Delegation of Quantum Computations

Based on Local Hamiltonians

October 20, 2019

Settings

- Classical client, quantum server

Settings

- Classical client, quantum server
- Client has circuit $C = U_n \dots U_1$ and input x, wants to compute and measure $C(|x\rangle)$ by interacting with the server

Settings

- Classical client, quantum server
- Client has circuit $C = U_n \dots U_1$ and input x, wants to compute and measure $C(|x\rangle)$ by interacting with the server
- Nice properties to have:

Settings

- Classical client, quantum server
- Client has circuit $C = U_n \dots U_1$ and input x, wants to compute and measure $C(|x\rangle)$ by interacting with the server
- Nice properties to have:
  - Verifiability

Settings

- Classical client, quantum server
- Client has circuit $C = U_n \dots U_1$ and input x, wants to compute and measure $C(|x\rangle)$ by interacting with the server
- Nice properties to have:
    - Verifiability
    - Privacy

Settings

- Classical client, quantum server
- Client has circuit $C = U_n \dots U_1$ and input x, wants to compute and measure $C(|x\rangle)$ by interacting with the server
- Nice properties to have:
  - Verifiability
  - Privacy
  - Long output

Settings

- Classical client, quantum server
- Client has circuit $C = U_n \dots U_1$ and input x, wants to compute and measure $C(|x\rangle)$ by interacting with the server
- Nice properties to have:
  - Verifiability
  - Privacy
  - Long output

BQNP (QMA)

- Quantum analogue of NP or MA

BQNP (QMA)

- Quantum analogue of NP or MA
- Certificate can be quantum

BQNP (QMA)

- Quantum analogue of NP or MA
- Certificate can be quantum
- Verifier is a BQP machine

BQNP (QMA)

- Quantum analogue of NP or MA
- Certificate can be quantum
- Verifier is a BQP machine

BQNP (QMA)

- Quantum analogue of NP or MA
- Certificate can be quantum
- Verifier is a BQP machine
- Verifier can store qubits and apply X/Z measurements.

BQNP (QMA)

- Quantum analogue of NP or MA
- Certificate can be quantum
- Verifier is a BQP machine
- Verifier can store qubits and apply X/Z measurements.
- Amplification can be done. (This isn't trivial.)

Local Hamiltonian

- A QMA-complete problem

Local Hamiltonian

- A QMA-complete problem
- Given the following input:

Local Hamiltonian

- A QMA-complete problem
- Given the following input:
  - $\{ H_j \}$ each Hermitian and acts on at most k qubits.

Local Hamiltonian

- A QMA-complete problem
- Given the following input:
  - $\{ H_j \}$ each Hermitian and acts on at most k qubits.
  - $a, b \in \mathbb{R}$; $b > a$ with at least inverse polynomial gap

Local Hamiltonian

- A QMA-complete problem
- Given the following input:
  - $\{ H_j \}$ each Hermitian and acts on at most k qubits.
  - $a, b \in \mathbb{R}$; $b > a$ with at least inverse polynomial gap
- Promise problem; decide which of the following is true about $H = \sum H_j$

Local Hamiltonian

- A QMA-complete problem
- Given the following input:
  - $\{ H_j \}$ each Hermitian and acts on at most k qubits.
  - $a, b \in \mathbb{R}$; $b > a$ with at least inverse polynomial gap
- Promise problem; decide which of the following is true about $H = \sum H_j$
  - H has an eigenvalue not exceeding a

Local Hamiltonian

- A QMA-complete problem
- Given the following input:
  - $\{ H_j \}$ each Hermitian and acts on at most k qubits.
  - $a, b \in \mathbb{R}$; $b > a$ with at least inverse polynomial gap
- Promise problem; decide which of the following is true about $H = \sum H_j$
  - H has an eigenvalue not exceeding a
  - All eigenvalues of H are greater than b

Local Hamiltonian

- A QMA-complete problem
- Given the following input:
  - $\{ H_j \}$ each Hermitian and acts on at most k qubits.
  - $a, b \in \mathbb{R}$; $b > a$ with at least inverse polynomial gap
- Promise problem; decide which of the following is true about $H = \sum H_j$
  - H has an eigenvalue not exceeding a
  - All eigenvalues of H are greater than b
- Special case:
  $H_j \in \mathcal{G}_{XZ} = \{ U_0 \otimes U_1 \otimes \ldots \otimes U_n : U_i \in \{ I, X, Z \} \}$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA

Goal: Given certificate ϕ, estimate

$$\langle\phi|H|\phi\rangle = \sum_{S\in\mathcal{G}_{XZ}} d_S S$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA

Goal: Given certificate ϕ, estimate

$$\langle \phi | H | \phi \rangle = \sum_{S \in \mathcal{G}_{XZ}} d_S S$$

$$\frac{1}{\sum |d_S|} \langle \phi | H | \phi \rangle$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA

Goal: Given certificate ϕ, estimate

$$\langle \phi | H | \phi \rangle = \sum_{S \in \mathcal{G}_{XZ}} d_S S$$

$$\frac{1}{\sum |d_S|} \langle \phi | H | \phi \rangle = \sum_{S \in \mathcal{G}_{XZ}} p_S \operatorname{sgn}(d_S) \langle \phi | S | \phi \rangle$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA

Goal: Given certificate ϕ, estimate

$$\langle \phi | H | \phi \rangle = \sum_{S \in \mathcal{G}_{XZ}} d_S S$$

$$\begin{aligned} \frac{1}{\sum |d_S|} \langle \phi | H | \phi \rangle &= \sum_{S \in \mathcal{G}_{XZ}} p_S \operatorname{sgn}(d_S) \langle \phi | S | \phi \rangle \\ &= \sum_{S \in \mathcal{G}_{XZ}} p_S \operatorname{sgn}(d_S) \mathbb{E}[\lambda_S] \end{aligned}$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA

Goal: Given certificate ϕ, estimate

$$\langle\phi|H|\phi\rangle = \sum_{S\in\mathcal{G}_{XZ}} d_S S$$

$$\begin{aligned}\frac{1}{\sum|d_S|}\langle\phi|H|\phi\rangle &= \sum_{S\in\mathcal{G}_{XZ}} p_S \,\mathrm{sgn}(d_S)\,\langle\phi|S|\phi\rangle \\ &= \sum_{S\in\mathcal{G}_{XZ}} p_S \,\mathrm{sgn}(d_S)\,\mathbb{E}[\lambda_S] \\ &= \mathop{\mathbb{E}}_{S}[\mathrm{sgn}(d_S)\,\mathbb{E}[\lambda_S]]\end{aligned}$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA

Goal: Given certificate ϕ, estimate

$$\langle\phi|H|\phi\rangle = \sum_{S\in\mathcal{G}_{XZ}} d_S S$$

$$\begin{aligned}
\frac{1}{\sum|d_S|}\langle\phi|H|\phi\rangle &= \sum_{S\in\mathcal{G}_{XZ}} p_S \operatorname{sgn}(d_S)\langle\phi|S|\phi\rangle \\
&= \sum_{S\in\mathcal{G}_{XZ}} p_S \operatorname{sgn}(d_S)\,\mathbb{E}[\lambda_S] \\
&= \mathop{\mathbb{E}}_S[\operatorname{sgn}(d_S)\,\mathbb{E}[\lambda_S]] \\
&= \mathop{\mathbb{E}}_S[\operatorname{sgn}(d_S)\lambda_S]
\end{aligned}$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA cont.

Let $p = P[\text{sgn}(d_S)\lambda_S = -1]$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA cont.

Let $p = P[\mathrm{sgn}(d_S)\lambda_S = -1]$

$$\Rightarrow \frac{1}{D}\langle\phi|H|\phi\rangle = \mathop{\mathbb{E}}_S[\mathrm{sgn}(d_S)\lambda_S] = -p + (1-p)$$

$\mathcal{G}_{XZ}$ Local Hamiltonian is in QMA cont.

Let $p = P[\text{sgn}(d_S)\lambda_S = -1]$

$$\Rightarrow \frac{1}{D}\langle\phi|H|\phi\rangle = \mathop{\mathbb{E}}_{S}[\text{sgn}(d_S)\lambda_S] = -p + (1-p)$$

$$\Rightarrow p = \frac{1}{2} - \frac{1}{2D}\langle\phi|H|\phi\rangle$$

Preliminary facts

Hadamard and Toffoli gates are:

- universal (with real states)
- in span $\mathcal{G}_{XZ}$

Local Hamiltonian is BQP-hard

Let $C = U_T \ldots U_1$ be a circuit using only Hadamard and Toffoli gates. Let $|x\rangle$ be the initial state.

Local Hamiltonian is BQP-hard

Let $C = U_T \ldots U_1$ be a circuit using only Hadamard and Toffoli gates. Let $|x\rangle$ be the initial state.
Goal: construct H such that

$$|\phi\rangle = \sum_{t=0}^{T} U_t \ldots U_1 |x\rangle \otimes |\hat{t}\rangle$$

is low energy on a yes-instance.

Checking for valid outputs

$$H_{out} = (I - |1\rangle\langle 1|_0) \otimes |\hat{T}\rangle\langle\hat{T}|$$

Checking for valid outputs

$$H_{out} = (I - |1\rangle\langle 1|_0) \otimes |\hat{T}\rangle\langle\hat{T}|$$

$$= \left(\frac{1}{2}(I - Z_1)\right) \otimes \left(\frac{1}{2}(1 + Z_T)\right) \in \operatorname{span} \mathcal{G}_{XZ}$$

Checking for valid inputs

$$H_{in} = \sum_{i=1}^{n} (I - |x_i\rangle \langle x_i|) \otimes |0\rangle \langle 0|_1$$

Checking for valid inputs

$$H_{in} = \sum_{i=1}^{n} (I - |x_i\rangle \langle x_i|) \otimes |0\rangle \langle 0|_1$$

$$= \sum_{i=1}^{n} \left(\frac{1}{2} I - (-1)^{x_i} Z_i \right) \otimes \left(\frac{1}{2} (I + Z_1) \right) \in \operatorname{span} \mathcal{G}_{XZ}$$

Checking for legal clock states

$$H_{clock} = \sum_{t=1}^{T-1} |01\rangle \langle 01|_{t,t+1}$$

Checking for legal clock states

$$H_{clock} = \sum_{t=1}^{T-1} |01\rangle\langle 01|_{t,t+1}$$

$$= \frac{1}{4}(Z_1 - Z_T) + \frac{1}{4}\sum_{t=1}^{T-1}(I - Z_t Z_{t+1})$$

Checking for valid propagation

$$H_{prop} = \sum_{t \in T_1} H_{prop,t}$$

Checking for valid propagation

$$H_{prop} = \sum_{t \in T_1} H_{prop,t}$$

Intuitively,

$$I \otimes |\widehat{t}\rangle \langle\widehat{t}| - U_t \otimes |\widehat{t}\rangle \langle\widehat{t-1}|$$

Checking for valid propagation

$$H_{prop} = \sum_{t \in T_1} H_{prop,t}$$

Intuitively,

$$I \otimes |\widehat{t}\rangle\langle\widehat{t}| - U_t \otimes |\widehat{t}\rangle\langle\widehat{t-1}|$$

$$H_{prop,t} = I \otimes |\widehat{t}\rangle\langle\widehat{t}| + I \otimes |\widehat{t-1}\rangle\langle\widehat{t-1}| - U_t \otimes |\widehat{t}\rangle\langle\widehat{t-1}| - U_t^{\dagger} \otimes |\widehat{t-1}\rangle\langle\widehat{t}|$$

$H_{prop} \in \operatorname{span} \mathcal{G}_{XZ}$

$$H_{prop,t} = I \otimes |\widehat{t}\rangle\langle\widehat{t}| + I \otimes |\widehat{t-1}\rangle\langle\widehat{t-1}| - U_t \otimes |\widehat{t}\rangle\langle\widehat{t-1}| - U_t^\dagger \otimes |\widehat{t-1}\rangle\langle\widehat{t}|$$

$H_{prop} \in \operatorname{span} \mathcal{G}_{XZ}$

$$H_{prop,t} = I \otimes |\widehat{t}\rangle\langle\widehat{t}| + I \otimes |\widehat{t-1}\rangle\langle\widehat{t-1}| - U_t \otimes |\widehat{t}\rangle\langle\widehat{t-1}| - U_t^\dagger \otimes |\widehat{t-1}\rangle\langle\widehat{t}|$$

$$= \frac{I}{4} \otimes (I - Z_{t-1})(I + Z_{t+1}) - \frac{U_t}{4} \otimes (I - Z_{t-1})X_t(I + Z_{t+1})$$

$H_{prop} \in \operatorname{span} \mathcal{G}_{XZ}$

$$H_{prop,t} = I \otimes |\hat{t}\rangle\langle\hat{t}| + I \otimes |\widehat{t-1}\rangle\langle\widehat{t-1}| - U_t \otimes |\hat{t}\rangle\langle\widehat{t-1}| - U_t^\dagger \otimes |\widehat{t-1}\rangle\langle\hat{t}|$$

$$= \frac{I}{4} \otimes (I - Z_{t-1})(I + Z_{t+1}) - \frac{U_t}{4} \otimes (I - Z_{t-1})X_t(I + Z_{t+1})$$

$$H_{prop,1} = \frac{1}{2}(I + Z_2) - U_1 \otimes \frac{1}{2}(X_1 + X_1 Z_2)$$

$$H_{prop,T} = \frac{1}{2}(I - Z_{t-1}) - U_T \otimes \frac{1}{2}(X_T - Z_{T-1}X_T)$$

Analysis of H_{prop}

By induction,

$$\Rightarrow K_{clock} \cap K_{prop} = \{ \sum_{t=0}^{T} U_t \ldots U_1 \mid y\rangle \otimes \mid \hat{t}\rangle : \mid y\rangle \in \mathcal{B}^{\otimes n} \}$$

Analysis of H_{prop}

By induction,

$$\Rightarrow K_{clock} \cap K_{prop} = \{ \sum_{t=0}^{T} U_t \ldots U_1 \mid y\rangle \otimes \mid \hat{t}\rangle : \mid y\rangle \in \mathcal{B}^{\otimes n} \}$$

Claim:

$$H_{prop} \geq 0$$

$H_{prop} \geq 0$

Consider the change of coordinates

$$W = \sum_{j=0}^{L} U_j \dots U_1 \otimes |j\rangle \langle j|$$

$H_{prop} \geq 0$

Consider the change of coordinates

$$W = \sum_{j=0}^{L} U_j \dots U_1 \otimes |j\rangle \langle j|$$

$$\Rightarrow W^\dagger |\phi\rangle = \sum_{t=0}^{T} |x\rangle \otimes |\hat{t}\rangle$$

$H_{prop} \geq 0$

Consider the change of coordinates

$$W = \sum_{j=0}^{L} U_j \dots U_1 \otimes |j\rangle \langle j|$$

$$\Rightarrow W^\dagger |\phi\rangle = \sum_{t=0}^{T} |x\rangle \otimes |\hat{t}\rangle$$

$$\Rightarrow W^\dagger H_{prop,t} W = I \otimes \left(|\widehat{t}\rangle \langle \widehat{t}| + |\widehat{t-1}\rangle \langle \widehat{t-1}| - |\widehat{t}\rangle \langle \widehat{t-1}| - |\widehat{t-1}\rangle \langle \widehat{t}| \right)$$

Analysis of H_{prop} cont.

$$\Rightarrow W^{\dagger} H_{prop,t} W = I \otimes \left(|\widehat{t}\rangle \langle\widehat{t}| + |\widehat{t-1}\rangle \langle\widehat{t-1}| - |\widehat{t}\rangle \langle\widehat{t-1}| - |\widehat{t-1}\rangle \langle\widehat{t}| \right)$$

Analysis of H_{prop} cont.

$$\Rightarrow W^\dagger H_{prop,t} W = I \otimes \left(|\widehat{t}\rangle\langle\widehat{t}| + |\widehat{t-1}\rangle\langle\widehat{t-1}| - |\widehat{t}\rangle\langle\widehat{t-1}| - |\widehat{t-1}\rangle\langle\widehat{t}| \right)$$

$$\Rightarrow W^\dagger H_{prop} W = 2 \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & & & & \\ -\frac{1}{2} & 1 & -\frac{1}{2} & & & \\ & -\frac{1}{2} & 1 & \ddots & & \\ & & \ddots & \ddots & -\frac{1}{2} & \\ & & & -\frac{1}{2} & 1 & -\frac{1}{2} \\ & & & & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Analysis of H_{prop} cont.

$$\Rightarrow W^\dagger H_{prop,t} W = I \otimes \left(|\widehat{t}\rangle\langle\widehat{t}| + |\widehat{t-1}\rangle\langle\widehat{t-1}| - |\widehat{t}\rangle\langle\widehat{t-1}| - |\widehat{t-1}\rangle\langle\widehat{t}| \right)$$

$$\Rightarrow W^\dagger H_{prop} W = 2 \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & & & & \\ -\frac{1}{2} & 1 & -\frac{1}{2} & & & \\ & -\frac{1}{2} & 1 & \ddots & & \\ & & \ddots & \ddots & -\frac{1}{2} & \\ & & & -\frac{1}{2} & 1 & -\frac{1}{2} \\ & & & & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$\Rightarrow \lambda(W^\dagger H_{prop} W) = 0$;
$\lambda_2(W^\dagger H_{prop} W)$ is inverse polynomially bounded away from 0

Projection Lemma

Let H_1, H_2 be local Hamiltonians where $H_2 \geq 0$. Let $K = \ker H_2$.

$$\exists J = \frac{\text{poly}(\|H_1\|)}{\lambda_2(H_2)}$$

$$\lambda(H_1\big|_K) - \frac{1}{8} \leq \lambda(H_1 + JH_2) \leq \lambda(H_1\big|_K)$$

Use of projection lemma

By applying the projection lemma iteratively,

$$\lambda(H_{out}\big|_K) - \frac{3}{8} \leq \lambda(H_{out} + J_{in}H_{in} + J_{clock}H_{clock} + J_{prop}H_{prop}) \leq \lambda(H_{out}\big|_K)$$

where $K = \text{span}\{\sum_{t=0}^{T} U_t \ldots U_1 \ | x\rangle \otimes \ | \hat{t}\rangle\}$

$\square$