Quantum Nonlocality Pt. 1: No-Signaling

PHYS 500 - Southern Illinois University

April 26, 2018

Quantum Entanglement and Instantaneous Communication

A common misconception is that quantum entanglement allows for instantaneous communication.

Quantum Entanglement and Instantaneous Communication

A common misconception is that quantum entanglement allows for instantaneous communication.

The goal of this lecture is to make precise what it means for one system to communicate with another and show that entangled systems do not allow for such communication.

Quantum Entanglement and Instantaneous Communication

A common misconception is that quantum entanglement allows for instantaneous communication.

The goal of this lecture is to make precise what it means for one system to communicate with another and show that entangled systems do not allow for such communication.

While quantum entanglement does not allow for instantaneous communication, it does allow for two systems to be correlated in ways that cannot be simulated using classical systems.

These quantum correlations are known as *nonlocality*, and the meaning of quantum nonlocality will be explored in the next few lectures.

The Meaning of Communication

Let us formalize the meaning of a communication system.

The Meaning of Communication

Let us formalize the meaning of a communication system.

Consider a scenario where Alice and Bob each possess a black box, the contents of which are unknown to both of them. However, Alice's box is able to receive an input number $x \in \{0, 1\}$ while Bob's box emits an output number $b \in \{0, 1\}$ whenever he presses a button on the top of the box.

The Meaning of Communication

Let us formalize the meaning of a communication system.

Consider a scenario where Alice and Bob each possess a black box, the contents of which are unknown to both of them. However, Alice's box is able to receive an input number $x \in \{0, 1\}$ while Bob's box emits an output number $b \in \{0, 1\}$ whenever he presses a button on the top of the box.

Intuitively, we would say these boxes allow for communication if Alice can choose a value $x \in \{0, 1\}$ and use the boxes to send this choice x to Bob.

The Meaning of Communication

Let us formalize the meaning of a communication system.

Consider a scenario where Alice and Bob each possess a black box, the contents of which are unknown to both of them. However, Alice's box is able to receive an input number $x \in \{0, 1\}$ while Bob's box emits an output number $b \in \{0, 1\}$ whenever he presses a button on the top of the box.

Intuitively, we would say these boxes allow for communication if Alice can choose a value $x \in \{0, 1\}$ and use the boxes to send this choice x to Bob.

If the boxes are ideal communication devices, then for each input $x \in \{0, 1\}$, Bob receives the exact same output x the next time he presses the button on his box.

The Meaning of Communication

However, Alice and Bob quickly observe that their boxes are non-ideal. Rather than perfect transmission, their boxes are seen to follow a set of **transition probabilities** $\{p(b|x)\}_{b,x\in\{0,1\}}$. That is, whenever Alice inputs value x into her box, Bob receives output b with probability $p(b|x)$.

The Meaning of Communication

However, Alice and Bob quickly observe that their boxes are non-ideal. Rather than perfect transmission, their boxes are seen to follow a set of **transition probabilities** $\{p(b|x)\}_{b,x\in\{0,1\}}$. That is, whenever Alice inputs value x into her box, Bob receives output b with probability $p(b|x)$.

Can these non-ideal boxes still be used for communication?

The Meaning of Communication

However, Alice and Bob quickly observe that their boxes are non-ideal. Rather than perfect transmission, their boxes are seen to follow a set of **transition probabilities** $\{p(b|x)\}_{b,x\in\{0,1\}}$. That is, whenever Alice inputs value x into her box, Bob receives output b with probability $p(b|x)$.

Can these non-ideal boxes still be used for communication?

Alice and Bob can use their boxes multiple times and Alice can encode a single choice $x \in \{0, 1\}$ across multiple inputs.

The Meaning of Communication

However, Alice and Bob quickly observe that their boxes are non-ideal. Rather than perfect transmission, their boxes are seen to follow a set of **transition probabilities** $\{p(b|x)\}_{b,x\in\{0,1\}}$. That is, whenever Alice inputs value x into her box, Bob receives output b with probability $p(b|x)$.

Can these non-ideal boxes still be used for communication?

Alice and Bob can use their boxes multiple times and Alice can encode a single choice $x \in \{0,1\}$ across multiple inputs.

For n uses of the box, Alice uses an encoding function f_{enc} and Bob uses a decoding function g_{dec};

$$f_{enc} : \{0,1\} \to \{0,1\}^{\times n}, \qquad g_{enc} : \{0,1\}^{\times n} \to \{0,1\}.$$

The Meaning of Communication

For each use of the boxes, the transition probabilities $\{p(b|x)\}_{b,x\in\{0,1\}}$ are the same and independent of previous uses. Therefore for any input sequence $x^n = (x_1, x_2, \cdots, x_n) \in \{0,1\}^{\times n}$, the probability of getting a particular output sequence $b^n = (b_1, b_2, \cdots, b_n) \in \{0,1\}^{\times n}$ is given by

$$p(b^n|x^n) = \prod_{i=1}^{n} p(b_i|x_i).$$

The Meaning of Communication

For each use of the boxes, the transition probabilities $\{p(b|x)\}_{b,x\in\{0,1\}}$ are the same and independent of previous uses. Therefore for any input sequence $x^n = (x_1, x_2, \cdots, x_n) \in \{0,1\}^{\times n}$, the probability of getting a particular output sequence $b^n = (b_1, b_2, \cdots, b_n) \in \{0,1\}^{\times n}$ is given by

$$p(b^n|x^n) = \prod_{i=1}^{n} p(b_i|x_i).$$

Definition

Two boxes with transition probabilities $\{p(b|x)\}_{b,x\in\{0,1\}}$ **allow for communication** if for every $\epsilon > 0$ and n sufficiently large there exists encoding and decoding functions f_{enc} and g_{dec} such that

$$p(g_{dec}^{-1}(0)|f_{dec}(0)) > 1-\epsilon, \qquad p(g_{dec}^{-1}(1)|f_{dec}(1)) > 1-\epsilon.$$

The Meaning of Communication

In other words, two boxes allow for communication if Alice can always send a message $x \in \{0, 1\}$ with arbitrarily small transmission error by using the boxes a large number of times.

The Meaning of Communication

In other words, two boxes allow for communication if Alice can always send a message $x \in \{0, 1\}$ with arbitrarily small transmission error by using the boxes a large number of times.

The following theorem allows us to characterize precisely which boxes allow for communication.

The Meaning of Communication

In other words, two boxes allow for communication if Alice can always send a message $x \in \{0, 1\}$ with arbitrarily small transmission error by using the boxes a large number of times.

The following theorem allows us to characterize precisely which boxes allow for communication.

Theorem

Two boxes with transition probabilities $\{p(b|x)\}_{b,x\in\{0,1\}}$ allow for communication if and only if

$$p(0|0) \neq p(0|1).$$

(Note that since $p(0|0) + p(1|0) = 1$ and $p(0|1) + p(1|1) = 1$, this condition is equivalent to $p(1|0) \neq p(1|1)$.)

The Meaning of Communication

The theorem of this proof (which we do not give here) follows from a fundamental result in information theory known as the "noisy channel coding theorem."

The Meaning of Communication

The theorem of this proof (which we do not give here) follows from a fundamental result in information theory known as the "noisy channel coding theorem."

Definition

In a general setting with a larger set of inputs $\mathcal{X} = \{0, 1, \cdots, |\mathcal{X}|\}$ and larger set of outputs $\mathcal{B} = \{0, 1, \cdots, |\mathcal{B}|\}$, two boxes with transition probabilities $\{p(b|x)\}_{b\in\mathcal{B}, x\in\mathcal{X}}$ are called **non-signaling** if

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

The Meaning of Communication

The theorem of this proof (which we do not give here) follows from a fundamental result in information theory known as the "noisy channel coding theorem."

Definition

In a general setting with a larger set of inputs $\mathcal{X} = \{0, 1, \cdots, |\mathcal{X}|\}$ and larger set of outputs $\mathcal{B} = \{0, 1, \cdots, |\mathcal{B}|\}$, two boxes with transition probabilities $\{p(b|x)\}_{b\in\mathcal{B}, x\in\mathcal{X}}$ are called **non-signaling** if

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

Two boxes do not allow for communication if and only if they are non-signaling.