EITQ TD: Quantum(-related) complexity

Renaud Vilmart
renaud.vilmart@inria.fr

1 QMA-Completeness

We consider here two decision problems:

1. **Non-Identity Check**
   Setup: A quantum circuit C that implements an (unknown) unitary U.
   Question: Does $U \neq e^{\mathbf{i}\phi}\text{Id}$ for all ϕ?

2. **Non-Equivalence Check**
   Setup: Two quantum circuits C_1 and C_2 that implement respectively U_1 and U_2.
   Question: Does $U_1 \neq e^{\mathbf{i}\phi}U_2$ for all ϕ?

Question 1. Is one of the two problems a sub-problem of the other?

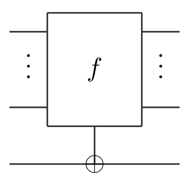
Question 2. Provide a polynomial reduction from the non-equivalence check problem to the non-identity check problem.

Question 3. Assuming the non-identity check problem is QMA-complete, show that the Non-Equivalence check problem is also QMA-complete.

2 Hermiticity Checking is coNP-hard

We are interested here in the following problem:
Setup: A circuit C built using gate set $\langle H, P(\alpha), \text{CNot}\rangle_{\alpha\in\mathbb{R}}$.
Question: Does C implement a Hermitian matrix?

Let f be a SAT formula. We define circuit C_f, represented as:



and which maps classical data as follows:

$$U_f|x_1, ..., x_n, y\rangle \mapsto |x_1, ..., x_n, y \oplus f(x_1, ..., x_n)\rangle$$

Question 1. Show that matrix U_f is block-diagonal (when taking the usual convention that A above B represents $A \otimes B$). What are the blocks on the diagonal, depending on the values of f?

Question 2. What is the matrix implemented by the circuit C'_f built from C_f by adding a Pauli Z gate on the last qubit at the end?

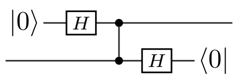
Question 3. Is Z Hermitian? Is ZX Hermitian? Then show that C'_f implements a Hermitian matrix iff f has no solution.

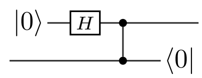
Question 4. Assuming that the unsatisfiability problem UNSAT (deciding if f has no solution) is **co-NP-complete**; and that C_f can be built from f using a number of gates drawn from $\langle H, P(\alpha), \text{CNot}\rangle_{\alpha\in\mathbb{R}}$ that is polynomial in the size of f, show that Hermiticity-checking is **co-NP-hard**.

Question 5. What can we say about the complexity of checking whether a circuit C implements an involutive matrix (i.e. $U \circ U = \text{Id}$)?

3 Unitarity Checking is coNP-hard

Question 1. Compute the operators implemented by the following circuits with postselections:

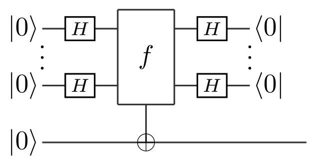




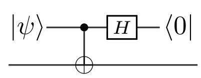
Are they unitary?

Let f be a SAT formula on n variables, and s be the number of variable assignments that satisfy f. We first want to encode the s into a quantum state $|\psi\rangle$ (using postselections).

Question 2. Show that the following circuit implements $|\psi\rangle := \frac{1}{N}\big((2^n - s)|0\rangle + s|1\rangle\big)$:



Question 3. What operator is implemented by the following circuit:

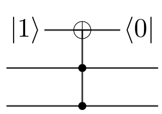


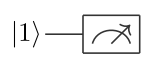
Check that it is unitary iff $s = 0$ or $s = 2^n$.

Question 4. Using the fact that UNSAT is a **coNP-complete** problem, conclude on the hardness of checking unitarity of circuits with postselections.
Hint: don't forget to deal with the $s = 2^n$ case.

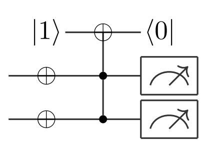
4 The Power of a Single Postselection

Question 1. Explain the behaviour of the following circuits (compute what they implement if you need), and provide an equivalent simplified circuit for each:





Question 2. Use the above to show that the following circuit is equivalent to 2 postselections in $\langle 0|$:



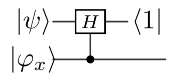
Question 3. Show that having a single postselection is as strong as having arbirarily many postselections.

5 PP $\subseteq$ PostBQP

Let f be a SAT formula on n variables, and s be the number of variable assignments that satisfy f. The majority problem asks whether $s < 2^{n-1}$ or $s \geq 2^{n-1}$.

We assume we know how to create state $|\psi\rangle$ from f as in Question 2 from Exercise 3.

Question 1. Let $|\varphi_x\rangle$ be the arbitrary state $\frac{1}{N}(|0\rangle + x|1\rangle)$ where N is a normalisation factor. Compute the state $|\psi_x\rangle$ created by the following circuit:



We then reason w.r.t. the value of s.

Question 2. If $s < 2^{n-1}$, explain which i maximises $\langle +|\psi_{2^i}\rangle$. Notice that for such i, if $|\psi_{2^i}\rangle = \alpha|0\rangle + \beta|1\rangle$, then α is within $\beta/2$ and 2β. Infer a lower bound on $\langle +|\psi_{2^i}\rangle$.

Question 3. If $s \geq 2^{n-1}$, show that for all $i \in [\![-n, n]\!]$, $|\langle +|\psi_{2^i}\rangle| \leq \frac{1}{\sqrt{2}} \simeq 0.707$.

Question 4. Using the above, come up with a polynomial time algorithm that decides the majority problem. Conclude on the interaction between **PP** and **PostBQP**.