Quantum Complexity Theory, UPB
Winter 2020, Assignment 4

To be completed by: Tuesday, December 15, start of tutorial

This assignment assumes the notation and terminology from Lectures 4 and 5.

1 Exercises

1. **A BQP-complete problem: Matrix inversion.** In this question, we assume the terminology from Section 3 of Lecture 4 of the course notes.

   (a) Recall from Lecture 4 the equation

   $$|\widetilde{x}\rangle = \frac{1}{\sqrt{m+1}}\left(|0\rangle|0^n\rangle + |1\rangle V_1|0^n\rangle + \cdots + |m\rangle V_m \cdots V_1|0^n\rangle\right).$$

   Assume, without loss of generality, that in all but the last time step, m, V sets the output qubit to $|0\rangle$, and only in time step m does V perform a CNOT to copy over its answer to the output qubit. Prove that (where recall $\Pi = |1\rangle\langle 1|$ is a single qubit projector onto the output qubit of the second register):

   - If V denotes a YES instance, then $\langle\widetilde{x}|\Pi|\widetilde{x}\rangle \geq \frac{2}{3(m+1)}$.
   - If V denotes a NO instance, then $\langle\widetilde{x}|\Pi|\widetilde{x}\rangle \leq \frac{1}{3(m+1)}$.

   (b) How can we modify V in a seemingly trivial manner in order to boost the completeness/soundness bounds of the previous exercise to constants (i.e. independent of m)?

   (c) Choose $A = I - e^{-1/m}U$ for scalar $e^{-1/m}$. Prove that now $\kappa(A) \in O(m)$ for the new definition of A. (Hint: You only need to use the fact that U is unitary, not the specific definition of U. Also, use the fact that for normal operators A, the singular values of A are $\{|\lambda(A)|\}$ (why?).)

2. **Weak error reduction for QMA.** Suppose the QMA prover sends k copies of its proof, $|\psi\rangle$, instead of a single copy. On the jth copy of the proof, the verifier runs the verification circuit Q_n. Finally, the verifier measures the output qubits of all runs of Q_n, takes a majority vote of the resulting bits, and accepts if and only if the majority function yields 1. Prove that this procedure indeed amplifies the completeness and soundness parameters for QMA. (Hint: In the NO case, a cheating prover is *not* obligated to send k copies of some state $|\psi\rangle$ in tensor product, but rather can cheat by sending a large entangled state $|\phi\rangle \in \mathcal{B}k \cdot p(n)$ across all k proof registers. Why does entanglement across proofs not help the prover in the NO case?)

3. **Strong error reduction for QMA.** All references below are to the Lecture 5 course notes.

   (a) Prove Equations (8)-(11).

   (b) What is $\left\| S_0 Q^\dagger E_1 Q|\phi\rangle \right\|_2$?

   (c) Prove that after we measure the right hand side of Equation (6) with $\{S_0, S_1\}$, we obtain S_1 with probability p and S_0 with probability $1-p$. Similarly, measuring the right hand side of Equation (7) with S_0, S_1 yields S_0 with probability p and S_1 with probability $1-p$.

(d) Conclude from the last exercise that after the first iteration of the while loop, $y_1 = y_2$ with probability p. Accordingly, $y_1 \neq y_2$ with probability $1 - p$.