CSE 291 / Math 277 - Quantum Complexity Theory (Fall 2024)
Homework 6
Due Thursday, November 14, 3:00pm

Note: It is highly recommended (though not required) that you type your answers. It is
your responsibility to make any handwriting clear and legible for grading. You may work
with 1-2 other collaborators, but you must write the solutions separately and clearly mark
the names of each person you worked with.

Problems:

1. **Postselection is powerful**

   Quantum measurements are inherently probabilistic, but what if they weren't? That
   is, what is the power of quantum mechanics when we get to choose or *postselect* which
   measurement outcome we get, regardless of how small the probability is of actually
   measuring that outcome. In this problem, we will explore the computational power of
   such a model of quantum computation. While this model of computation may sound
   somewhat strange, we will see later that it turns out to be surprisingly relevant to the
   story of quantum advantage.

   Let's try to formally define a quantum postselection class. First, let's fix a gate set of
   "reasonable" gates, say, with algebraic entries.

   Postselected Bounded Error Quantum Polynomial Time ($\mathsf{PostBQP}$)
   The class of languages L such that there is a poly-uniform family of polynomial-size
   quantum circuits $\{Q_n\}_{n=1}^{\infty}$ such that for all $x \in \{0,1\}^n$:

   (a) The probability of measuring $|1\rangle$ on the first qubit of $Q_n |x\rangle |0\cdots 0\rangle$ is nonzero.

   (b) If $x \in L$, then conditioned on the first qubit being $|1\rangle$, the probability of measuring
       $|1\rangle$ on the second qubit is at least $2/3$.

   (c) If $x \notin L$, then conditioned on the first qubit being $|1\rangle$, the probability of measuring
       $|1\rangle$ on the second qubit is at most $1/3$.

   We will eventually show that this class is extremely powerful, equal to the complexity
   class PP. For now, let's warm up with a simpler inclusion:

   (a) Show that $\mathsf{NP} \subseteq \mathsf{PostBQP}$.

       Hint: Show that you can find a solution to any polynomially computable function
       $f \colon \{0,1\}^n \to \{0,1\}$. *It should be intuitive that if you can postselect on a par-*
       ticular measurement outcome, then you should be able to postselect on seeing a
       solution to f. Fitting this into the definition of $\mathsf{PostBQP}$ requires some care since
       your postselection must always succeed (c.f., Condition (a) in the definition of
       $\mathsf{PostBQP}$).

   Our goal for the remainder of this problem is to show that in fact $\mathsf{PostBQP} = \mathsf{PP}$. The
   inclusion $\mathsf{PostBQP} \subseteq \mathsf{PP}$ follows immediately from our previous proof that $\mathsf{BQP} \subseteq \mathsf{PP}$,

so let's focus on the other direction. We will use the fact that a complete problem for PP is determining if some polynomially computable function $f\colon \{0,1\}^n \to \{0,1\}$ has fewer than 2^{n-1} solutions. Let $s \in \mathbb{N}$ be the number of solutions to f. It will be useful in the proof to assume that $s > 0$, so let's make that assumption (though this is not required).

We start by preparing the state

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\, |f(x)\rangle\,.$$

(b) Write the single-qubit state $|\psi\rangle$ on the second register you obtain after applying Hadamard gates to the first n qubits and postselecting on them being the state $|0^n\rangle$. The amplitudes on $|0\rangle$ and $|1\rangle$ should be in terms of s and n. Remember that $|\psi\rangle$ should be properly normalized.

Note: This procedure might seem somewhat strange since we're postselecting on n qubits rahter than a single qubit as indicated in the defintion PostBQP. *Notice, however, that we could apply an OR gate to the first n qubits, and postselect on the output of that OR function being $|0\rangle$.*

Our next step will be to prepare the state $\alpha\,|0\rangle\,|\psi\rangle + \beta\,|1\rangle\,H\,|\psi\rangle$ for some $\alpha, \beta \in \mathbb{R}^+$ to be chosen later. Here, H is the usual Hadamard gate.

(c) Staring with the state $\alpha\,|0\rangle\,|\psi\rangle + \beta\,|1\rangle\,H\,|\psi\rangle$, show that postselecting the second qubit on being $|1\rangle$ yields the state

$$\left|\varphi_{\beta/\alpha}\right\rangle := \frac{\alpha s\,|0\rangle + (\beta/\sqrt{2})(2^n - 2s)\,|1\rangle}{\sqrt{\alpha^2 s^2 + (\beta^2/2)(2^n - 2s)^2}}$$

on the first qubit.

Our goal will be to use the $\left|\varphi_{\beta/\alpha}\right\rangle$ state to determine whether or not $s < 2^{n-1}$. Let's first consider the case where $s < 2^{n-1}$. The claim is now that a careful setting of α and β will make the $\left|\varphi_{\beta/\alpha}\right\rangle$ state close to $|+\rangle$. To get some intuition, notice that setting $\beta = 0$ implies $\left|\varphi_{\beta/\alpha}\right\rangle = |0\rangle$ and setting $\alpha = 0$ implies $\left|\varphi_{\beta/\alpha}\right\rangle = |1\rangle$. For intermediate values of α and β, notice that the amplitudes on the $|0\rangle$ and $|1\rangle$ state are positive since $2^n - 2s > 0$ whenever $s < 2^{n-1}$. In other words, as we tune β from 0 to 1, the state must cross over the $|+\rangle$ state.

(d) Suppose that $s < 2^{n-1}$. Show that there exist an $i \in \{-n, n\}$ such that when $\beta/\alpha = 2^i$, we have

$$|\langle + | \varphi_{2^i} \rangle| \geq \frac{1 + \sqrt{2}}{\sqrt{6}} \geq 0.985.$$

Hint: As we increase i, the worse case distance from $|+\rangle$ happens when $|\langle + | \varphi_{2^i} \rangle| = |\langle + | \varphi_{2^{i+1}} \rangle|$. This occurs when

$$|\varphi_{2^i}\rangle = \gamma_0\,|0\rangle + \gamma_1\,|1\rangle$$

for some γ_0, $\gamma_1 > 0$ *with* $\gamma_0^2 + \gamma_1^2 = 1$ *and*

$$|\varphi_{2^{i+1}}\rangle = \frac{\gamma_0 |0\rangle + 2\gamma_1 |1\rangle}{\sqrt{\gamma_0^2 + 4\gamma_1^2}} = \gamma_1 |0\rangle + \gamma_0 |1\rangle$$

What must γ_0 *and* γ_1 *be?*

(e) Suppose that $s \geq 2^{n-1}$. What is the largest that $|\langle +|\varphi_{2^i}\rangle|$ could possibly be for any i?

   Hint: Think about the sign of the amplitude on the $|1\rangle$ state on any $|\varphi_{2^i}\rangle$.

(f) Put everything together. That is, show there is a polynomial-time quantum algorith with postselection that can determine if $s < 2^{n-1}$. Hence, PP $\subseteq$ PostBQP.

   Hint: You may have to run the algorithm for several $|\varphi_{2^i}\rangle$.