Quantum Computation **(CMU 18-859BB, Fall 2015)**

Lecture 25: QMA(2)

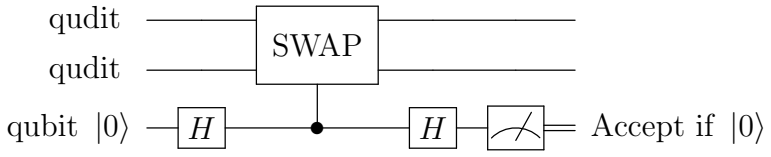
December 7, 2015

Lecturer: Ryan O'Donnell *Scribe: Yongshan Ding*

1 Introduction

So far, we have seen two major quantum complexity classes, namely BQP and QMA. They are the quantum analogue of two famous classical complexity classes, P (or more precisely BPP) and NP, respectively. In today's lecture, we shall extend to a generalization of QMA that only arises in the Quantum setting. In particular, we denote QMA(k) for the case that quantum verifier uses k quantum certificates.

Before we study the new complexity class, recall the following "swap test" circuit from homework 3:



When we measure the last register, we "accept" if the outcome is $|0\rangle$ and "reject" if the outcome is $|1\rangle$. We have shown that this is "similarity test". In particular we have the following:

- $\Pr[\text{Accept } |\psi\rangle \otimes |\varphi\rangle] = \frac{1}{2} + \frac{1}{2}|\langle\psi|\varphi\rangle|^2 = 1 - \frac{1}{2}d_{tr}(|\psi\rangle, |\varphi\rangle)^2$
- $\Pr[\text{Accept } \rho \otimes \rho] = \frac{1}{2} + \frac{1}{2}\sum_{i=1}^{d} p_i^2$, if $\rho = \{p_i |\psi_i\rangle\}$.

2 QMA(2): The 2-Prover QMA

Recall from last time, we introduced the QMA class where there is a prover who is trying to prove some instance x is in the language L, regardless of whether it is true or not. Figure. 1 is a simple picture that describes this.

The complexity class we are going to look at today involves multiple provers. Kobayashi et al. [KMY03] first introduced and studied the class QMA with multiple provers who are promised to be unentangled. Intuitively, multiple prover system can often help the verifier to make fewer mistakes. Probably for the same reason, police often wants to cross check among multiple criminals in order to catch lies. For simplicity, let's start with two provers. Similarly, we have the picture for QMA(2) as in Figure. 2:

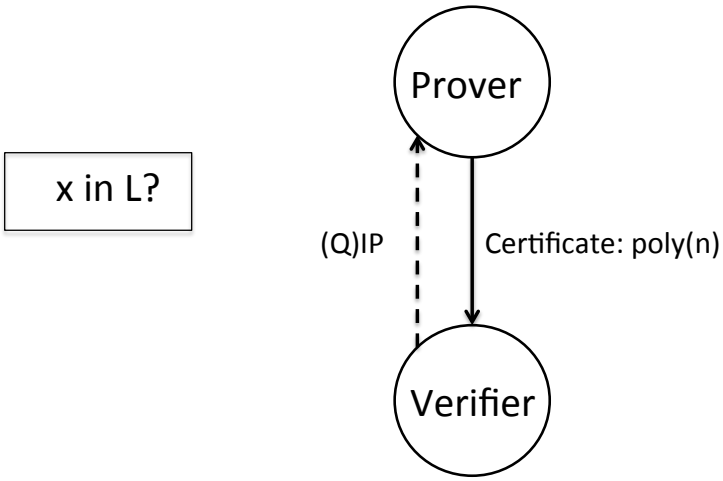


Figure 1: Schematics of QMA

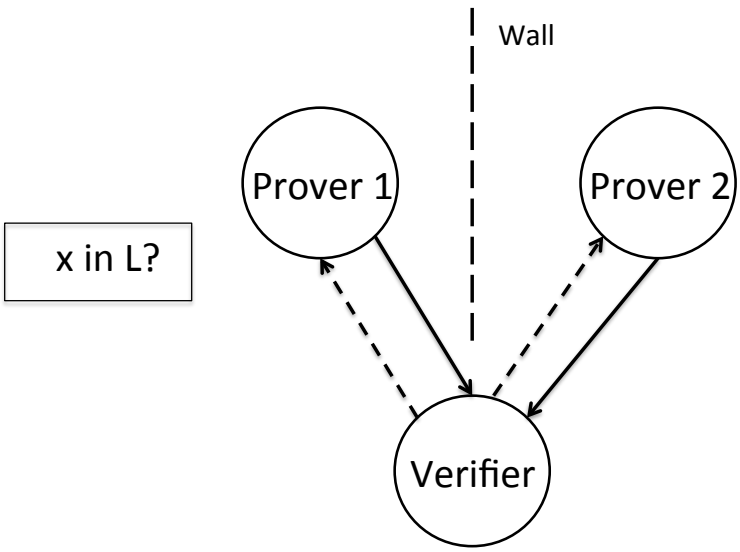


Figure 2: Schematics of QMA(2)

Notice that we have drawn a wall between the two prover so that they cannot communicate with each other. We will explain this assumption more formally very soon. For now, let's first think about the situation in the classical setting. Why don't we have a complexity class that assumes multiple non-interactive provers?

In fact, classically this situation is exactly the same as NP/MA, i.e. the verifier gains no power from the multiple provers. It is pointless to have two provers trying to convince the verifier, because one single prover can give that both sets of information to the verifier and still have the same effect. So the multiple-prover protocol can only help in an interactive setting.

However, in the quantum setting, the "wall" can prevent the provers from being entangled. In other words, assume in the two-prover case, we are granted the assumption that the verifier gets a quantum state $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, with $|\psi_1\rangle$ from prover 1 and $|\psi_2\rangle$ from prover 2. The fact that we can write the overall state in the tensor form guarantees the states *to be unentangled*.

Let's now look at the quantum setting, and try to derive some properties of the new complexity class with multiple provers.

Definition 2.1. QMA(2) is the set of all languages L such that there exists a ("BQP") verifier V such that

- (Completeness) If $x \in L$, $\exists\ |\psi_1\rangle, |\psi_2\rangle$, each with $l = poly(n)$ qubits long, s.t.

$$\Pr[V(|x\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle) \text{ accepts}] \geq 2/3 =: c$$

- (Soundness) If $x \notin L$, $\forall\ |\psi_1\rangle, |\psi_2\rangle$, each with $l = poly(n)$ qubits long, s.t.

$$\Pr[V(|x\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle) \text{ accepts}] \leq 1/3 =: s$$

Recall from last time, we said the constants c, s don't matter for QMA because they end up to be the same class. It is not yet clear if this is the case here. In general, we can sometimes put all the parameters together in a compact form: $\text{QMA}_l(k)_{c,s}$, where l is the number of qubits in the certificate that the verifier receives from each prover, k is the number of provers, c is the *completeness* probability and s is the *soundness* probability. It is clear that $\text{QMA}(k) \subseteq \text{QMA}(k')$ for $k \leq k'$, since the verifier can simply interact with the first k provers and ignore the rest.

3 Power of Non-entanglement

It is conjectured that the multi-prover protocol with the non-entanglement promise is more powerful than QMA. In fact, Liu et al [LCV07] proposed a problem that is in QMA(2) but is not known to be in QMA, namely the N-representability problem. Several other works can be found in [BT09], [Bei10], [ABD+09], [CD10]

Theorem 3.1 ([BT09])**.** *NP $\subseteq$ QMA(2) with $l = \log(n), c = 1$ and $s = 1 - \frac{1}{poly(n)}$.*

In other words, using 2 unentangled proofs, each with $O(\log n)$ qubits long, the verifier:

- accpets satisfiable formulas always;
- rejects unsatisfiable formulas with probability $\frac{1}{\text{poly}(n)}$.

Remark 3.2. It is still highly doubtful whether SAT $\in \text{QMA}_{\log}(2)$ with $c = 1, s = 0$, even for $l = o(n)$. Because if it were true, then we can solve SAT quantumly in $2^{o(n)}$ time.

Remark 3.3. It is also doubtful whether NP $\subseteq \text{QMA}_{\log}(2)$ with $c = 2/3, s = 1/3$. For the same logic, we can probably show NEXP $\subseteq \text{QMA}_{\log}(2)$ by extending the length of proofs to exponentially long.

Another invariant of the work is proposed by Aaronson et al. using the 3SAT problem:

Theorem 3.4 ([ABD$^+$09])**.** *NP* $\subseteq$ $QMA_l(k)_{c,s}$ *with* $l = \log m, k = \tilde{O}(\sqrt{m}), c = 1, s = 0.999$.

Notice that the soundness probability is now a constant.

Furthermore, Harrow and Montanaro [HM12] have shown that it is possible to apply efficient soundness amplification and prover reduction. And in fact, it is shown by Kobayashi et al. [KMY03] that soundness amplification and prover reduction are equivalent. Intuitively, at least one of the direction sounds plausible. Suppose we used many copes of proofs to reduce error. We let each copy of the proof be sent by each of the k provers. If k can be reduced to 2, then error reduction is also possible.

4 Prover Reduction

Theorem 4.1 ([HM12])**.** *k number of unentangled provers can be reduced to only two.*

Before we prove this theorem, let's first try to reduce down to one provers. In other words, we want to show QMA(k) $\subseteq$ QMA(1). It is easy to see that the verifier now receives one giant state $|\Psi\rangle$, and the prover can virtually send anything. There is no way we can still guarantee the promise of non-entanglement we had before (i.e. $|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$). Now, let's see how could QMA(2) help us reassure the non-entanglement, thereby showing QMA(k) $\subseteq$ QMA(2).

Clearly, it is equivalent to test non-entanglement of any k-partite state $|\Psi\rangle$ using just two (identical) copies of $|\Psi\rangle$. It is possible to remove the assumption of "identical" copies. We will leave it to the reader.

Now if we are given two copies of $|\Psi\rangle$, the problem is then reduced to testing purity, because if $|\Psi\rangle$ is an entangled states, then discarding $|\psi_2\rangle, \ldots, |\psi_k\rangle$ will give us a mixed state at $|\psi_1\rangle$.

[Insert product test diagram]

Therefore, as shown in the diagram above, we can apply "swap test" to the n pairs of corresponding $|\psi_i\rangle$ in each copy of $|\Psi\rangle$. ■

Combining the results, we thereby obtain that

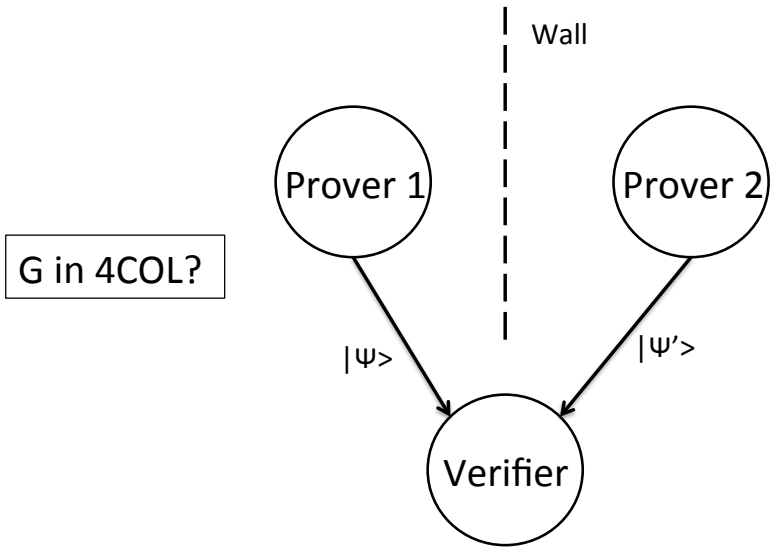


Figure 3: Schematics of QMA(2) for verifying 4COL

- 3SAT $\in$ QMA($\tilde{O}(\sqrt{m})$) where each prover sends $\log(m)$ qubits, with completeness $c = 1$ and constant soundness s.
- 3SAT $\in$ QMA(2) where each prover sends $\tilde{O}(\sqrt{m})$ qubits, with completeness $c = 1$ and constant soundness s.

5 NP $\subseteq$ QMA(2)

In this section, we want to prove the following theorem using 4COL:

Theorem 5.1 ([BT09])**.** *NP $\subseteq$ QMA(2). In particular, 4COL $\in QMA_{\log}(2)$ with $c = 1, s = 1 - \frac{1}{poly(n)}$*

Given input graph $G = (V, E)$, we have the QMA(2) protocol to determine if $G \in$ 4COL: WLOG, let $n = |V|$ be a power of 2. We want to show:

- (Completeness) If $G \in$ 4COL, $\exists\ |\psi\rangle, |\psi'\rangle$ s.t.

$$\Pr[\text{Verifier accepts}] = 1$$

- (Soundness) If $G \notin$ 4COL, $\forall\ |\psi\rangle, |\psi'\rangle$ s.t.

$$\Pr[\text{Verifier rejects}] \geq \frac{1}{\text{poly}(n)}$$

In other words, we want to always accept correct proofs and to catch a lie with non-negligible probability. Let's first consider the easy case ("completeness"), with $G \in$ 4COL. What should the prover send? In this case, trying to help the verifier, the prover might as well send a valid coloring of the graph.

Let $\chi : V \to \{0, 1, 2, 3\}$ be a valid coloring, where each color is labeled as integers $1, \ldots, 3$. Then the two provers will send the state:

$$|\psi\rangle = \frac{1}{\sqrt{n}} \sum_{v \in V} |v\rangle |\chi(v)\rangle$$

Notice that the first "vertex register" $|v\rangle$ contains $\log_2(n)$ qubits, and the "color register" $|\chi(v)\rangle$ contains 2 qubits.

The verifier will thus the following protocol consisting of 3 testing components (by performing one of the following three tests with equal probability):

- Coloring Test
- Equality Test
- Uniformity Test

Let's now look at each test separately.

1. "Coloring":

   - Measure the two proofs: $|\psi\rangle \to |v\rangle |c\rangle$, $|\psi'\rangle \to |v'\rangle |c'\rangle$
   - If $(v, v') \in E$, then accept if $c \neq c'$, and reject otherwise.
   - Else if $v \neq v'$, then accept if $c \neq c'$, and reject otherwise.

   Notice from the second item that if $|\psi\rangle = |\psi'\rangle$ then we are done, since it has $\geq \frac{1}{n^2}$ chance of catching a lie.

2. "Equality":

   - Use "swap test" on $|\psi\rangle, |\psi'\rangle$: This is good for completeness, because if true, the verifier will accept with probability 1.

3. "Uniformity": Recall Fourier Transform $\mathcal{F}_N$ over $\mathbb{Z}_N$, we know that the indicator function can be transformed to a uniform superposition, up to a phase.

   - Apply $\mathcal{F}_N$ to the color register. In the good case, we obtain

   $$\frac{1}{\sqrt{n}} \sum_{v \in V} |v\rangle \left(\frac{1}{2} \sum_{c \in \{0,1,2,3\}} i^{c \cdot \chi(v)} |c\rangle \right)$$

   where i is the forth-root-of-unity.

- Measure the color register: Then reject if we get $|00\rangle$, and accept otherwise.

We have therefore shown that the protocol has completeness $c = 1$: i.e. If $G \in$ 4COL, then there exists a proof that the verifier accepts with probability 1. We will leave the soundness proof of this protocol to the reader. For detailed results, one can refer to [BT09].

References

[ABD+09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. volume 5, pages 1–42, 2009.

[Bei10] Salman Beigi. Tnp vs. qmalog(2). *Quantum Information and Computation*, 54(1 / 2):0141–0151, 2010.

[BT09] Hugue Blier and Alain Tapp. All languages in np have very short quantum proofs. *In ICQNM '09: Proceedings of the 3rd International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, 2009.

[CD10] Jing Chen and Andrew Drucker. Short multi-prover quantum proofs for sat without entangled measurements. 2010.

[HM12] Aram Harrow and Ashley Montanaro. Testing product states,quantum merlin-arthur games and tensor optimization. *J. ACM*, 60(1):1–43, 2012.

[KMY03] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur? *Algorithms and Computation*, 2906:189–198, 2003.

[LCV07] Yi-Kai Liu, Matthias Christandl, and Frank Verstraete. Quantum computational complexity of the n-representability problem: Qma complete. *Physical Review Letters*, 98(11), 2007.