CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Thursday, March 7 - Lecture 9.2

Today's scribe: Eric L. [Note: note proofread by Eric S.]

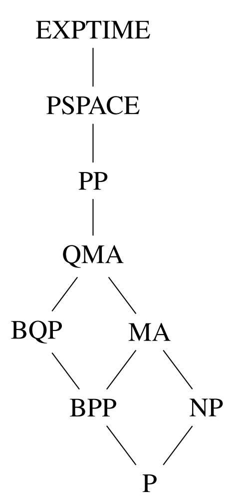
Agenda:

1. QMA
2. Local Hamiltonian Problem
3. Kitaev's Theorem

1 QMA

Quantum Merlin Arthur - Arthur is the "verifier" and Merlin is the "prover".

We have an analogy: QMA:BQP::NP:P::MA:BPP
BQMP is another sensible name for QMA.
Big picture:



NP/MA: non-deterministic polynomial time with coin flips = decision problems for which YES instances have "short" proofs of their YES-ness that can be checked in classical polynomial time with coin flips.

An *instance* of a problem in NP is a T/F question which the test taker Merlin is trying to convince Arthur that the answer is T, and Arthur checks the proof.

MA: non-deterministic polynomial time with coin flips

QMA: non-deterministic quantum polynomial time = decision problems for which YES instances have short *quantum* proofs of their YES-ness that can be checked in quantum polynomial time.

Definition. *A decision problem $L : \{0,1\}^* \to \{0,1\}$ is in QMA if there exists a classical polynomial time algorithm which on input $x \in \{0,1\}^n$ prepares a quantum circuit C_x with an input register of size O(poly(n)) and an ancilla register of size O(poly(n)) such that*

i. (completeness) If $L(x) = 1$, then there exists a state $|\psi\rangle$ on the input qubits of C_x such that

$$\text{Prob}(C_x \text{ outputs } 1 | \text{ input } |\psi\rangle \otimes |0...0\rangle) \geq 2/3$$

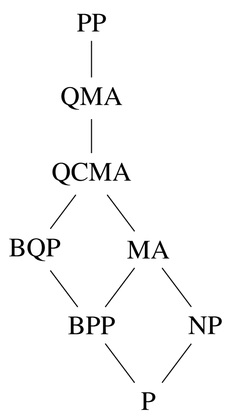
ii. (soundness) If $L(x) = 0$, then for all $|\psi\rangle$ on the input qubits,

$$\text{Prob}(C_x \text{ outputs } 1 | \text{ input } |\psi\rangle \otimes |0...0\rangle) \leq 1/3$$

Two remarks:

1. As usual, the 2/3 and 1/3 above are more-or-less arbitrary. All we need is a "good" gap between them. One uses usual "amplification of probability of success" (Chernoff bound) technique, but a new subtelty arises: Merlin could try to "trick" Arthur if he knows Arthur will run several proof checks in parallel by entangling the proofs!

2. We can modify the definition of QMA to get another interesting complexity class called "Classical Merlin Quantum Arthur". In this case, Merlin only gives classical proofs and $|\psi\rangle$ is a computation basis state. *Should* be called CMQA, unfortunately it's called QCMA.



2 k-Local Hamiltonian Problem

Recall: a decision problem looks like

$$L : \{0,1\}^* \to \{0,1\}$$

A *promise* is a subset $S \subseteq \{0,1\}^*$.

A *promise decision problem* with promise S is a function

$$L : S \to \{0,1\}$$

Moral: Checking the promise S could be hard, but we treat it as a distraction. Because of the promise, it is in QMA.

Kitaev's Theorem says 5-local Hamiltonian Problem is QMA-complete. That is, it is in QMA and every problem in QMA can be reduced to it in quantum polynomial time. This is a quantum analog of the Cook-Levin Theorem, which says that Boolean (circuit) satisfiability (3-SAT) is NP-complete.

Definition. *A k-local Hamiltonian on n qubits is a Hermitian operator H on* $(\mathbb{C}^2)^{\otimes n}$ *expressed/encoded as*

$$H = \sum_{J \subseteq 1,\ldots,n} H_J$$

where $|J| = k$ *and* H_J *is a Hamiltonian supported on the qubits in* J*.*

We assume we "explicitly" know all entries of H_J. In particular, H has at most $\binom{n}{k} = O(n^k)$ non-trivial terms, and $||H|| \leq poly(n)$.

k-Local Hamiltonian Problem

Fix $p(n) = poly(n)$.
Input:

- a local Hamiltonian H on n qubits
- two real numbers $a < b$ such that $b - a > 1/p(n)$

Promise: H has no eigenvalues between b and a.
Output: YES if H has any eigenvalues $\lambda \leq a$, NO otherwise.

Lemma 1. *k-local Hamiltonian problem is in QMA.*

Basic idea: Merlin will give Arthur state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$. Then Arthur will use some quantum algorithm to (approximate) whether or not $|\psi\rangle$ is an eigenvector of H with eigenvalue $\leq a$. Main issue is that Arthur needs to do this to high enough precision to be sure he does not get the wrong answer very often. This is where the promise $b - a > 1/p(n)$ gets used. To actually do this, two approaches:

i. QPE.
ii. Normalize so $0 \leq H_J \leq 1$. Now Arthur randomly picks a J and tests if $|\psi\rangle$ is "low energy" for H_J. Apply amplification.

3 Kitaev's Theorem

Theorem 2. *5-local Hamiltonian problem is QMA-complete.*

Proof uses a "circuit-to-Hamiltonian" "clock construction".
Improvements have been made.

1. How low can we go? $k = 3$? Yes. $k = 2$? Yes, if P$\neq$QMA.
2. "Geometric locality" vs. "abstract locality".

   Intuition: a general 3-local Hamiltonian on n qubits looks like "all triangles in a $(n-1)$-simplex"

   Geometric locality: work in a *fixed* dimension, e.g. 5-local Hamiltonian with nearest neighbor interactions in dimension 2.