathbb{P}[\text{ Verifier accepts } |\pi\rangle] = \langle \pi | M_1 | \pi \rangle$

So, to maximize choose $|\pi\rangle = \text{argmax } \langle \pi | M_1 | \pi \rangle$

If spectral decomposition of $M_1 = \sum \lambda_i |v_i\rangle\langle v_i|$

Then, choose $|\pi\rangle =$ max eigenvector $|v^*\rangle$

Then, $\mathbb{P}[\, V(x) \text{ accepts } |\pi\rangle] =$ max eigenvalue $= \lambda^*$

Lemma If $L \in$ QMA, then $\exists$ efficient POVM M_1 s.t.

if $x \in L \Rightarrow$ max. eigenvalue of $M_1 \geq 2/3$

if $x \notin L \Rightarrow$ max. eigenvalue of $M_1 \leq 1/3$

Since max eigenvalue of $2^{\text{poly}(n)} \times 2^{\text{poly}(n)}$ matrix can be computed in $2^{\text{poly}(n)}$ time this implies that

$$\text{QMA} \subseteq \text{EXP}$$

In fact, QMA $\subseteq$ PSPACE as well (exercise)

Error Reduction in QMA

Recall that error of BQP algorithm can be made exponentially small

This also means that exact error threshold does not matter $\left(\frac{2}{3} \text{ vs any constant } \frac{1}{2}+\varepsilon\right)$

Here, we will show an analogous result for QMA

$\boxed{\text{Lemma}}$ If $L \in$ QMA, then $\exists$ quantum verifier V s.t.

if $x \in L \Rightarrow \exists\ |\pi\rangle$ s.t. $\mathbb{P}[V(x) \text{ accepts } |\pi\rangle] \geq 1-2^{-\Theta(n)}$

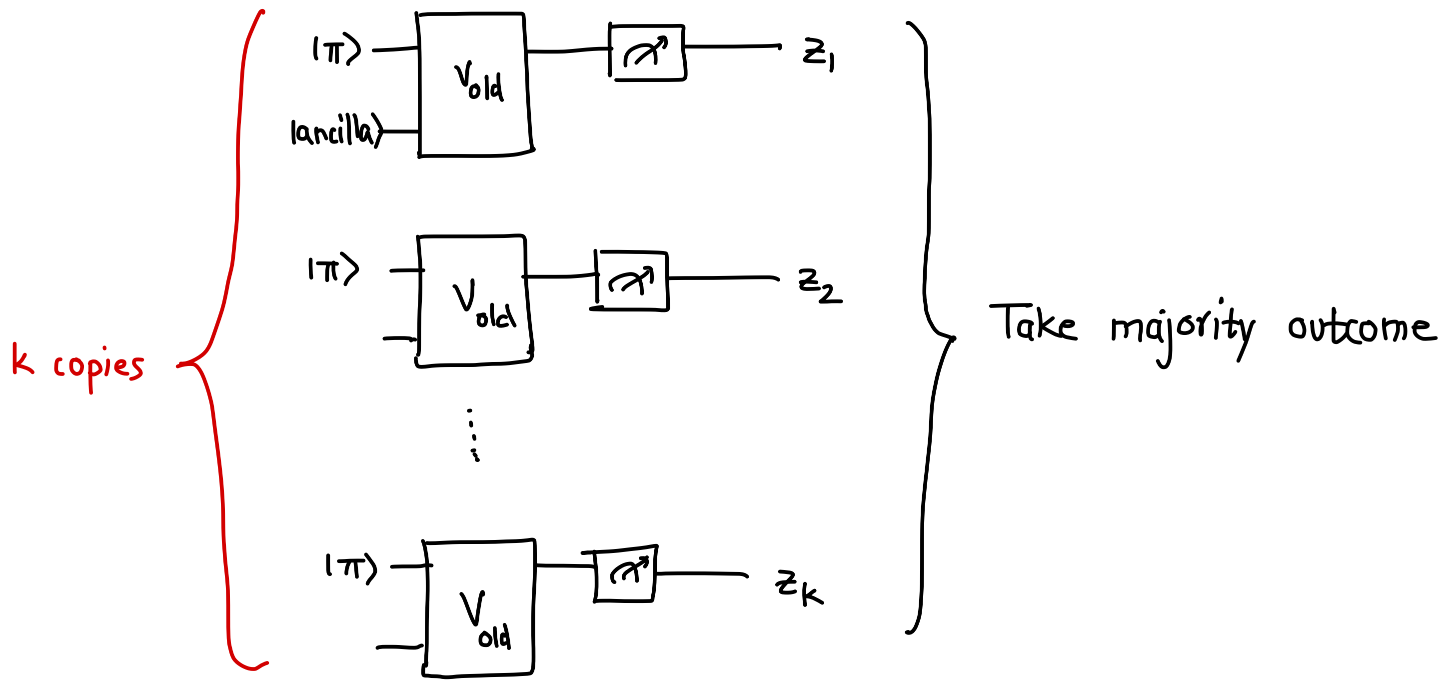
if $x \notin L \Rightarrow \forall \pi$ $\quad \mathbb{P}[\ \text{———}\ ] \leq 2^{-\Theta(n)}$

Also works for classical proofs

<u>Proof</u> The idea is as before : the majority trick

If V_{old} is a verifier with error $1/3$

Consider a new verifier that takes $k = \Theta(n)$ copies of the proof $|\pi\rangle$



Let us call this new verifier V and say that $|\pi\rangle$ has $m = poly(n)$ qubits

Then, if $x \in L \Rightarrow \exists$ proof $|\pi\rangle^{\otimes k}$ s.t. $\mathbb{P}[V(x) \text{ accepts } |\pi\rangle^{\otimes k}]$

$$= \mathbb{P}[MAJ(z_1, \dots z_k) = 1]$$

Note that since $|\pi\rangle^{\otimes k}$ is a product state, $z_1, \dots z_k$ are independent $\{0,1\}$ random variables with $\mathbb{E}[z_i] \geq 2/3$

So, $\mathbb{P}\left[\sum_{i=1}^{k} z_i \geq 0.51k\right] = 1 - 2^{-\Theta(k)} = 1 - 2^{-\Theta(n)}$ (Completeness holds)

What about soundness ?

We want to argue that

if $x \notin L \Rightarrow \forall$ all proofs $|\Pi\rangle \in \left((\mathbb{C}^2)^{\otimes m}\right)^{\otimes k}$, $\mathbb{P}[\, V(x) \text{ accepts } |\Pi\rangle \,] \leq 2^{-\Theta(n)}$

If $|\Pi\rangle = |\pi\rangle^{\otimes k}$, then $\mathbb{P}[\, V(x) \text{ outputs } z_1 \ldots z_k \text{ on } |\pi\rangle^{\otimes k}]$

$$= \prod_{i=1}^{k} \mathbb{P}[\, V_{old}(x) \text{ outputs } z_i \text{ on } |\pi\rangle \,]$$

so distribution of each bit z_i is independent
and we also know that $\mathbb{P}[z_i = 1] \leq \frac{1}{3}$ always

so, $\mathbb{E}[\#z_i\text{'s that are } 1] \leq \frac{n}{3}$

and hence the $\mathbb{P}[\, maj(z_1 \ldots z_k) = 1 \,] = 2^{-\Theta(n)}$

The same also works if $|\Pi\rangle = |\pi_1\rangle \otimes \cdots \otimes |\pi_k\rangle$ because bits are still independent (although not iid)

In the general case, the subtlety is that Merlin could cheat and not give the verifier a product state

In this case it is not obvious the majority argument goes through since the measurement outcomes are not independent

In fact, we are going to show that entangled proofs are only worse

To analyze this, let M_1 be the POVM element corresponding to $V_{old}(x)$ accepts a given proof $|\pi\rangle \in (\mathbb{C}^2)^{\otimes m}$

$M_0 = I - M_0$ be POVM element corresponding to reject

Then, given a possibly entangled proof $|\Pi\rangle \in (\mathbb{C}^2)^{\otimes mk}$,

$\mathbb{P}[\, V(x) \text{ produces outcome } z_1, \ldots z_k \,]$

$$= \langle \Pi | M_{z_1} \otimes M_{z_2} \otimes \cdots \otimes M_{z_k} | \Pi \rangle$$

Let us decompose $M_1 = \sum \lambda_i |i\rangle\langle i|$ and $M_0 = \sum (1-\lambda_i) |i\rangle\langle i|$
where $\{|i\rangle\}$ are the eigenvectors (Note that $|i\rangle$ is not a standard basis vector)

Let us denote $\lambda_{i,1} = \lambda_i$ and $\lambda_{i,0} = 1 - \lambda_i$ $\Rightarrow$ Note: $\lambda_{i,0} + \lambda_{i,1} = 1$

Then, $\mathbb{P}[V(x) \text{ measures } z_1, \dots z_k]$

$$= \langle \pi | \left(\sum_{i_1} \lambda_{i_1, z_1} |i_1\rangle\langle i_1| \right) \otimes (\cdots) \cdots (\quad) | \pi \rangle$$

$$= \langle \pi | \sum_{i_1 \dots i_k} \lambda_{i_1, z_1} \lambda_{i_2, z_2} \cdots \lambda_{i_k, z_k} |i_1 \dots i_k\rangle\langle i_1 \dots i_k| \, |\pi\rangle$$

$$= \sum_{i_1 \dots i_k} \lambda_{i_1, z_1} \lambda_{i_2, z_2} \cdots \lambda_{i_k, z_k} \langle \pi | i_1 \dots i_k \rangle\langle i_1 \dots i_k | \pi \rangle$$

$$= \sum_{i_1 \dots i_k} \lambda_{i_1, z_1} \cdots \lambda_{i_k, z_k} |\langle \pi | i_1 \dots i_k \rangle|^2$$

Let us define a new POVM $O = \{ |i_1 \dots i_k\rangle \}$

Then, above $= \sum_{i_1 \dots i_k} \lambda_{i_1, z_1} \cdots \lambda_{i_k, z_k} \, \mathbb{P}[O \text{ measures } i_1 \dots i_k \text{ on } |\pi\rangle]$

We make one more observation

$$\sum_{z_1 \dots z_k \in \{0,1\}^k} \lambda_{i_1, z_1} \cdots \lambda_{i_k, z_k}$$

$$= \left(\sum_{z_1} \lambda_{i_1, z_1} \right) \left(\sum_{z_2} \lambda_{i_2, z_2} \right) \cdots \left(\sum_{z_k} \lambda_{i_k, z_k} \right) = 1$$

Thus, given a fixed $i_1 \dots i_k$ this also forms a probability distribution

Overall one can write,

$$\mathbb{P}[V(x) \text{ outputs } z_1 \dots z_k] = \sum_{i_1 \dots i_k} \mathbb{P}\left[\begin{matrix} O \text{ outputs } i_1 \dots i_k \\ \text{on } |\pi\rangle \end{matrix} \right] \cdot \mathbb{P}[z_1 \dots z_k \mid i_1 \dots i_k]$$

Thus, we can think of the distribution of $z_1 \dots z_k$ as follows

① First sample hidden variables $i_1 \dots i_k$ by measuring $|\pi\rangle$ with O
This distribution depends on $|\pi\rangle$
Call this distribution $P_{|\pi\rangle}$

② sample $z_1 \dots z_k$ conditioned on $i_1 \dots i_k$ where $\mathbb{P}[z_1 \dots z_k | i_1 \dots i_k]$ are fixed and don't depend on $|\pi\rangle$

Now, $\mathbb{P}[\text{maj}(z_1 \dots z_k) = 1] = \mathbb{E}_{i_1 \dots i_k \sim P_{|\pi\rangle}} \left[\underbrace{\mathbb{P}[\text{maj}(z_1 \dots z_k) = 1 \mid i_1 \dots i_k]}_{\text{this number does not depend on which } |\pi\rangle \text{ we choose}} \right]$

What $|\pi\rangle$ do we choose to maximize this probability ?

choose the outer distribution $P_{|\pi\rangle}$ to be the one which puts all the weight on the largest value

In other words, $P_{|\pi\rangle}(i_1^*, \ldots, i_k^*) = 1$ for some fixed $i_1^*, \ldots, i_k^*$

Recall that $P_{|\pi\rangle}(i_1, \ldots, i_k) = |\langle \pi | i_1, \ldots, i_k\rangle|^2$

we can see that this means that the proof $\pi = |i_1^*, \ldots, i_k^*\rangle$
$= |i_1^*\rangle \otimes \ldots |i_k^*\rangle$

Thus, the maximum success probability is achieved when Merlin gives a tensor product proof and we already saw that in this case $\mathbb{P}[\text{maj} = 1]$ is $2^{-\Theta(n)}$, so we are done

Amplification with a single copy of the proof

One curious aspect of the proof above is that the size of the proof increases by a factor of the number of repetitions since Merlin needs to provide k-copies of the proof

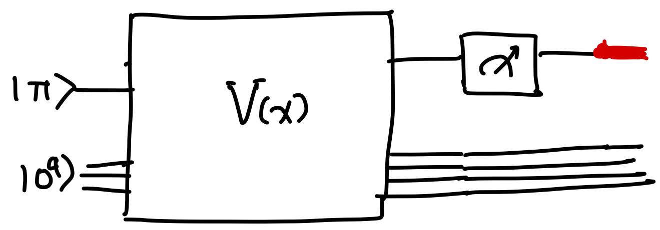
This issue does not arise if the proof was classical since Arthur can make copies of the proof but if the proof was quantum, Arthur can not make copies because of the No-cloning theorem

Is there a way to amplify using a single copy of the proof ?

Theorem Single copy of proof suffices for error reduction in QMA

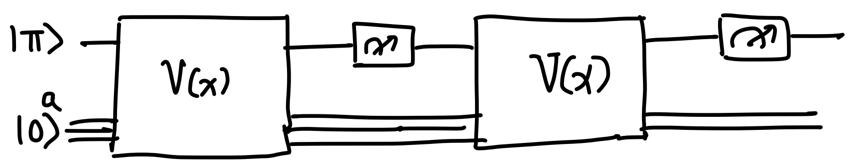
(Marriott- Watrous)

What can we do with a single copy of the proof ?



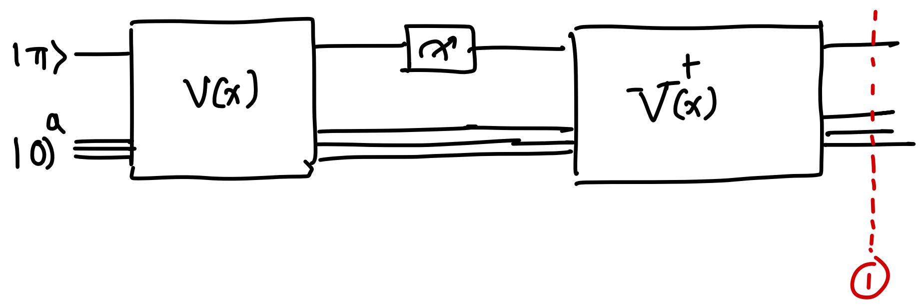
The output bit is classical and can be copied

Can we just run the circuit again ? For instance,



Not at all clear what this circuit would do since the first measurement destroys the proof

How about uncomputing first ?

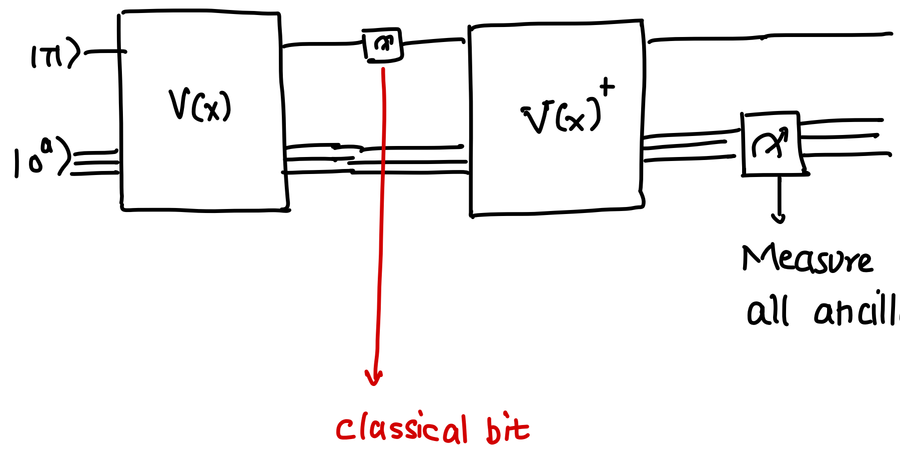


If the final state at ①' is close to $|\pi\rangle \otimes |0^a\rangle$ we could repeat

Again not at all clear why this would be the case because of the intermediate measurement

The Mariott-Watrous algorithm shows that the state at ①' could somehow be reused

In particular, Marriott & Watrous showed that the following algorithm works

① 

--- Repeat poly(n) times

Measure if all ancillas are $|0^a\rangle\langle 0^a|$ or not

② Compute some function of all classical output bits to compute the answer

NEXT TIME Marriott-Watrous Algorithm