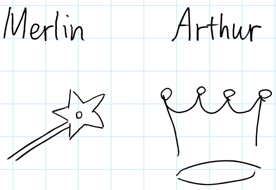
QMA: Quantum Merlin Arthur

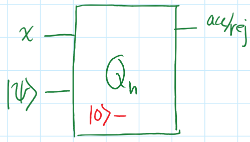
Merlin Arthur

public-coin



1. Definition

Let $A = (A_{yes}, A_{no})$ be a promise problem and let $c, s: \mathbb{N} \to [0,1]$ be functions. Then $A \in \text{QMA}(c, s)$ if and only if there exists a *polynomial-time uniform family of quantum circuits* $\{Q_n : n \in \mathbb{N}\}$, where Q_n takes $n + m(n)$ qubits as input for some polynomial m and outputs 1 bit, such that



- *(Completeness)* if $x \in A_{yes} \cap \Sigma^n$ then there exists an $m(n)$-qubit state $|\psi\rangle$ such that $\Pr[Q_n(x, |\psi\rangle) = 1] \geq c(n)$, and
- *(Soundness)* if $x \in A_{no} \cap \Sigma^n$ then for all $m(n)$-qubit state $|\psi\rangle$, $\Pr[Q_n(x, |\psi\rangle) = 1] \leq s(n)$.

The class QMA is defined as QMA(2/3,1/3).

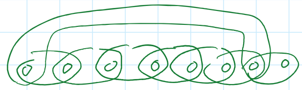
- proof verification
- non-determinism

Quantization of both the witness and the circuit

P NP

BQP QMA

2. Quantum Cook-Levin theorem



Satisfiability and local Hamiltonian problem

Definition. A k-local Hamiltonian H is a summation $H = \sum_{j=1}^{m} H_j$ of local terms H_j acting on at most k qubits (out of n qubits). The k-local Hamiltonian problem is the promise problem with

$H_j \otimes I$

- *Input*: (H, a, b) where H is a k-local Hamiltonian, a, b are real numbers such that $b - a \geq 1/poly(n)$,
- *Yes instances*: The smallest eigenvalue of H is at most a,
- *No instances*: The smallest eigenvalue of H is at least b.

$$H = \begin{pmatrix} 0 & & & & \\ & 1 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

A 3-SAT clause as a Hamiltonian term

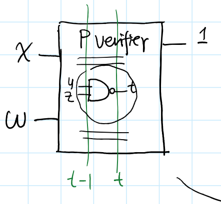
$(x_1 \vee x_2 \vee \neg x_3) \wedge \cdots$

$0 \quad 0 \quad 1$

Theorem. The k-local Hamiltonian problem is QMA-complete for all $k \geq 2$.

Our discussion follows [Quantum NP: A Survey]

Classical proof

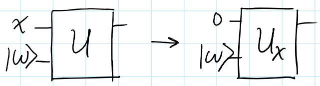


Computation is local

history of computation / propagation

write down a Boolean formula

Circuit to Hamiltonian construction



Review of classical Cook-Levin theorem

Simplification: embed input x to the circuit

Clock register and computation register

History state $|\eta\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_{clock} \otimes U_t \cdots U_2 U_1 (|0^n\rangle |\psi\rangle)$

Consider Hamiltonian terms

Can we check the propagation of quantum computation "locally"

$$H_{in} = \sum_{j=1}^{n} |0\rangle\langle 0|_{clock} \otimes \Pi_j^1,$$

$$H_{out} = |T\rangle\langle T|_{clock} \otimes \Pi_1^0,$$

$$H_{prop}^{(t)} = \frac{1}{2}(|t-1\rangle\langle t-1|_{clock} \otimes I + |t\rangle\langle t|_{clock} \otimes I$$
$$- |t\rangle\langle t-1|_{clock} \otimes U_t - |t-1\rangle\langle t|_{clock} \otimes U_t^\dagger)$$

$|GHZ_\pm\rangle = \frac{1}{\sqrt{2}}(|00\cdots0\rangle \pm |11\cdots1\rangle)$

Even hard to check identity

$-|t\rangle\langle t-1|_{clock} \otimes U_t - |t-1\rangle\langle t|_{clock} \otimes U_t^\dagger)$

Even hard to check identity

$H_{prop} = \sum_{t=1}^{T} H_{prop}^{(t)}$.

The Hamiltonian corresponding to the circuit is $H = H_{in} + H_{out} + H_{prop}$, and we set $a = 1/T^{10}$ and $b = 1/4(T+1)^3$.

Proof

1. Completeness. Easy to check!
2. Soundness. If $x \in A_{no}$, the Hamiltonian H has energy at least b

- Analyse the spectrum of $H_{io} = H_{in} + H_{out}$ and H_{prop}
- Consider the ground spaces N_{io} and N_{prop} of H_{io} and H_{prop} respectively
- Define $R = \sum_{t=0}^{T} U_t \cdots U_1 \otimes |t\rangle\langle t|$

  a. H_{io} is a projector, the second eigenvalue is 1

  b. H_{prop} has a special form under the conjugation of R and the second eigenvalue is at least $1/2(T+1)^2$

  c. have a noticeable angle θ with $\sin^2(\theta/2) \geq 1/2(T+1)$

  From $O(\log(T))$-local to 5-local

H_{io} H_{prop}

1 ―― λ ――

0 ―― 0 ――

not well aligned.

$\lambda_{min}(H_{io} + H_{prop}) \geq 2\lambda \sin^2(\theta/2)$

$R^\dagger H_{prop} R = E_{clock} \otimes I$

$$E_{clock} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & & & \\ -\frac{1}{2} & 1 & -\frac{1}{2} & & \\ & -\frac{1}{2} & 1 & -\frac{1}{2} & \\ & & \ddots & \ddots & -\frac{1}{2} \\ & & & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

has unique ground state $|+\rangle$

For the estimate of $A_2|_{\mathcal{L}_2^\perp}$ we need to find the smallest positive eigenvalue of the matrix E. The eigenvectors and eigenvalues of E are

$$|\psi_k\rangle = \alpha_k \sum_{j=0}^{T} \cos\left(q_k\left(j+\frac{1}{2}\right)\right)|j\rangle, \qquad \lambda_k = 1 - \cos q_k,$$

$q_k = k\pi/(T+1)$

Screen clipping taken: 9/10/2020 12:31 PM

3. Error reduction for QMA

- Standard error reduction: requires multiple copies of the quantum witness state
- Strong error reduction: a single copy of quantum witness state suffices

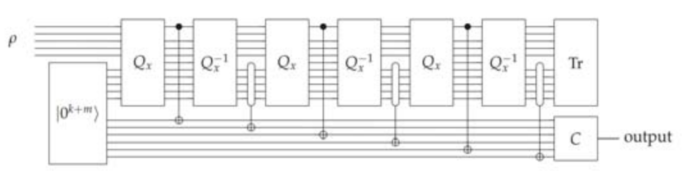


Figure 10: Illustration of the strong error reduction procedure for QMA. The circuit Q_x represents a unitary purification of a given QMA verification procedure on an input x, while the circuit C determines whether to accept or reject based on the number of alternations of its input qubits. The quantum proof is denoted by ρ.

Screen clipping taken: 9/10/2020 12:33 PM

4. Discussions

1. QMA (local Hamiltonian problem) and optimization

   Maximize: $\mathrm{tr}(H\rho)$
   Subject to: ρ is semidefinite positive and trace 1

2. Other complete problems for QMA
    - 1-D local Hamiltonian problem
    - Circuit non-identity
    - Density matrix consistency / N-representability
3. Variants of QMA

5. Exercise 5

Prove that the local Hamiltonian problem is in QMA.

6. Exercise 6

For which circuit is the EPR state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ a history state? Write down the Hamiltonian for this circuit and check that the EPR state is the ground state of that Hamiltonian.

7. Research Problem

Understand the relation of QMA and its variants QCMA, QMA_1, QMA(2).