QALCO: Quantum Algorithms and Complexity **2025 - 2026**

Exercises - Lecture 5

Lecturer: Alex B. Grilo

Exercise 1 (Choice of gatesets)**.** Let $\mathcal{G}$ be a set of quantum gates. We say that $\mathcal{G}$ is *universal*, if every unitary U can be approximated by a circuit composed by gates $\mathcal{G}$ up to an arbitrary desired precision. Maybe surprisingly, there are finite universal gatesets! For examples, the following set is universal for quantum computing:

$$\left\{ P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\pi/4} \end{bmatrix}, H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}, CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \right\}.$$

The Solovay-Kitaev theorem is a fundamental result comparing different gatesets.

Theorem 1 (Solovay-Kitaev theorem)**.** *Fix some constant $d \in \mathbb{N}$. Let $\mathcal{G}$ be a subset of unitary matrices in a d-dimensional Hilbert space that is universal and closed under inversions. Then any d-dimensional unitary operator U can be approximated within precision ε using $O(polylog(1/\varepsilon))$ gates in $\mathcal{G}$. Moreover, this can be done in (classical) polynomial-time.*

1. Let $\mathcal{G}$ and $\mathcal{G}'$ be two universal gatesets that contain gates acting on a d-dimensional Hilbert space, for some $d = O(1)$. Show that if a problem L can be decided in quantum polynomial-time using gates in $\mathcal{G}$, then L can be also decided in quantum polynomial-time using gates in $\mathcal{G}'$.

2. Show that BQP is invariant to universal gatesets.

Exercise 2 (Using BQP algorithms as subroutine of other BQP algorithms [1])**.**

1. Show that if $P \in \mathsf{BQP}$, then there exists a quantum circuit that on input $|x, 0, 0^a\rangle$, it outputs $|\psi\rangle$ such that
$$|\langle x, f(x), 0^a|\psi\rangle|^2 = 1 - 2^{-n^c},$$
where $f(x) = 0$ if x is a no-instance and $f(x) = 1$ if x is a yes-instance.

2. Suppose that P' can be solved by a BQP algorithm with oracle access to P. Then If P is in BQP, then so is P'.

3. Show that $\mathsf{BQP}^{\mathsf{BQP}} = \mathsf{BQP}$.

Exercise 3 (Error reduction for QMA verification)**.** In this exercise, we will show that the choice of the completeness and soundness parameters for QMA can be chosen to have exponentially small error (as BQP – see Exercise 3 of Exercise List 5.). Let V be the circuit corresponding to a QMA protocol for a problem $L = (L_{yes}, L_{no})$ with completeness $2/3$ and soundness $1/3$. Show that there exists a QMA verification V' such that:

1. if $x \in L_{yes}$, $\exists$ a quantum proof that makes V' accept x with probability at least $1 - 2^{-n^c}$.

2. if $x \in L_{no}$, all quantum proofs make V' accept x with probability at most 2^{-n^c}.

Hint: Consider the parallel repetition of V and use Chernoff bound (see Appendix A).

[1] This exercise was taken from the lecture notes of Ronald de Wolf [1]

Exercise 4 (Group non-membership)**.** Suppose that we are given a finite group $(G, *)$, [2] a subgroup $(H, *)$, an element $g \in G$, and that we have a unitary map $V : |h_1\rangle |h_2\rangle \to |h_1\rangle |h_1 * h_2\rangle$, where $h_1, h_2 \in G$. We will show a simplified version of the statement that deciding if $g \notin H$ is in QMA. In particular, we will assume that the given proof is of the form $|H\rangle = \frac{1}{|H|} \sum_{h \in H} |h\rangle$.

1. Show that if $g \in H$, then $V(|g\rangle |H\rangle) = |g\rangle |H\rangle$.
2. Show that if $g \notin H$, then $\langle g| \langle H| V(|g\rangle |H\rangle) = 0$.

Consider the following procedure

(A) Prepare state $|+\rangle |g\rangle |H\rangle$.

(B) Conditioned on the first qubit, apply the unitary V on the last two registers.

(C) Apply Hadamard on the first qubit and measure it. Accept iff the output is $|1\rangle$.

which is a simplified QMA verification for group non-membership.

3. Show that if $g \notin H$, the procedure accepts with probability $\frac{1}{2}$.
4. Show that if $g \in H$, the procedure accepts with probability 0.

Exercise 5 (QMA-completeness of the Local Hamiltonian problem)**.** Let us consider again the Local Hamiltonian instance H_C that comes from the circuit verification $C = U_T ... U_1$. Remember that this circuit comes from a QMA verification, and we asssume that if x is a yes-instance, then there exists some $|\psi\rangle$ such that $||(|1\rangle \langle 1| \otimes I)C |x\rangle |\psi\rangle |0\rangle^{\otimes q(|x|)} ||^2 \geq 1 - 2^{-n}$; and if x is a no-instance, then for all $|\psi\rangle$, we have that$||(|1\rangle \langle 1| \otimes I)C |x\rangle |\psi\rangle |0\rangle^{\otimes q(|x|)} ||^2 \leq 2^{-n}$.
Let $m = T + n + q + 2$. We define

$$H_C = \frac{1}{m} \left(H^{out} + \left(\sum_{j \in [q]} H_j^{init} \right) + \left(\sum_{j \in [n]} H_j^{input} \right) + \left(\sum_{t \in [T]} H_t^{prop} \right) + H_{T+1}^{prop} \right). \tag{1}$$

initialization For $j \in [q]$, $H_j^{init} = |0\rangle \langle 0|_C \otimes |1\rangle \langle 1|_{A_j}$, and for $j \in [n]$, $H_j^{input} = |0\rangle \langle 0|_C \otimes |\overline{x_j}\rangle \langle \overline{x_j}|_{I_j}$,

propagation Let G_t be the set of qubits on which U_t acts non-trivially.
$H_0^{prop} = \frac{1}{2} \Big(|0\rangle \langle 0|_C \otimes I_{G_1} + |1\rangle \langle 1| \otimes I - |1\rangle \langle 0| \otimes U_1 - |0\rangle \langle 1| \otimes U_1^\dagger \Big)$
$H_T^{prop} = \frac{1}{2} \Big(|T-1\rangle \langle T-1|_C \otimes I_{G_{T-1}} + |T\rangle \langle T| \otimes I - |T\rangle \langle T-1| \otimes U_{T-1} - |T-1\rangle \langle T| \otimes U_T^\dagger \Big)$
For $1 \leq t \leq T-1$,
$H_t^{prop} = \frac{1}{2} \Big(|t-1\rangle \langle t-1|_C \otimes I_{G_t} + |t\rangle \langle t| \otimes I - |t\rangle \langle t-1| \otimes U_t - |t-1\rangle \langle t| \otimes U_t^\dagger \Big)$.

output $H^{out} = |T\rangle \langle T|_C \otimes |0\rangle \langle 0|_O$.

In this definition, we have that the register C corresponds to the clock register (as seen in class), the register A_j corresponds to the j-th ancilla qubit; the register I_j corresponds to the j-th bit of the instance; the register G_i corresponds to the qubits touched by the gate i.

1. Show that if $C_{|x|}$ accepts x with probability $1 - \varepsilon$ on quantum proof $|\psi\rangle$, then

$$| \langle \mathsf{hist}| H |\mathsf{hist}\rangle | \leq \frac{\varepsilon}{m}, \tag{2}$$

for $|\mathsf{hist}\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=\{0,...,T\}} |t\rangle \otimes U_t ... U_1 (|x\rangle |\psi\rangle |0\rangle^{\otimes q})$. Notice that this prove the completeness part of QMA-hardness of the local Hamiltonian problem.

[2] See Appendix B for a reminder of the definition of groups and subgroups.

Let us now define the state $|\psi\rangle = \sum_{t\in\{0,\dots,T\}} \alpha_t |t\rangle \otimes |\phi_t\rangle$ and let us assume $\alpha_t \in \mathbb{R}$ for simplicity.

2. Show that if $\sum_{t\in\{0,\dots,T\}} |\alpha_t - \alpha_{t+1}|^2 \geq \delta$, then

$$|\langle\psi| H |\psi\rangle| \geq \frac{\delta}{m}. \tag{3}$$

Let us now redefine the state $|\psi'\rangle = \frac{1}{\sqrt{T+1}} \sum_{t\in\{0,\dots,T\}} |t\rangle \otimes |\phi_t\rangle$, where $|\phi_t\rangle$ is an arbitrary (normalized) quantum state.

3. Show that if there exists one t such that $|\langle\phi_t| U_t |\phi_{t-1}\rangle| \leq 1-\delta$, then

$$|\langle\psi'| H |\psi'\rangle| \geq \frac{\delta}{mT}, \tag{4}$$

4. Show that if $|\langle x| \otimes I \otimes \langle 0|^{\otimes q} |\phi_0\rangle| \leq 1-\delta$, then

$$|\langle\psi'| H |\psi'\rangle| \geq \frac{\delta}{mT}, \tag{5}$$

5. Show that if $|\langle 0| \otimes I |\phi_T\rangle|^2 \leq 1-\delta$, then

$$|\langle\psi'| H |\psi'\rangle| \geq \frac{\delta}{mT}, \tag{6}$$

6. (Challenge) Prove that if for every $|\psi\rangle$, $C_{|x|}$ accepts x with probability at most 2^{-n^c} on the quantum proof $|\psi\rangle$, then for every $|\phi\rangle$, $\langle\phi| H |\phi\rangle \geq \Omega\left(\frac{1}{T^6}\right)$.

A Chernoff bound

Theorem 2 (Chernoff bound)**.** *Let $X_1, \dots, X_m \in \{0,1\}$ be random variables such that for each $i = 1, ..., m$ we have that*

$$X_i = \begin{cases} 1, & \textit{with probability } p \\ 0, & \textit{with probability } 1-p \end{cases}.$$

Let also $X = \sum_{i=1}^m X_i$ and $\mu = \mathbb{E}[X] = pm$. We have that for any $0 \leq \delta \leq 1$,

$$Pr\left(|X-\mu| \geq \mu\delta\right) \leq e^{-\delta^2\mu/3}.$$

B Groups

We remind that a group $(G, *)$ is composed by a set G and a binary operation $* : G \times G \to G$, with the following properties

1. Associativity: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
2. Identity element: $\exists e \in G, \forall a \in G$, $e * a = a * e = a$.
3. Inverse element: $\forall a \in G, \exists b \in G$, $a * b = b * a = e$.

A subgroup $(H, *)$ is a subgroup of $(G, *)$ if $H \subset G$ and $(H, *)$ is a group.

References

[1] Ronald de Wolf. Quantum computing: Lecture notes, 2019.