Quantum Nonlocality Pt. 2: No-Signaling and Local Hidden Variables

May 1, 2018
Non-Signaling Boxes

The primary lesson from last lecture is that a pair of input/output boxes can be used for communication if and only if they violate the non-signaling condition.

Non-Signaling Condition

Two boxes with inputs belonging to set $\mathcal{X} = \{1, \cdots , |\mathcal{X}|\}$, outputs belong to set $\mathcal{B} = \{, 1, \cdots , |\mathcal{B}|\}$ and transition probabilities $\{p(b|x)\}_{b \in \mathcal{B}, x \in \mathcal{X}}$ are called non-signaling if

$$p(b|x) = p(b|x') \quad \forall b \in \mathcal{B}, \quad \forall x, x' \in \mathcal{X}.$$

In this lecture we will return to the quantum setting and see if quantum entanglement can be used faster-than-light communication.
Suppose Alice and Bob share some bipartite state $\rho^{AB}$.

They have read a popular science magazine claiming that quantum entanglement allows for “spooky action at a distance.”

They get excited and think this means their entanglement can be used for instantaneous communication.

Alice: *I will perform one of two quantum operations on my system. This will cause an instantaneous change on your system so that by measuring your system you will be able to determine which action I performed.*

*Then if I want to send message 0, I will perform operation $\{A_0^{(0)}, A_1^{(0)}\}$ and if I want to send message 1, I will perform action $\{A_0^{(1)}, A_1^{(1)}\}$.***
Bob: Great idea! But what measurement should I use to recover your message? Let me choose between two of them - \( \{ B_0^{(0)}, B_1^{(0)} \} \) or \( \{ B_0^{(1)}, B_1^{(1)} \} \) - and see which one works better.

The measurements \( \{ B_0^{(0)}, B_1^{(0)} \} \) and \( \{ B_0^{(1)}, B_1^{(1)} \} \) are two decoding operations for Alice’s message. He measures his system and claims that Alice sent value \( x \) if he obtains measurement outcome \( x \).

Alice and Bob’s strategy can be described within the “black box” framework. These boxes are more sophisticated since they have pairs of inputs and pairs of inputs.
Quantum Boxes

The transition probabilities are given by

\[ p(a, b|x, y) = \text{tr} [(A^{(x)}_a \otimes B^{(y)}_b) \rho^{AB} (A^{(x)}_a \otimes B^{(y)}_b)^\dagger] \quad a, b, x, y \in \{0, 1\}. \]

Do these boxes allow for communication?

There are two possibilities now: communication from Alice to Bob or communication from Bob to Alice.

For Alice to Bob, we look at Bob’s output distribution \( p(b|x, y) \). For each of his inputs \( y \), this generates an input/output box \( p_y(b|x) := p(b|x, y) \) where

\[ p(b|x, y) = \sum_a p(a, b|x, y). \]
Quantum Boxes

No signaling from Alice to Bob means that $p_y(b|x) = p_y(b|x')$; in other words

$$\sum_a p(a, b|x, y) = \sum_a p(a, b|x, y') \quad b, x, y, y'.$$

No signaling from Bob to Alice means that

$$\sum_b p(a, b|x, y) = \sum_b p(a, b|x', y) \quad a, y, x, x'.$$

Do quantum boxes satisfy the non-signaling conditions with transition probabilities given by

$$p(a, b|x, y) = \text{tr}[(A_a^{(x)} \otimes B_b^{(y)}) \rho^{AB} (A_a^{(x)} \otimes B_b^{(y)})^\dagger]$$?
Quantum Boxes

Check: \[ \sum_{a} p(a, b|x, y) = \sum_{a} tr[(A_{a}^{(x)} \otimes B_{b}^{(y)}) \rho^{AB} (A_{a}^{(x)} \otimes B_{b}^{(y)})^\dagger] \]
\[ = \sum_{a} tr[(A_{a}^{(x)})^\dagger A_{a}^{(x)} \otimes (B_{b}^{(y)})^\dagger B_{b}^{(y)} \rho^{AB}] \]
\[ = tr[\mathbb{I} \otimes (B_{b}^{(y)})^\dagger B_{b}^{(y)} \rho^{AB}] = tr[(B_{b}^{(y)})^\dagger B_{b}^{(y)} \rho^{B}]. \]

This is just the probability that Bob obtains outcome b when he performs measurement \{ B_{b}^{(y)} \} on his reduced state \rho^{B}.

It is independent of both Alice’s input and output \Rightarrow p(b|x, y) = p(b|x', y)

It satisfies the non-signaling conditions. Quantum entanglement does not allow instantaneous communication!
Quantum Boxes

The transition probabilities \( \{p(a, b|x, y)\}_{a,b,x,y} \) generated by quantum boxes (i.e. generated by measuring an entangled quantum state) do not allow for communication between two spatial positions \( X_1 \) and \( X_2 \) in a time interval faster than \( c\Delta X \) (i.e. Special Relativity is not violated).

Does this mean that spatially separated classical systems can also generate these transition probabilities \( \{p(a, b|x, y)\} \)?

To properly answer this question, let us develop a general framework of input/output boxes that will allow us to distinguish between classical and quantum boxes.
The Theory of Correlated Boxes

Definition

Let $\mathcal{A}, \mathcal{B}, \mathcal{X},$ and $\mathcal{Y}$ be arbitrary finite sets of integers. A set of correlations is a collection of non-negative numbers

$$\{p(a, b|x, y)\}_{a \in \mathcal{A}, b \in \mathcal{B}, x \in \mathcal{X}, y \in \mathcal{Y}}$$

such that $\sum_{a \in \mathcal{A}, b \in \mathcal{B}} p(a, b|x, y) = 1$ for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$.

The correlations are called **non-signaling** (NS) if

$$\sum_a p(a, b|x, y) = \sum_a p(a, b|x, y')$$
$$\sum_b p(a, b|x, y) = \sum_b p(a, b|x', y)$$

for all $b, x, y, y'$ and $a, y, x, x'$. 
The Theory of Correlated Boxes

The correlations are called **quantum correlations** (QC) if there exists a bipartite quantum state $\rho^{AB}$ as well as quantum operations $\{A^a\}_{a \in A}$ and $\{B^b\}_{b \in B}$ for all $(x, y) \in X \times Y$ such that

$$p(a, b|x, y) = tr[(A^{(x)}_a \otimes B^{(y)}_b)\rho^{AB}(A^{(x)}_a \otimes B^{(y)}_b)\dagger].$$

What are the type of correlations that can be generated by classical boxes? Classical systems are assumed to satisfy a property known as “locality”. The following meaning of locality will suffice for our purposes.

Two boxes are said to function **locally** if their correlations take the form $p(a, b|x, y) = p(a|x)p(b|y)$. In other words, for every input and output of one box, the input/output statistics of the other box are not changed (i.e. $p(a, b|x, y) = p(a, b'|x, y')$ and $p(a, b|x, y) = p(a', b|x', y)$; compare with NS boxes).
The Theory of Correlated Boxes

However, classical physics clearly does not require that every pair of boxes behave locally. Classical physics allows for interaction between systems, and this interaction establishes correlation.

Consider a drawer of full of socks and each sock has two properties: (i) Color ∈ \{Black, White\} and (ii) Fabric ∈ \{Cotton, Nylon\}. For simplicity also assume that each sock either belongs to a right or left foot.

Each pair in the drawer consists of a right and left sock, but the color and fabric properties are not matched! Each pair is described by a list

\[ \lambda_{C_LF_LC_RF_R} = (\text{Color } C_L, \text{Fabric } F_L, \text{Color } C_R, \text{Fabric } F_R), \]

where \( C_L/F_L \) is the color/fabric of the left sock and \( C_R/F_R \) is the color/fabric of the right sock.
The Theory of Correlated Boxes

Suppose that the pairs of socks are distributed in the drawer according to probabilities $p(\lambda_{C_L F_L C_R F_R})$ with $C_{L/R} \in \{B, W\}$ and $F_{L/R} \in \{C, N\}$.

I reach into the drawer and randomly select a pair. I then put the left sock in a black box and give that to Alice, and I put the right sock in a black box and give that to Bob.

Each boxes are designed so that it reveals only the Color or the Fabric of the sock it holds, but Alice and Bob can choose which property is revealed.

Let $x \in \{C, F\}$ be the property that Alice chooses to learn, and $y \in \{C, F\}$ the property that Bob chooses to learn.
The Theory of Correlated Boxes

Their boxes are described by the correlations $p(x_L, y_L|x, y)$.

The outputs $(x_L, y_L)$ will depend not only on the choices $(x, y)$ but also which socks were drawn from the drawer.

To compute $p(x_L, y_L|x, y)$ we need to sum over all the socks in the drawer:

$$p(x_L, y_L|x, y) = \sum_{C_LF_LC_RF_R} p(x_L, y_L, \lambda C_LF_LC_RF_R|x, y)$$

$$= \sum_{C_LF_LC_RF_R} p(x_L, y_L|x, y, \lambda C_LF_LC_RF_R) p(\lambda C_LF_LC_RF_R).$$
The Theory of Correlated Boxes

We obviously have that

$$p(x_L, y_L|x, y, \lambda_{C_L F_L C_R F_R}) = p(x_L|x, \lambda_{C_L F_L C_R F_R})p(y_L|y, \lambda_{C_L F_L C_R F_R})$$

since $\lambda_{C_L F_L C_R F_R}$ specifies the value of $x_L$ and $y_L$ for every choice of $x$ and $y$.

Thus, Alice and Bob’s function locally given the value of $\lambda_{C_L F_L C_R F_R}$.

Their correlations have the form

$$p(x_L, y_L|x, y) = \sum_{C_L F_L C_R F_R} p(x_L|x, \lambda_{C_L F_L C_R F_R})p(y_L|y, \lambda_{C_L F_L C_R F_R})p(\lambda_{C_L F_L C_R F_R}).$$
The Theory of Correlated Boxes

Alice and Bob’s boxes are not local since they do not have the form
\[ p(x_L, y_L | x, y) = p(x_L | x)p(y_L | y). \]

However their boxes are local given the value of some hidden variable \( \lambda_{CLFLCRFR} \).

The boxes became dependent on the hidden variable \( \lambda_{CLFLCRFR} \) by some interaction in the past. Specifically, this interaction was when I distributed the pair of socks to each box.

The boxes came together at sometime in the past when I distributed the socks. This made them correlated for all future times, regardless of how far apart they were separated.
Local Hidden Variables

In general, a set of correlations \( \{ p(a, b|x, y) \} \) are called **local hidden variable** (LHV) correlations if they can be written as

\[
p(a, b|x, y) = \sum_{\lambda} p(\lambda) p_A(a|x, \lambda) p_B(b|y, \lambda) \quad \forall a, b, x, y
\]

for some variable \( \lambda \) with distribution \( p(\lambda) \). Here \( p_A(a|x, \lambda) p_B(b|y, \lambda) \) is a product of local probability distributions.

What is the relationship between the various correlations \( LHV, QC, \) and \( NS \)?

We have already shown that \( QC \subset NS \). To conclude today’s lecture, we will make two simple observations: (i) \( LHV \subset CQ \) and (ii) The quantum correlations generated by every separable state belong to \( LHV \).