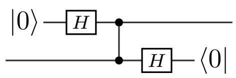
EITQ TD: Quantum(-related) complexity

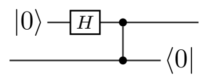
Renaud Vilmart
renaud.vilmart@inria.fr

November 6, 2024

1 Unitarity Checking is coNP-hard

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

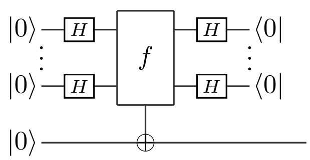




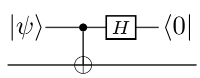
Are they unitary?

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:

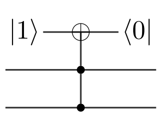


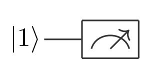
Check that it is unitary iff $s = 0$ or $s = 2^n$.

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.*

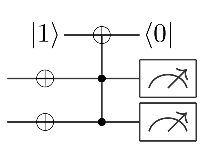
2 The Power of a Single Postselection

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 $\langle 0|$:



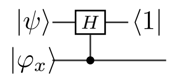
Question 3. Show that having a single postselection is as strong as having arbirarily many postselections.

3 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 1.

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 start with $|\psi\rangle \otimes |\varphi_x\rangle = \frac{1}{N'}((2^n - s)|00\rangle + s|10\rangle + x(2^n - s)|01\rangle + xs|11\rangle$. After application of the controlled-H gate, we have:

$$\frac{1}{N'}\left((2^n - s)|00\rangle + s|10\rangle + \frac{x(2^n - s) + xs}{\sqrt{2}}|01\rangle + \frac{x(2^n - s) - xs}{\sqrt{2}}|11\rangle\right)$$

After postselection of the first qubit in $|1\rangle$, we have:

$$|\psi_x\rangle = \frac{1}{N''}\left(s|0\rangle + \frac{x(2^n - 2s)}{\sqrt{2}}|1\rangle\right)$$

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

Question 2. If $s < 2^{n-1}$, explain how to pick i that 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 $\langle +|\psi_{2^i}\rangle$.

If $s < 2^{n-1}$, and $x = 2^i$, then both amplitudes are positive. To maximise $\langle +|\psi_{2^i}\rangle$ we want both amplitudes to be as close as possible, hence ideally $i = \log_2\left(\frac{s\sqrt{2}}{2^n - 2s}\right)$. i has to be an integer, so we simply round this value to get the best value.

With the above observation, $\langle +|\psi_{2^i}\rangle$ has to be at least as big as both $\langle +|\varphi_2\rangle$ and $\langle +|\varphi_{1/2}\rangle$, both of which are $\frac{3}{\sqrt{10}} \geq 0.948$. Hence $\langle +|\psi_{2^i}\rangle \geq 0.948$.

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

If $s \geq 2^{n-1}$, for all values of i, the second amplitude of $|\psi_{2^i}\rangle$ is non-positive while the first is positive. There exists θ such that $|\psi_{2^i}\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$. Then:

$$|\langle +|\psi_{2^i}\rangle| = \frac{1}{\sqrt{2}}|\cos\theta - \sin\theta| \leq \frac{1}{\sqrt{2}} \simeq 0.707$$

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**.

If $s < 2^{n-1}$, there exists $i \in [-n, n]$ such that $|\langle +|\psi_{2^i}\rangle|^2 \geq 0.9$, however if $s \geq 2^{n-1}$ then for all i, $|\langle +|\psi_{2^i}\rangle|^2 \leq 0.5$. For each i between $-n$ and n, we build the state $|\psi_{2^i}\rangle$ and measure it in the X basis. We do so n times, so that we can discriminate between the two possibilities with exponentially good certainty. We hence run the circuit $n(2n+1)$ times, i.e. we have a polynomial-sized algorithm with postselections that solve the majority problem.

Since this problem is **PP-complete** and we have a polynomial reduction from this problem to a **PostBQP** problem, we can conclude that **PP** $\subseteq$ **PostBQP**.

4 Simulation via Perfect Matchings

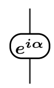
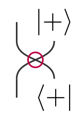
We want to show here how to turn any quantum circuit composed of the usual gates and postselections: $\mathcal{G} = \{H, P(\alpha), \mathrm{CNot}, |0\rangle, \langle 0|\}_{\alpha\in\mathbb{R}}$, which implement respectively:

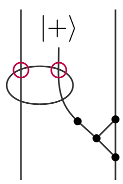
$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \begin{pmatrix}1 & 0\\ 0 & e^{i\alpha}\end{pmatrix} \qquad \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \qquad \begin{pmatrix}1\\ 0\end{pmatrix} \qquad \begin{pmatrix}1 & 0\end{pmatrix}$$

Question 1. Remind how we implement $|0\rangle$ and $\langle 0|$.

They are respectively and its upside-down version.

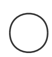
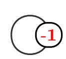
Let's first assume that our tensor networks allow the $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ state.

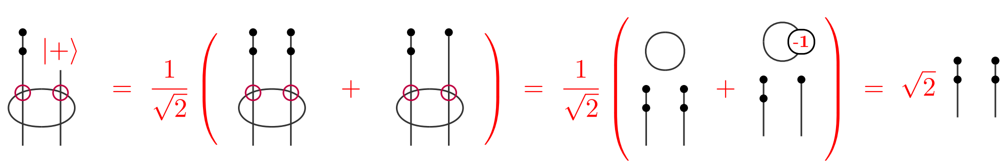
Question 2. Show that  implements $P(\alpha)$. Same question with  that implements $\sqrt{2}\cdot H$ and

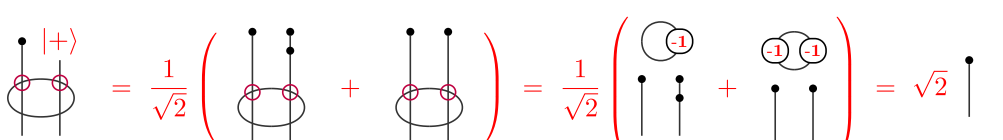
 that implements $\sqrt{2}\cdot\mathrm{CNot}$.

If the edge is part of the matching, we count the weight, otherwise we don't. In other words, the first diagram sends $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $e^{i\alpha}|1\rangle$, which is exactly $P(\alpha)$.

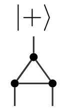
$\langle +|$ in terms of perfect matchings, always accepts the "value" of its input edge, i.e. no matter if it is in the matching or not. In the second diagram, if at least one of the edges is not in the matching, then we accept, without changing the overall scalar. If both edges are in the matching, the "fermionic swap" creates a -1 scalar, but the configuration is also accepted. We hence have something that implements $\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ which is $\sqrt{2}\cdot H$.

For CNot, notice first that  and  represent respectively the 2 and 0 scalars. Indeed, a closed loop can either be or not in a matching (as it is not connected to an edge), so it amounts to 2 possibilities. In the second case, these two possibilities cancel out due to the -1 parameter. Using the fact that $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, we can check the following:





In other words, the gadget copies whether the input edge is in the matching or not, into both outputs. If the left edge in the diagram for CNot is not in the matching, we can then check that the second input edge is in the matching iff the second output edge also is. On the other hand, if the right edge is in the matching, we can check that the second input edge is in the matching iff the second output edge is not. This implements CNot (up to the $\sqrt{2}$ scalar from the copy gadget).

Question 3. Show that 

implements $\sqrt{2}|++\rangle$. Explain how we can get rid of all but 1 occurrence of $|+\rangle$.

Checking the equality is direct using the same decomposition of $|+\rangle$ as above. Then, given a diagram, as long as there are at least 2 occurrences of $|+\rangle$, we can use this equality from right to left to replace them with a single occurrence of $|+\rangle$ and 3 additional nodes. We only stop when one occurrence of $|+\rangle$ is left.

Question 4. Suppose we have a circuit C implementing U and we want to compute the amplitude $\langle 0...0|U|0...0\rangle$. Explain how we can turn this quantity into a tensor network with a single $|+\rangle$.

What is the number of perfect matchings in a graph with an odd number of vertices? Noticing that $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, explain how we can get rid of the last $|+\rangle$.

Assuming C is only composed of Hadamard, Phase and CNot gates, we can turn it in a graph (with input and output edges) with $|+\rangle$s using the results from Question 2. The pre and post-selection in $|0...0\rangle$ can be represented as pieces of graphs (Question 1). We can plug those on all the input/output edges of the graph, to get a graph (without input/output edges this time), but with several occurrences of $|+\rangle$. Using Question 3, we can get rid of all but 1 occurrence of $|+\rangle$.

In a graph with an odd number of vertices, the number of perfect matchings is necessarily 0, since not all vertices can be paired with another. $|0\rangle$ is represented by a pair of vertices, while $|1\rangle$ is represented by a single vertex. Hence, if we replace the last $|+\rangle$ by the sum of the two, one of the resulting diagrams will have an odd number of vertices, which can be checked efficiently. The contribution of this graph will be 0, so in the end computing $\langle 0...0|U|0...0\rangle$ amounts to computing the number of perfect matchings in the graph with an even number of vertices.