Quantum Algorithms
Lecture 28
The quantum analogue of NP: the class BQNP II

Zhejiang University

Local Hamiltonian is BQNP-complete

Theorem

The problem local Hamiltonian is BQNP-complete with respect to the Karp reduction.

In other words, each problem that belongs to BQNP can be reduced to the local Hamiltonian problem.

Main idea

The main idea goes back to Feynman: replacing a unitary evolution by a time independent Hamiltonian (i.e., transition from the circuit to a local Hamiltonian).

Thus, suppose we have a circuit $U = U_L \cdots U_1$ of size L. We will assume that U acts on N qubits, the first m of which initially contain Merlin's message $|\xi\rangle$, the rest being initialized by 0. The gates U_j act on pairs of qubits.

Proof steps

- The Hamiltonian associated with the circuit
- Change of basis
- Existence of a small eigenvalue if the answer is “yes”
- Lower bound for the eigenvalues if the answer is “no”
- Realization of the counter

The Hamiltonian associated with the circuit

Structure

- Two spaces – first for circuit (Hamiltonian) + second for counter: $\mathcal{L} = \mathcal{B}^{\otimes N} \otimes \mathbb{C}^{L+1}$
- Three terms of Hamiltonian:

$$H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$$

- Finding minimum eigenvalue – cost function:

cost function $f(|\eta\rangle) = \langle\eta|H|\eta\rangle$

- $|\xi\rangle$ causes U to output 1 with high probability, relation with minimizing vector $|\eta\rangle$:

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{j=0}^{L} U_j \cdots U_1 |\xi, 0\rangle \otimes |j\rangle$$

Structure

- H_{in} collects penalties

$$H_{\text{in}} = \left(\sum_{s=m+1}^{N} \Pi_s^{(1)} \right) \otimes |0\rangle\langle 0|$$

- Output, first qubit should be in state $|1\rangle$, otherwise will be penalty

$$H_{\text{out}} = \Pi_1^{(0)} \otimes |L\rangle\langle L|$$

- Propagation through circuit: Transition from $j-1$ to j

$$H_{\text{prop}} = \sum_{j=1}^{L} H_j$$

$$H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$$

Change of basis

Ideas

Measuring operator W is used to change the basis.

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

- H_{in} is not changed
- H_{out} $$\widetilde{H}_{\text{out}} = W^\dagger H_{\text{out}} W = \left(U^\dagger \Pi_1^{(0)} U\right) \otimes |L\rangle\langle L|$$
- H_{prop}: each H_j consists of 3 terms, authors analyze them, result: $$\widetilde{H}_{\text{prop}} = W^\dagger H_{\text{prop}} W = I \otimes E,$$

$$E = \sum_{j=1}^{L} E_j = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & & & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & & \\ & -\frac{1}{2} & 1 & -\frac{1}{2} & \\ 0 & & -\frac{1}{2} & \ddots & \ddots \\ & & & \ddots & \ddots \end{pmatrix}$$

Existence of a small eigenvalue if the answer is “yes”

Ideas

Authors start analysis with this probability:

$$\mathbf{P}(0) = \langle \xi, 0 | U^\dagger \Pi_1^{(0)} U | \xi, 0 \rangle \leq \varepsilon$$

$f(|\tilde{\eta}\rangle) = \langle \tilde{\eta} | \widetilde{H} | \tilde{\eta} \rangle$ minimum is at eigenvector, find with small eigenvalue.

Counter is initialized in equal superposition:

$$|\psi\rangle = \frac{1}{\sqrt{L+1}} \sum_{j=0}^{L} |j\rangle$$

Analysis of values

$$f(|\tilde{\eta}\rangle) = \langle\tilde{\eta}|\widetilde{H}|\tilde{\eta}\rangle$$

- For H_{in} the value will be 0
- For H_{prop} the value will be 0
- For H_{out}:

$$\mathbf{P}(0)\,\frac{1}{L+1} \leq \frac{\varepsilon}{L+1}$$

And this contributes to the result – which gives us an upper bound for answer “yes”.

Lower bound for the eigenvalues if the answer is “no”

Starting ideas

For answer “no” for any vector |ξ⟩:

$$\langle \xi, 0 | U^\dagger \Pi_1^{(0)} U | \xi, 0 \rangle \geq 1 - \varepsilon$$

In such case all eigenvalues for H are

$$\geq c\,(1 - \sqrt{\varepsilon})\,L^{-3}$$

The Hamiltonian is analyzed in the following way: $\widetilde{H} = A_1 + A_2$. $A_1 = \widetilde{H}_{in} + \widetilde{H}_{out}$, $A_2 = \widetilde{H}_{prop}$.

Authors obtain lower bounds for nonzero eigenvalues: 1 for A_1 and $c'L^{-2}$ for A_2.

For smallest eigenvalue of $A_1 + A_2$ authors analyze the angle between the null subspaces.

Lemma

Let A_1, A_2 be nonnegative operators, and L_1, L_2 their null subspaces, where $L_1 \cap L_2 = \{0\}$. Suppose further that no nonzero eigenvalue of A_1 or A_2 is smaller than v. Then

$$A_1 + A_2 \geq v \cdot 2\sin^2 \frac{\vartheta}{2}$$

where $\vartheta = \vartheta(L_1, L_2)$ is the angle between L_1 and L_2.

Lemma outcome

We will get the estimates 1 and $c'L^{-2}$ for the nonzero eigenvalues of A_1 and A_2 (as already mentioned), and $\sin^2\vartheta \geq (1-\sqrt{\varepsilon})/(L+1)$ for the angle. From this we derive the desired inequality

$$H \geq c(1-\sqrt{\varepsilon})\, L^{-3}$$

Realization of the counter

Issue of degree of locality

Counter can be represent by $O(logL)$ qubits, but then the Hamiltonian would be only $O(logL)$-local, not $O(1)$-local. Remember, we solve k-local Hamiltonian problem.

Authors use the embedding $C^{L+1} \to B^L$.

$$|j\rangle \mapsto |\underbrace{1,\ldots,1}_{j},\underbrace{0,\ldots,0}_{L-j}\rangle$$

The operators on C^{L+1} are replaced. Result is 5-local Hamiltonian.

Remark – this is why 5-local Hamiltonian is QMA-complete, later improved to 2-local.

Analysis

Solution has been adapted for new counter, now Hamiltonian is H_{ext} . Counter now has extended space and unused states, additional term for Hamiltonian is used:

$$H_{\text{stab}} = I_{\mathcal{B}^{\otimes N}} \otimes \sum_{j=1}^{L-1} \Pi_j^{(0)} \Pi_{j+1}^{(1)}$$

Analysis shows that for answer “yes” there are no changes, and for answer “no”:

$$H_{\text{ext}} + H_{\text{stab}} \geq c(1 - \sqrt{\varepsilon}) L^{-3}$$

The place of BQNP among other complexity classes

Introduction

It follows directly from the definition that the class BQNP contains the class MA (and so also BPP and NP). Nothing more definitive can be said at present about the strength of “nondeterministic quantum algorithms”.

Nor can much more be said about its “weakness”.

BQNP ⊆ PSPACE

The maximum probability that Merlin's message will be accepted by Arthur is equal to the maximum eigenvalue of the operator

$$X^{(a)} = \mathrm{Tr}_{[m+1,\ldots,N]}\left(U^\dagger \Pi_1^{(a)} U \left(I_{\mathcal{B}^{\otimes m}} \otimes |0^{N-m}\rangle\langle 0^{N-m}|\right)\right)$$

We will need to compute this quantity with precision $O(n^{-\alpha})$, $\alpha > 0$.

It suffices to compute the trace of the d-th power of X, with d polynomial in m. It is achieved with polynomial memory.

BQNP ⊆ PP

Proof is similar to the proof of

BPP ⊆ BQP ⊆ PP ⊆ PSPACE

The class PP consists of predicates of the form

$$Q(x) = \Big(\big| \{ y : R_0(x,y) \} \big| < \big| \{ y : R_1(x,y) \} \big| \Big)$$

where $R_0, R_1 \in P$, and y runs through all words of length bounded by some polynomial $q(x)$.

One more remark

A quantum game with three messages (i.e., 1.5 rounds) has the same complexity as the game with polynomially many rounds. The corresponding complexity class is called QIP; it contains PSPACE (and is equal to PSPACE). This contrasts with the properties of classical Arthur-Merlin games. In the classical case, the game with polynomially many rounds yields PSPACE. But in wide circles of narrow specialists the opinion prevails that no fixed number of rounds would suffice.

It is widely believed that “the polynomial hierarchy does not collapse”, i.e., co-NP = $\Pi 1 \subset \Pi 2 \subset \Pi 3 \subset \cdots \subset$ PSPACE (the inclusions are strict)

QIP classes

- QIP with one message = QMA,
- QIP with two messages
- QIP with 3 and more messages = QIP

QIP = IP = PSPACE

Thank you for your attention!