Quantum Proofs, Semester A 2024

Homework # 4 **due: 5pm, February 15th, 2024**

Ground rules:

Homework is due through Moodle. If you are having issues with this, email the instructor (thomas.vidick@weizmann.ac.il) or drop your work in my mailbox at the top of the central stairs in Ziskind. Solutions can be latexed or handwritten. In the latter case, please make sure that your handwriting is legible. Special care should be taken in writing up a precise solution. If I am not able to follow the logic in your argument, if there is a small gap or an uncovered case, you will lose points.

You are encouraged to collaborate with your classmates on homework problems, but each person must write up the final solutions individually. You should note on your homework specifically which problems were a collaborative effort and with whom. You may not search online for solutions, but if you do use research papers or other sources in your solutions, you must cite them.

Late homework will not be accepted or graded.

Any changes since the first posting will be marked in blue.

Problem:

1. **Another complete problem for QSZK.**

   Recall the (α, β) close quantum states (CQS) problem: the input is a pair of quantum circuits Q_0, Q_1 each taking no input and outputting quantum states of the same number of qubits ρ_0, ρ_1 respectively. The instance is a yes-instance if $\|\rho_0 - \rho_1\|_{tr} \leq \alpha$, and it is a no-instance if $\|\rho_0 - \rho_1\|_{tr} \geq \beta$. As seen in class this problem is QSZK-complete for any $2^{-p} < \alpha \leq \beta^2 - 1/q \leq 1 - 2^{-p}$, where p, q are any (positive) polynomials.

   Define a new problem (α, β) product state as follows. The input is a single quantum circuit Q, together with two integers (m_A, m_B) such that Q has zero input qubits and $m = m_A + m_B$ output qubits. The circuit Q prepares a state ρ, and we let ρ_A be the reduced density of ρ on the first m_A qubits and ρ_B its reduced density on the last m_B qubits. Then the instance is a:

   - yes-instance if ρ is α-close to a product state, namely there exists σ_A and σ_B on m_A and m_B qubits respectively such that $\|\rho - \sigma_A \otimes \sigma_B\|_{tr} \leq \alpha$.
   - no-instance if ρ is β-far from every product state, namely for every σ_A and σ_B on m_A and m_B qubits respectively it holds that $\|\rho - \sigma_A \otimes \sigma_B\|_{tr} \geq \beta$.

(a) Suppose that $\|\rho - \sigma_A \otimes \sigma_B\|_{tr} \leq \alpha$ for some σ_A, σ_B. Show that $\|\rho - \rho_A \otimes \rho_B\|_{tr} \leq 3\alpha$, where ρ_A and ρ_B are the reduced densities of ρ.

(b) Show a reduction from (α, β)-product state to $(3\alpha, \beta)$-QCS.

We now make our way towards a reduction in the other direction.

(c) Given two states ρ_0 and ρ_1 on the same number of qubits, determine the projective measurement $\{\Pi_0, \Pi_1 = \mathbb{I} - \Pi_0\}$ that maximizes $\frac{1}{2}\mathrm{Tr}(\Pi_0\rho_0) + \frac{1}{2}\mathrm{Tr}(\Pi_1\rho_1)$. What is the maximum value that this expression can attain (over all projective $\{\Pi_0, \Pi_1\}$, ρ_0 and ρ_1 being fixed)? *[Hint: Yes, this appeared in a previous homework!]*

Let

$$\omega = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_1 \ .$$

Our goal in the next questions is to find a lower bound on the trace distance of this state from any product state. For this, we will use that the trace distance is non-increasing under CPTP maps (quantum channels). In particular, it suffices to prove a lower bound on the distance between any two states obtained by performing the same quantum transformation on ω and on an arbitrary product state, respectively. Let $\Phi = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$.

(d) Suppose that we measure the first (single-qubit) register of ω in the computational basis, yielding a bit b_0, and then measure the second register using $\{\Pi_0, \Pi_1\}$, yielding a bit b_1. Let σ be the mixed state that represents the two-bit outcome of this procedure, i.e. $\sigma = \sum_{b_0, b_1 \in \{0,1\}} \mathbf{Pr}(b_0, b_1)|b_0, b_1\rangle\langle b_0, b_1|$. Determine $\|\sigma - \Phi\|_1$. *[Hint: you should be able to compute each probability $\mathbf{Pr}(b_0, b_1)$ explicitly.]*

(e) Suppose that the same procedure is applied to a product state, yielding a (diagonal) density σ' on two qubits. Show that $\|\sigma' - \Phi\|_{tr} \geq \frac{1}{4}$.

(f) Conclude a lower bound, depending on $\|\rho_0 - \rho_1\|_{tr}$, on the trace distance between ω and any product state.

(g) Use the previous questions to devise a reduction from (α, β)-QCS to (α', β')-product state, for some α', β' that you will evaluate (as a function of α, β).

We remark that, interestingly, if in the definition of the (α, β)-product state problem all states (the input state ρ, and the product states considered in the definition of yes- and no-instances) are assumed to be pure, then the resulting problem is BQP-complete (as long as α, β are constants that are sufficiently far apart from each other). It is an (optional!) exercise to demonstrate this.