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

Lecture 24: QMA: Quantum Merlin-Arthur

December 2, 2015

Lecturer: Ryan O'Donnell *Scribe: Sidhanth Mohanty*

1 Introduction

In this lecture, we shall probe into the complexity class QMA, which is the quantum analog of NP.

Recall that NP is the set of all decision problems with a one-way deterministic proof system.

More formally, NP is the set of all decision problems for which we can perform the following setup.

Given a string x and a decision problem L, there is an omniscient prover who sends a string $\pi \in \{0,1\}^n$ to a *polytime deterministic* algorithm called a verifier V, and $V(x,\pi)$ runs in polynomial time and returns 1 if x is a YES-instance and 0 if x is a NO-instance. The verifier must satisfy the properties of soundness and completeness: in particular, if x is a YES-instance of L, then there exists π for which $V(x,\pi) = 1$ and if x is a NO-instance of L, then for any π that the prover sends, $V(x,\pi) = 0$.

From now on, think of the prover as an unscrupulous adversary and for any protocol the prover should not be able to cheat the verifier into producing the wrong answer.

2 Merlin-Arthur: An upgrade to NP

If we take the requirements for a problem to be in NP and change the conditions slightly by allowing the verifier V to be a BPP algorithm, we get a new complexity class, MA. A decision problem L is in MA iff there exists a probabilistic polytime verifier V (called Arthur) such that when x is a YES-instance of L, there is π (which we get from the omniscient prover Merlin) for which $\mathbf{Pr}(V(x,\pi) = 1) \geq \frac{3}{4}$ and when x is a NO-instance of L, for every π, $\mathbf{Pr}(V(x,\pi) = 1) \leq \frac{1}{4}$. The choice of $\frac{3}{4}$ was arbitrary. As long as you pick a constant greater than $\frac{1}{2}$, error reduction is easy.

It turns out that if you mandate that the probability of being correct when x is a YES-instance to 1, MA still stays the same, by a very nontrivial theorem whose proof you can see in [FGM89]. However, if you add the condition that Arthur can never be duped, that is, remove room for error when x is a NO-instance, then the class simply becomes NP.

NP $\subseteq$ MA because for any NP problem, a probabilistic verifier V' could simply run the deterministic algorithm of the NP verifier V, ignore the random bits, and accurately verify proofs.

It is believed that NP = MA, though no proof is known. There is evidence to believe that NP = MA as research suggests that 'good enough' pseudorandom generators exist. For a detailed overview, refer to [BFA03] and [Vad12].

As an interlude, the name Merlin-Arthur for this complexity class is due to Laszlo Babai, introduced in [BM88].

3 Quantum Merlin-Arthur

The next upgrade that results in a new class comes from letting the verifier V be a quantum algorithm and allowing the prover to send qubits instead of bits. In other words, the verifier is in BQP. The class of problems that can be solved under this protocol is called QMA.

Definition: QMA is the set of all decision problems that can be solved with a quantum algorithm V such that for all possible inputs x, if x is a YES-instance, then there is $|\varphi\rangle$ for which $V(x, |\varphi\rangle) = 1$ with probability $\geq \frac{3}{4}$ and if x is a NO-instance, for every $|\varphi\rangle$, the probability that $V(x, |\varphi\rangle) = 1$ is $\leq \frac{1}{4}$.

3.1 Robustness of QMA

The next thing we probe into is how robust QMA is. If we force the acceptance probability to be 1, does QMA remain the same? It is unknown if this same oddity that is a property of MA holds in QMA.

However, we don't want our definition of QMA to hinge on numbers like $\frac{3}{4}$, so we would like an error amplification protocol that amplifies the success probability to any constant less than 1 of our choice. The amplification can be more formally expressed as: say we have a quantum algorithm V and input x for which there exists a state $|\varphi\rangle$ where $\mathbf{Pr}[V(x, |\varphi\rangle) = 1] \geq c$ when x is a YES-instance and $\mathbf{Pr}[V(x, |\varphi\rangle) = 1] \leq s$ when x is a NO-instance with the promise that $c - s \geq \frac{1}{\text{poly}(n)}$, can we boost the success probability to $1 - 2^{-\text{poly}(n)}$?

It would be easy to boost our probability if we could replicate the proof state $|\varphi\rangle$ that Merlin sent several times, run verifier V on $(x, |\varphi\rangle)$ several times for some input x and take the majority, but unfortunately, you cannot clone an unknown quantum state. And using your proof state by making a measurement renders it unusable for a second time.

The solution to this is make Merlin send the state a bunch of times. In the first proof system, the prover was supposed to send $|\varphi\rangle$ but in this new protocol, we require him to send $|\varphi\rangle^{\otimes T}$ where $T \in O(\text{poly}(n))$. And then Arthur runs his algorithm on each one and returns the majority.

But we are not done yet, as there is another subtlety left to address. When the input x is a NO-instance, then Arthur must reject with high probability. What if Merlin, in his efforts to dupe Arthur, sends quantum states that are entangled with eachother? Then the states can be seen as a mixed states (result from lecture 16). Arthur's probability of accepting a mixed state p when it would be correct to reject is the a convex linear combination of the probabilities that Arthur accepts each pure state that comprises the mixed state. There is some pure state for which Arthur has a probability $p_i > p$ of accepting.

And we know that for each pure state $|\pi\rangle$, $\mathbf{Pr}[V(x, |\pi\rangle) = 1] \leq s$. Therefore, $p_i \leq s$ and $p \leq s$ and our boosting works even if Merlin sends entangled states.

3.2 MA ⊆ QMA, NP ⊆ QMA and QMA ⊆ PP

Since NP ⊆ MA, it shall follow from MA ⊆ QMA that NP ⊆ QMA.

To see why MA is contained in QMA, we first recall that any randomized algorithm can be simulated by a quantum computer efficiently. So for any decision problem $L \in$ MA, we first force the proof sent by Merlin to be classical by measuring all the bits, and then we simulate the verifier's algorithm V with a quantum algorithm V' on input x and this classical proof. This means that L is also in QMA and as a result MA ⊆ QMA.

It is also known that QMA ⊆ PP. (Proof is a homework problem)

There is another complexity class between QMA and MA known as QCMA. This is the class of problems that are solvable if the prover can only send classical bits but the verifier has a Quantum algorithm. Not much is known about QCMA.

4 Some problems in QMA

Here are 3 problems of which we will prove membership in QMA.

1. k-Local Hamiltonians Problem [KSV02]

2. Consistency of local density matrices [Liu06]

3. Group Nonmembership [Wat00]

4.1 k-Local Hamiltonians Problem

The k-Local Hamiltonians Problem is the quantum analogue of Max k-SAT, which is the problem of maximizing the nunber of clauses satisfied in a k-CNF formula.

The problem is physically motivated: roughly, it asks 'You have a Hamiltonian, what is the energy of the ground state?'. More formally, the problem involves a n-qubit state $|\psi\rangle$

Let $|\psi\rangle$ be a n-qubit state. A k-Local Hamiltonian is a Hermitian Matrix H_α acting on n qubits and has the property that it is the identity on all except k of the qubits.

The input to the k-Local Hamiltonian problem is m k-Local Hamiltonians, $H_1, H_2, \ldots, H_m$ with the eigenvalues of each H_i being between 0 and 1.

Let $H = H_1 + H_2 + \ldots + H_m$. Define the ground state energy as $\xi = \min_{|\psi\rangle} \langle\psi| H |\psi\rangle$. The decision problem can be framed as $k{-}\mathrm{LH}_{\alpha,\beta}$ with $\alpha > \beta$, where we say "YES" if $\xi \leq \beta$, "NO" if $\xi \geq \alpha$. In other words, a YES-instance is exactly one where there exists some $|\psi\rangle$ for which $\langle\psi| H |\psi\rangle \leq \beta$ and a NO-instance is one where for every $|\psi\rangle$, $\langle\psi| H |\psi\rangle \geq \alpha$.

Theorem 4.1. $k - \mathrm{LH}_{\alpha,\beta} \in \mathrm{QMA}$ *with* $c = 1 - \frac{\beta}{m}$ *and* $s = 1 - \frac{\alpha}{m}$. *In fact, the problem is in QMA provided* $\alpha - \beta \geq \frac{1}{\mathrm{poly}(n)}$.

Proof. Merlin sends the state $|\psi\rangle$ that minimizes $\langle\psi| H |\psi\rangle$. Pick a uniformly random H_i from $H_1, \ldots, H_m$ and measure $|\psi\rangle$ with the POVM $\{H_i, I - H_i\}$. The probability that the measurement outcome corresponds to H_i for some i is $\sum \langle\psi| \frac{1}{m} H_i |\psi\rangle = \frac{1}{m} \langle\psi| H |\psi\rangle$.

By having Merlin send multiple copies, and measuring each one, we can discern the value of $\langle\psi| H |\psi\rangle$ within a negligible error margin, and check if it is $\leq \beta$ or $\geq \alpha$.

□

As an exercise, one may try showing that 3SAT is a subproblem of $3{-}\mathrm{LH}_{1,0}$.

Kitaev showed that the problem is QMA-complete for $k \geq 5$ in [KSV02]. This result was improved to $k \geq 3$ in [KR03], and further improved to $k \geq 2$ in [KKR06]. The proof is along the lines of the proof of Cook-Levin theorem, but much harder.

4.2 Consistency of local density matrices

The inputs to this problem are as follows: m k-qubit density matrices $\rho_1, \rho_2, \ldots, \rho_m$ and subsets $S_1, \ldots, S_n \subseteq [n]$ where ρ_i is the identity on all qubits except for the ones in S_i.

You are given a promise that either there is a global n-qubit density matrix σ such that $\mathrm{tr}_{\overline{S_i}}(\sigma) = \rho_i$ for every i or for all n-qubit density matrices σ, there is $i \in [m]$, $\|\mathrm{tr}_{\overline{S_i}} - \rho_i\|_1 \geq \frac{1}{\mathrm{poly}(n)}$.

QMA-completeness: One can reduce this problem from k-Local Hamiltonians problem as illustrated in [Liu06].

To show membership in QMA we sketch a proof.

Theorem 4.2. *Consistency is in QMA.*

Proof. The prover Merlin sends the correct density matrix. The verifier then picks a random subset S_i and checks if $\mathrm{Tr}_{\overline{S_i}}(\sigma)$ is close to ρ_i.

□

4.3 Group Nonmembership

Laszlo Babai conjectured that this problem is in MA. This problem has to do with a whole theory of black box groups due to Laszlo Babai and Endre Szemeredi, introduced and described in [BS84]. For a more modern survey, look at [BB99].

Say you are given a group of size $\leq 2^n$, its elements could either be encoded as permutations (as every group of size n is a subgroup of the symmetric group S_n), finite fields or in black box fashion (a black box specifies the inverse of an element or the product of two elements). And a group G is specified by its generators. A result by Babai and Szemeredi in [BS84] shows that a group can be specified by a set of generators of size at most $(1+\log|G|)^2$.

We shall follow the convention where each group element is encoded by a unique binary string (x is denoted as $\mathrm{enc}(x)$). And we assume we are given an oracle that maps $(\mathrm{enc}(x), \mathrm{enc}(y))$ to $\mathrm{enc}(xy)$ and $\mathrm{enc}(x)$ to $\mathrm{enc}(x^{-1})$. Henceforth, as a measure to not get too cumbersome with notation, $|x\rangle$ shall be used to denote an abstract group element.

4.3.1 An easier problem: Group Membership

Given as input generators of a group $|g_1\rangle, |g_2\rangle, \ldots, |g_n\rangle$ and a target $|x\rangle$, we want to check if $|x\rangle$ is in the group generated by $\{|g_i\rangle\}$.

Theorem 4.3. *Group Membership is in NP.*

At first glance, it may appear that the prover Merlin can simply send a concatenation of generator elements, because it seems like the verifier Arthur can multiply the concatenation and check if it is equal to $|x\rangle$. However, there is an issue with this intuition: it is not at all obvious why the length of the sequence of elements won't be exponential in size. But this has a fix.

Theorem 4.4 (Babai, Szemeredi, Cooperman). *There is a* $\mathrm{poly}(n)$ *time randomized algorithm that multiplies* $T(\approx \mathrm{poly}(n))$ *many* g_i*'s and* g_i^{-1}*'s together and its output is exponentially close to uniformly random on* H*. [Bab91] and [BCF+95]*

Proof. 5-10 pages of Fourier analysis and group theory.

□

The theorem is a very strong statement. As a corollary, we know the following.

Corollary 4.5. *Every element of* H *has a chance of being outputted.*

This means that for every element $x \in H$ there is a nonzero chance that it is outputted, which means there is a polylength sequence of g_i's and g_i^{-1}'s whose product is x and the problem is indeed in NP.

4.3.2 Back to group nonmembership

Now, given $g_1, g_2, \ldots, g_n$ as generators for a subgroup H, we want to decide if $x \notin H$.

One natural way to solve this problem in QMA is to have Merlin send the state

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

But before we proceed further to see why sending that state helps us solve the problem in QMA, let us take a step back and see why the verifier cannot prepare the state himself.

While we can sample a uniformly random $h \in H$, running the randomized algorithm on a quantum computer to obtain the uniform superposition would yield something like

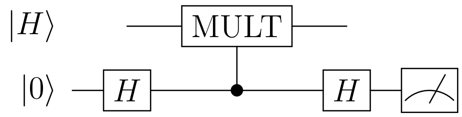
$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |h\rangle \, |\text{garbage}(h)\rangle$$

And it is not clear how one gets rid of the garbage. Yet, it is the verifier's dream to have

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

Thus, a good prover sends the state $|H\rangle$ to the verifier.

Then the verifier attaches a $|0\rangle$ to the second register and runs it through the following circuit.



Applying the first Hadamard changes the state $|H\rangle\,|0\rangle$ to $|H\rangle \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)$.

And then, the second register undergoes a controlled-MULT with the element $|x\rangle$ and the new state is $\frac{1}{\sqrt{2}}\,|H\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|Hx\rangle\,|1\rangle$. If $x \in H$, this state is exactly $|H\rangle \left(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\right)$ since $Hx = H$. If $x \in H$, the final Hadamard sends this state back to $|H\rangle\,|0\rangle$. Measuring the second register always yields $|0\rangle$.

In the case when $x \notin H$, Hx is disjoint from H. And as a consequence, $|Hx\rangle \perp |H\rangle$. If we Hadamard for a second time and measure the second register, we see $|0\rangle$ with probability $\frac{1}{2}$ and $|1\rangle$ with probability $\frac{1}{2}$ each.

To summarize, when $x \in H$, measurement always gives us $|0\rangle$. Whereas, when $x \notin H$, measurement gives us each possibility with an equal probability. There is a one-sided error of $\frac{1}{2}$ that can be boosted.

Thus, we have checked the completeness case. But it remains to verify that the protocol is sound. That is, the prover cannot cheat the verifier.

(The rest is all taken from Piazza)

What if the prover Merlin sends Arthur some state that is not $|H\rangle$? Let's say Merlin sends Arthur some state given by

$$|M\rangle = \sum_{y \in G} \alpha_y \,|y\rangle$$

Arthur could generate a random element $z_1 \in H$, attach a $|0\rangle$ to $|M\rangle$, apply a Hadamard on $|0\rangle$, perform a controlled MULT on $|M\rangle$ with $|z_1\rangle$, apply another Hadamard and then perform a measurement. If the measurement yields $|1\rangle$, it means that elements in the superposition $|M\rangle$ are not all in the same coset of $|H\rangle$, which means that the state is definitely not $|H\rangle$ and we immediately reject.

If we measure $|0\rangle$, the state becomes

$$\sum_{g \in G} \alpha_g |g\rangle + \alpha_g |gz_1\rangle$$

Now, if we do the same thing with a second uniformly random z_2, the resulting state we get is

$$\sum_{g \in G} \alpha_g |g\rangle + \alpha_g |gz_1\rangle + \alpha_g |gz_2\rangle + \alpha_g |gz_1 z_2\rangle$$

And we keep going with $z_1, z_2, \ldots, z_n$ polynomially many times.

Pretty soon, as long as $|\psi\rangle$ is passing the checks, it will become (exponentially close to) H-invariant, of the form $e^{i\theta} |Hg_0\rangle$.

This leads to a situation where the verifier can assume he has a desirable state and proceed with the protocol.

For a deeper summary of results on QMA, one can refer to [AK07].

References

[AK07] Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. In *Computational Complexity, 2007. CCC'07. Twenty-Second Annual IEEE Conference on*, pages 115–128. IEEE, 2007.

[Bab91] László Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 164–174. ACM, 1991.

[BB99] László Babai and Robert Beals. A polynomial-time theory of black box groups i. *London Mathematical Society Lecture Note Series*, pages 30–64, 1999.

[BCF$^+$95] László Babai, Gene Cooperman, Larry Finkelstein, Eugene Luks, and Ákos Seress. Fast monte carlo algorithms for permutation groups. *Journal of Computer and System Sciences*, 50(2):296–308, 1995.

[BFA03] Harry Buhrman, Lance Fortnow, and Pavan Aduri. Some results on derandomization. *Lecture notes in Computer Science*, 2607:212–222, 2003. `http://people.cs.uchicago.edu/~fortnow/papers/derand.pdf`.

[BM88] László Babai and Shlomo Moran. Arthur-merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[BS84] Lászío Babai and Endre Szemerédi. On the complexity of matrix group problems i. In *Foundations of Computer Science, 1984. 25th Annual Symposium on*, pages 229–240. IEEE, 1984.

[FGM89] Martin Furer, Oded Goldreich, and Yishay Mansour. On completeness and soundness in interactive proof systems. 1989.

[KKR06] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.

[KR03] Julia Kempe and Oded Regev. 3-local hamiltonian is qma-complete. *arXiv preprint quant-ph/0302079*, 2003.

[KSV02] A Y Kitaev, A H Shen, and M N Vyalyi. *Classical and Quantum Computation.* 2002.

[Liu06] Yi-Kai Liu. Consistency of local density matrices is qma-complete. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 438–449. Springer, 2006.

[Vad12] Salil P Vadhan. *Pseudorandomness.* 2012.

[Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 537–546. IEEE, 2000.