Quantum Proofs, Semester A 2024

Homework # 3 Solutions **February 5th, 2024**

Please read the document and check your understanding of the answer. If you feel that your solution was correct, but I mistakenly did not award you all points, please talk to me. If my sketch is not detailed enough and you would like to see a full solution, please ask me as well.

Problems:

1. **Practice with semidefinite programs**

   Recall that a semidefinite program is said in *primal normal form* if it is written as

$$\begin{aligned} \sup \quad & B \bullet X \\ s.t. \quad & A_i \bullet X = a_i \,, \quad \forall\, i = 1, \ldots, m \\ & X \geq 0 \,, \end{aligned}$$

   where we used the shorthand notation $X \bullet Y = \mathrm{Tr}(X^\dagger Y)$, $B, A_1, \ldots, A_m$ are complex Hermitian matrices of the same size as X, and $a_1, \ldots, a_m$ real numbers.

   (a) Suppose given a complex Hermitian matrix $A \in \mathbb{C}^{d\times d}$. Write a semidefinite program, in primal normal form, whose optimum is the largest eigenvalue of A.

$$\begin{aligned} \sup \quad & A \bullet X \\ s.t. \quad & \mathrm{Tr}(X) = 1 \\ & X \geq 0 \,. \end{aligned}$$

   (b) Can you do the same with $\|A\|_1$, the sum of the singular values of A?

   The simplest way to write this is using two inequalities on X:

$$\begin{aligned} \sup \quad & A \bullet X \\ s.t. \quad & X \geq -\mathbb{I} \\ & X \leq \mathbb{I} \,. \end{aligned}$$

   The fact that the constraints do not have a single positive semidefinite constraint confused some of you. Here, there are various ways to get around this. One possibility is to rewrite the program in a new variable

$$Z = \begin{pmatrix} \mathbb{I} - X & 0 \\ 0 & X + \mathbb{I} \end{pmatrix} \qquad (1)$$

   as follows

$$
\begin{aligned}
\sup \quad & \frac{1}{2}\begin{pmatrix} A & 0 \\ 0 & -A \end{pmatrix} \bullet Z \\
s.t. \quad & F_{i,j} \bullet Z = f_{i,j}\ , \quad \forall\, i,j = 1,\ldots,d \\
& Z \geq 0\ ,
\end{aligned}
$$

where the constraint matrices $F_{i,j}$ are designed to force the form (1). In fact, because the objective only looks at the diagonal blocks we only need to care about them. So, let $F_{i,j} = \begin{pmatrix} E_{ij} & 0 \\ 0 & E_{ij} \end{pmatrix}$, where E_{ij} is all 0's except for a single 1 in position (i,j), and $f_{i,j} = 2\delta_{ij}$ with δ_{ij} the Kronecker symbol.

(c) Deduce a semidefinite program whose optimum is the trace distance $\|\sigma_0 - \sigma_1\|_{tr} = \frac{1}{2}\|\sigma_0 - \sigma_1\|_1$ between two density matrices σ_0 and σ_1 (given explicitly, as matrices).

We apply the previous question to $A = \sigma_0 - \sigma_1$.

(d) Suppose given an ensemble $\{(p_i, \rho_i) : i \in \mathcal{I}\}$, where: $\mathcal{I}$ is a finite index set; for each i, $p_i \in [0,1]$ such that $\sum_{i\in\mathcal{I}} p_i = 1$; and for each i, ρ_i is a density matrix on n qubits, specified explicitly (in matrix form, as for the previous question). Write the maximum success probability of the adversary in the following game, played against a trusted challenger, as the optimum of a semidefinite program:

i. The challenger selects $i \in \mathcal{I}$ according to the distribution (p_i). They prepare the quantum state ρ_i and send it to the adversary.

ii. The adversary performs a measurement and returns to the challenger an index $i' \in \mathcal{I}$.

iii. The challenger declares that the adversary has won if and only if $i' = i$.

$$
\begin{aligned}
\sup \quad & \sum_i p_i\, P_i \bullet \rho_i \\
s.t. \quad & \sum_i P_i = \mathbb{I} \\
& P_i \geq 0\ , \quad \forall i\ .
\end{aligned}
$$

Note that the constraint $\sum_i P_i = \mathbb{I}$ is in fact $\sum_i E_{jk} \bullet P_i = \delta_{jk}$ for all $j,k \in \{1,\ldots,d\}$, which is a collection of linear constraints. Here again, the program can be written in standard form by introducing a new variable X which has $(P_1,\ldots,P_{|\mathcal{I}|}, \mathbb{I} - \sum_i P_i)$ in its diagonal blocks.

2. The diamond norm and error amplification

In this problem, T denotes a "super-operator," which in general is any linear map $T : L(\mathcal{N}) \to L(\mathcal{M})$. Here, $\mathcal{N}$ and $\mathcal{M}$ are (finite-dimensional) Hilbert spaces and $L(\mathcal{N})$

and $L(\mathcal{M})$ are the space of linear operators on $\mathcal{N}$ and $\mathcal{M}$ respectively. Said in other words, $\mathcal{N} = \mathbb{C}^{d_\mathcal{N}}$ for some integer $d_\mathcal{N}$ and $L(\mathcal{N}) = \mathbb{C}^{d_\mathcal{N} \times d_\mathcal{N}}$, the space of $d_\mathcal{N} \times d_\mathcal{N}$ matrices. So, T is a linear map that sends $d_\mathcal{N} \times d_\mathcal{N}$ matrices to $d_\mathcal{M} \times d_\mathcal{M}$ matrices. (If T is additionally completely positive and trace preserving, then it is a channel; but for the time being we allow general linear T.)

A natural norm on the space of such linear maps T is the operator norm induced by the 1 norm, i.e.

$$|||T|||_1 := \sup_{X \neq 0} \frac{\|T(X)\|_1}{\|X\|_1} . \tag{2}$$

Here, $\|X\|_1 = \mathrm{Tr}\sqrt{XX^\dagger}$ is the 1 norm of the matrix X, which is the sum of the singular values. The norm $|||\cdot|||_1$ has the following inconvenient:

(a) Let $T : L(\mathbb{C}^2) \to L(\mathbb{C}^2)$ be defined by $T : |i\rangle\langle j| \mapsto |j\rangle\langle i|$ for all $i, j \in \{0, 1\}$, and extended by linearity to all 2×2 matrices. (So, T is the transpose map!) Show that $|||T|||_1 \leq 1$, but $|||T \otimes \mathbb{I}_2|||_1 \geq 2$, where $\mathbb{I}_2$ is the identity map on 2×2 matrices.

This question was generally solved correctly. For the example, a possible choice was to apply T to an EPR pair.

You may notice that while the projection on an EPR pair has a single eigenvalue 1, its partial transpose has a negative eigenvalue. If a bipartite density matrix is such that, by transposing one of the two systems, one obtains a matrix that is no longer positive, the corresponding state must be entangled. There are some states that are entangled and yet have positive partial transpose, so this is not a perfect test for entanglement (indeed, checking if a density matrix corresponds to a separable state is an NP-hard problem, even allowing for approximations).

The previous question shows that $|||\cdot|||_1$, when used on super-operators, does not "stabilize". This property is not welcome when discussing quantum channels, as we would not want that the "norm" of a channel tensored with the identity is bigger than the norm of the channel itself. So instead, we define

$$|||T|||_\diamond := \sup_{d \geq 1} \left|\left|\left| T \otimes \mathbb{I}_{L(\mathbb{C}^d)} \right|\right|\right|_1 ,$$

where $|||\cdot|||_1$ is as defined in (2), and $\mathbb{I}_{L(\mathbb{C}^d)}$ denotes the identity super-operator from $L(\mathbb{C}^d)$ to itself.

(b) Show that for any superoperators R, S it holds that $|||RS|||_\diamond \leq |||R|||_\diamond |||S|||_\diamond$. (You may use that the same inequality holds for the norm $\|\cdot\|_1$, without reproving this fact.)

This question was solved correctly by everyone.

In the remainder of this problem we use the norm $|||\cdot|||_\diamond$ to characterize the maximum acceptance probability of a $\mathsf{QIP}(3)$ verifier, and give an alternate proof of error amplification.

In the following fix a $\mathsf{QIP}(3)$ verifier $V = (V_1, V_2)$ in purified form. Here, V_1 is a unitary that acts on the message $\mathcal{Y}$ received from the prover, and the verifier's private space $\mathcal{Z}$. It produces a message sent back to the prover, which for convenience we assume lies on the same space $\mathcal{Y}$, and a residual memory state. So, V_1 is a unitary on $\mathcal{Z} \otimes \mathcal{Y}$. Similarly, V_2 is the unitary on $\mathcal{Z} \otimes \mathcal{Y}$ applied by the verifier upon receipt of the prover's second message. After V_2 has been applied, the verifier measures using a measurement (Π_{acc}, Π_{rej}) that we assume acts on the entire space $\mathcal{Z} \otimes \mathcal{Y}$. Finally, let Π_{init} denote the projection on the space where all verifier's qubits (the register $\mathcal{Z}$) are initialized to 0.

Let $W_1 = V_1 \Pi_{init}$ and $W_2 = V_2^\dagger \Pi_{acc}$. Let $T : L(\mathcal{Z} \otimes \mathcal{Y}) \to L(\mathcal{Y})$ be the superoperator defined as $T(X) = \mathrm{Tr}_{\mathcal{Z}}(W_1 X W_2^\dagger)$.

(c) Show that $\omega(V) = \max\{|\langle|\phi|W_2^\dagger U W_1 |\psi\rangle|^2\}$, where the maximum is taken over all states $|\psi\rangle, |\phi\rangle \in \mathcal{Z} \otimes \mathcal{Y} \otimes \mathcal{W}$ and unitaries U on $\mathcal{Y} \otimes \mathcal{W}$, with $\mathcal{W}$ the prover's private space.

This question was also generally solved correctly.

(d) For a fixed space $\mathcal{H}$, show that the maximum of $\|T \otimes \mathbb{I}_{L(\mathcal{H})}(Y)\|_1$ over all Y such that $\|Y\|_1 = 1$ is attained at a Y of the form $Y = |\psi\rangle\langle\phi|$, for normalized vectors $|\psi\rangle, |\phi\rangle$.

Here the main observation is that any Y such that $\|Y\|_1 = 1$ has a decomposition $Y = \sum_i p_i Y_i$ where (p_i) is a probability distribution and Y_i has rank one for each i, i.e. $Y_i = |\psi_i\rangle\langle\phi_i|$. (This is by the SVD.) Moreover, $\|T \otimes \mathbb{I}_{L(\mathcal{H})}(Y)\|_1$ is a convex function of Y — this is by linearity of T and convexity of $\|\cdot\|_1$. Therefore,

$$\begin{aligned}\|T \otimes \mathbb{I}_{L(\mathcal{H})}(Y)\|_1 &\le \sum_i p_i \|T \otimes \mathbb{I}_{L(\mathcal{H})}(Y_i)\|_1 \\ &\le \max_i \|T \otimes \mathbb{I}_{L(\mathcal{H})}(Y_i)\|_1 \, .\end{aligned}$$

(e) Deduce from the previous questions that $\omega(V) = |||T|||_\diamond^2$.

For any fixed $\mathcal{H}$, by the previous question

$$\begin{aligned}\sup_Y \|T \otimes \mathbb{I}_{L(\mathcal{H})}(Y)\|_1 &= \sup_{|\psi\rangle,|\phi\rangle} \|T \otimes \mathbb{I}_{L(\mathcal{H})}(|\psi\rangle\langle\phi|)\|_1 \\ &= \sup_{|\psi\rangle,|\phi\rangle,U} \left|\mathrm{Tr}\big(U \cdot T \otimes \mathbb{I}_{L(\mathcal{H})}(|\psi\rangle\langle\phi|)\big)\right| \\ &= \sup_{|\psi\rangle,|\phi\rangle,U} \left|\mathrm{Tr}\big((\mathbb{I}_{\mathcal{Z}} \otimes U) \cdot W_1 |\psi\rangle\langle\phi| W_2^\dagger\big)\right| \\ &= \sup_{|\psi\rangle,|\phi\rangle,U} |\langle\phi|W_2^\dagger U W_1|\psi\rangle| \, ,\end{aligned}$$

which solves the question. Here the main step is the second equality, which uses $\|X\|_1 = \sup_U |\mathrm{Tr}(UX)|$, where the supremum is taken over all unitaries. The third line uses the definition of T and the last line cyclicity of the trace.

(f) Suppose that V' is another verifier, not necessarily identical to V. Let $V \otimes V'$ denote the verifier that runs V and V' in parallel and accepts if and only if both accept. Use the previous questions to show that $\omega(V \otimes V') \leq \omega(V)\omega(V')$.

This was solved correctly.

3. **Competing-prover games**

This problem didn't create particular difficulties. (If anyone is interested in more background, the problem is adapted from the paper "Quantum Interactive Proofs with Competing Provers" by Gutoski and Watrous.)