Assignment: Quantum strategies

Due at 23:59 on Friday, May 25, 2012.

There are 30 marks available in this assignment. The assignment will be graded out of 20.

1. **Co-strategies are adjoint channels.** *[5 marks.]* Let $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ be any super-operator. By analogy with matrices, the *adoint* of Φ is the unique super-operator $\Phi^* : \mathrm{L}(\mathcal{Y}) \to \mathrm{L}(\mathcal{X})$ satisfying $\langle \Phi(X), Y \rangle = \langle X, \Phi^*(Y) \rangle$ for all $X \in \mathrm{L}(\mathcal{X})$ and $Y \in \mathrm{L}(\mathcal{Y})$.

   It is easy to see that if $\Phi : X \mapsto \sum_i A_i X A_i^*$ then $\Phi^* : Y \mapsto \sum_i A_i^* Y A_i$ and you may use this fact without proof in your answer.

   Prove that if Φ is completely positive then $J(\Phi^*) = W J(\Phi)^{\mathsf{T}} W^*$ where

   $$W : \mathcal{Y} \otimes \mathcal{X} \to \mathcal{X} \otimes \mathcal{Y} : |j\rangle|i\rangle \mapsto |i\rangle|j\rangle$$

   is the unitary swap operator.

   Remark. Let $J(\Xi)$ be an $(r+1)$-round strategy for input spaces $\mathbb{C}, \mathcal{Y}_1, \ldots, \mathcal{Y}_r$ and output spaces $\mathcal{X}_1, \ldots, \mathcal{X}_r, \mathbb{C}$ where the channel $\Xi : \mathrm{L}(\mathcal{Y}_{1\ldots r}) \to \mathrm{L}(\mathcal{X}_{1\ldots r})$ is of the form described in lecture.

   In lecture we defined an r-round co-strategy for input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_r$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$ by $W J(\Xi)^{\mathsf{T}} W^*$, which you now know is equal to $J(\Xi^*)$. In other words, the Choi-Jamiołkowski representation of a co-strategy is simply the Choi matrix of the *adjoint* Ξ^* of the super-operator Ξ described in lecture.

2. **Characterization of measuring strategies.** *[5 marks.]* Prove that if $\{Q_a\} \subset \mathrm{Pos}(\mathcal{Y}_{1\ldots r} \otimes \mathcal{X}_{1\ldots r})$ is a finite set for which $\sum_a Q_a$ is an r-round non-measuring strategy for input spaces $\mathcal{X}_1, \ldots, \mathcal{X}_r$ and output spaces $\mathcal{Y}_1, \ldots, \mathcal{Y}_r$ then $\{Q_a\}$ is an r-round measuring strategy for the same input and output spaces.

3. **Lower-bound for quantum coin-flipping.** *[5 marks.]* Consider a scenario in which Alice and Bob wish to flip a fair coin but do not trust each other. A *quantum coin-flipping protocol with cheating probability* p is a specification of an r-round measuring strategy $\{A_0, A_1\}$ for Alice and an r-round measuring co-strategy $\{B_0, B_1\}$ for Bob with the following properties:

   Honest parties flip fair coins.
   $\langle A_0, B_0 \rangle = \langle A_1, B_1 \rangle = \frac{1}{2}$.

   Cheaters can't cheat too much.
   For any outcome $i \in \{0, 1\}$ we have the following:
   For every r-round measuring co-strategy $\{B_0', B_1'\}$ for Bob it holds that $\langle A_i, B_i' \rangle \leq p$.
   For every r-round measuring strategy $\{A_0', A_1'\}$ for Alice it holds that $\langle A_i', B_i \rangle \leq p$.

   By definition, every protocol must have $p \geq 1/2$. Use the formula for maximum output probabilities to prove that every quantum coin-flipping protocol has cheating probability $p \geq 1/\sqrt{2} \approx 0.707$.

   Hint. Fix $i \in \{0, 1\}$ and let p be the maximum probability that a cheating Bob can force honest-Alice to output i. By the formula for maximum output probabilities we know there exists a strategy Q for Alice with $A_i \preceq pQ$. What happens if a cheating Alice uses strategy Q against honest-Bob?

4. **Channel-channels are two-round strategies.** We all know that channels map quantum states to quantum states and that a super-operator Φ is a channel if and only if Φ is completely positive and trace-preserving. But what kind of mappings map quantum *channels* to quantum *channels*?

   Let $\mathrm{T}(\mathcal{H}_{\mathrm{in}}, \mathcal{H}_{\mathrm{out}})$ denote the space of super-operators of the form $\Phi : \mathrm{L}(\mathcal{H}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{H}_{\mathrm{out}})$. A mapping

$$\mathcal{C} : \mathrm{T}(\mathcal{H}_{\mathrm{in}}, \mathcal{H}_{\mathrm{out}}) \to \mathrm{T}(\mathcal{K}_{\mathrm{in}}, \mathcal{K}_{\mathrm{out}}) \tag{1}$$

   is called *completely completely positive* if for every choice of spaces $\mathcal{X}_{\mathrm{in}}, \mathcal{X}_{\mathrm{out}}$ and every choice of completely positive super-operators $\Psi : \mathrm{L}(\mathcal{H}_{\mathrm{in}} \otimes \mathcal{X}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{H}_{\mathrm{out}} \otimes \mathcal{X}_{\mathrm{out}})$ it holds that the super-operator

$$\left(\mathcal{C} \otimes \mathbb{1}_{\mathrm{T}(\mathcal{X}_{\mathrm{in}}, \mathcal{X}_{\mathrm{out}})}\right)(\Psi) : \mathrm{L}(\mathcal{K}_{\mathrm{in}} \otimes \mathcal{X}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{K}_{\mathrm{out}} \otimes \mathcal{X}_{\mathrm{out}}) \tag{2}$$

   is also completely positive. (Here $\mathbb{1}_{\mathrm{T}(\mathcal{X}_{\mathrm{in}}, \mathcal{X}_{\mathrm{out}})}$ denotes the identity mapping on $\mathrm{T}(\mathcal{X}_{\mathrm{in}}, \mathcal{X}_{\mathrm{out}})$, as you might expect.)

   We say that $\mathcal{C}$ is *trace-preserving-preserving* if for every choice of trace-preserving super-operators $\Phi : \mathrm{L}(\mathcal{H}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{H}_{\mathrm{out}})$ it holds that $\mathcal{C}(\Phi)$ is also trace-preserving. We say that $\mathcal{C}$ is a *channel-channel* if it is both completely completely positive and trace-preserving-preserving.

   For any mapping $\mathcal{C}$ of the form (1) let us define a super-operator $K_{\mathcal{C}}$ so that

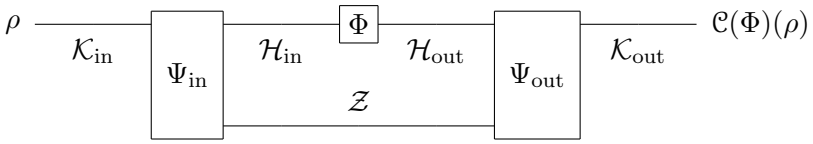
$$K_{\mathcal{C}} : \mathrm{L}(\mathcal{H}_{\mathrm{out}} \otimes \mathcal{H}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{K}_{\mathrm{out}} \otimes \mathcal{K}_{\mathrm{in}}) : J(\Phi) \mapsto J(\mathcal{C}(\Phi)) \tag{3}$$

   (a) **(Challenge problem.)** *[5 marks.]* Prove that if $\mathcal{C}$ is a channel-channel then $J(K_{\mathcal{C}})$ is a two-round strategy for input spaces $\mathcal{K}_{\mathrm{in}}, \mathcal{H}_{\mathrm{out}}$ and output spaces $\mathcal{H}_{\mathrm{in}}, \mathcal{K}_{\mathrm{out}}$.

   (b) *[5 marks.]* Use the link product to prove that every channel-channel $\mathcal{C}$ admits a physical implementation whereby there exists a memory space $\mathcal{Z}$ and channels

$$\Psi_{\mathrm{in}} : \mathrm{L}(\mathcal{K}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{H}_{\mathrm{in}} \otimes \mathcal{Z})$$
$$\Psi_{\mathrm{out}} : \mathrm{L}(\mathcal{H}_{\mathrm{out}} \otimes \mathcal{Z}) \to \mathrm{L}(\mathcal{K}_{\mathrm{out}})$$

   such that for every channel $\Phi : \mathrm{L}(\mathcal{H}_{\mathrm{in}}) \to \mathrm{L}(\mathcal{H}_{\mathrm{out}})$ and every input state $\rho \in \mathrm{Dens}(\mathcal{K}_{\mathrm{in}})$ it holds that the output state $\mathcal{C}(\Phi)(\rho) \in \mathrm{Dens}(\mathcal{K}_{\mathrm{out}})$ is given by the following circuit.



(4)

   (c) *[5 marks.]* Prove the converse of question 4a: if $S \in \mathrm{L}(\mathcal{K}_{\mathrm{out}} \otimes \mathcal{K}_{\mathrm{in}} \otimes \mathcal{H}_{\mathrm{out}} \otimes \mathcal{H}_{\mathrm{in}})$ is a two-round strategy for input spaces $\mathcal{K}_{\mathrm{in}}, \mathcal{H}_{\mathrm{out}}$ and output spaces $\mathcal{H}_{\mathrm{in}}, \mathcal{K}_{\mathrm{out}}$ then $S = J(K_{\mathcal{C}})$ for some channel-channel $\mathcal{C}$.