Lecture 16 Quantum nonlocality

Xiao Yuan

December 7, 2021

In this lecture, we introduce Bell inequalities, the concept of quantum nonlocality, and its applications.

1 Framework of nonlocal games

We focus on the nonlocal game scenario, where two distantly separated parties, Alice and Bob, are asked to play a game. In particular, as shown in Fig. 1, they receive random inputs x and y from a referee with probability $q(x, y)$, and give outputs a and b, respectively. Consider a payoff function $\beta(a, b, x, y)$ and denote the strategy of Alice and Bob by $p(a, b|x, y)$, the average payoff is

$$I = \sum_{a,b,x,y} \beta(a, b, x, y)p(a, b|x, y)q(x, y). \tag{1}$$

For simplicity, we consider binary inputs and outputs and assume that the inputs are generated uniformly random with $q(x, y) = 1/4$. Then we have

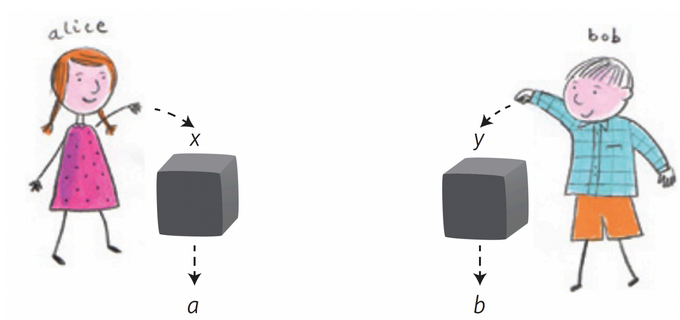

Figure 1: Bell Nonlocality. Figure from Nature Physics volume 10, pages 264270 (2014).

We will show that the average payoff obtained from any classical strategy is upper bounded, and such a bound is called a Bell inequality, i.e.,

$$I = \frac{1}{4} \sum_{a,b,x,y} \beta(a, b, x, y)p(a, b|x, y) \leq u_{\mathrm{C}} \tag{2}$$

Yet, this upper bound could be violated when we use quantum strategies. Therefore, the violation of Bell's inequality indicated the existence of quantumness. We discuss that this feature could be exploited to design device independent or self-testing quantum information protocols.

2 Classical, quantum, no-signalling correlations

2.1 Classical

We first consider what is a classical strategy. In the Bell nonlocality scenario, we assume that Alice and Bob cannot communicate once they have started the game. In this case, Alice and Bob have to use independent strategies $p(a|x)$ and $p(b|y)$, respectively, which defines the joint strategy $p(a|x)p(b|y)$. Yet, since Alice and Bob can communicate before the game, their strategies can indeed depend on some predetermined rules, say λ. Therefore, any classical strategy could be described by

$$p_{\mathrm{C}}(a,b|x,y) = \sum_{\lambda} q(\lambda) p_A(a|x,\lambda) p_B(b|y,\lambda) \tag{3}$$

We note that this also includes the cases where the strategy could also vary with different rounds of the game. The theory described by $p_{\mathrm{C}}(a,b|x,y)$ is also called a local hidden variable model (LHVM), since the correlation[1] is actually generated by the local hidden variable λ.

Can we generate any correlation using a classical LHVM? The answer is no and a simple counter example is as follows,

$$p_{\mathrm{SWAP}}(a,b|x,y) = \begin{cases} 1 & a = y \\ 1 & b = x \end{cases} \tag{4}$$

which effectively output the swapped inputs of Alice and Bob. Such a probability distribution is equivalent to the swap gate. Obviously it cannot be realized by LHVM since it is equivalent to sending Alice and Bob's inputs to the other party and LHVM is forbid to communicate.

2.2 NS

Can we formalize the requirement of no-communication or no-signaling (NS)? We first define the partial probability

$$p(a|x,y) = \sum_b p(a,b|x,y), \quad p(b|x,y) = \sum_a p(a,b|x,y). \tag{5}$$

Since the output a (b) is determined by Alice (Bob) while the input y (x) is sent to Bob, a no-signaling strategy thus requires

$$p_{\mathrm{NS}}(a|x,y) = p(a|x,y'), \quad p_{\mathrm{NS}}(b|x,y) = p(b|x',y), \tag{6}$$

and such a condition is also called the no-signaling condition. It is easy to verify that LHVM satisfy NS.

Can LHVM generate any NS correlation? Interestingly, the answer is still no and an explicit counter example is the PR-box, defined as

$$p_{\mathrm{PR}}(a,b|x,y) = \begin{cases} 1/2 & a \oplus b = xy \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

At this point, it is not obvious why LHVM cannot generate the PR-box. But we will see this soon using the CHSH inequality.

2.3 Quantum

Another important family of strategy is using quantum mechanics. Specifically, Alice and Bob can share some entangled state ρ_{AB} and measure the state with POVM $\{M^A_{a|x} \geq 0\}$ and $\{M^B_{b|y} \geq 0\}$ satisfying $\sum_a M^A_{a|x} = \mathbb{I}_A$ for all x and $\sum_b M^B_{b|y} = \mathbb{I}_B$ for all y. The correlation generated in this way is

$$p_{\mathrm{Q}}(a,b|x,y) = \mathrm{Tr}[\rho_{AB}(M^A_{a|x} \otimes M^B_{b|y})] \tag{8}$$

Again, can you generate any quantum correlation using LHVM? The answer is still no and we will prove it using the tool of Bell inequalities. In particular, we will introduce a Bell inequality such that the payoff I_{C} using LHVM is upper bounded by 2, yet the maximal payoff I_{Q} and I_{NS} using quantum and NS strategies reach $2\sqrt{2}$ and 4. The relationship between NS, quantum correlation, and classical LHVMs can be summarized as in Fig. 2.

[1] For two random variables X and Y, we say they are correlated simply mean $p(X,Y) \neq p(X)p(Y)$.

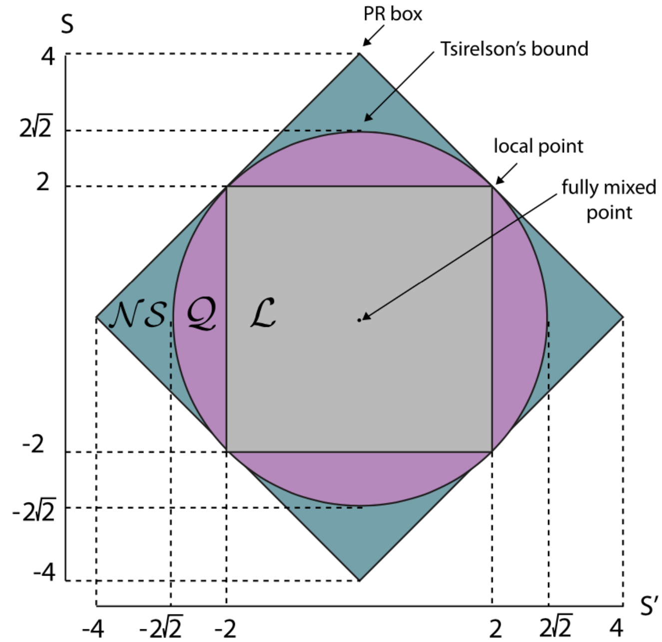

Figure 2: No-signalling, quantum, and classical correlations. Here the value is related to the CHSH inequality by $I' = 8I - 4$. Figure from Rev. Mod. Phys. 86, 419 (2014).

3 CHSH inequality

3.1 Definition

The CHSH inequality is different from the original inequality proposed by Bell, but it is much easier to understand and is more widely studied now. The payoff function of the CHSH inequality is defined by

$$\beta(a, b|x, y) = \begin{cases} 1 & a \oplus b = xy \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

The payoff table with nonzero payoff β is given in Table 1.

Table 1: Payoff table for the CHSH inequality.

x	y	a	b	β
0	0	0	0	1
0	0	1	1	1
0	1	0	0	1
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	1	1
1	1	1	0	1

3.2 NS

First we can prove that the average payoff I is upper bounded by 1. That is

$$
\begin{aligned}
I &= \frac{1}{4}\sum_{a,b,x,y}\beta(a,b,x,y)p(a,b|x,y), \\
&= \frac{1}{4}\sum_{a\oplus b=xy}p(a,b|x,y), \\
&\leq \frac{1}{4}\sum_{xy}1, \\
&= 1.
\end{aligned}
\tag{10}
$$

Here we have used the normalization condition $\sum_{ab}p(a,b|x,y)=1$. It is not hard to see that the PR-box achieves this upper bound.

3.3 LHVMs

Next, we prove that the average payoff I_{C} using LHVMs is upper bounded by 3/4. First, we have

$$
\begin{aligned}
I_{\mathrm{C}} &= \frac{1}{4}\sum_{a\oplus b=xy}p_{\mathrm{C}}(a,b|x,y), \\
&= \frac{1}{4}\sum_{a\oplus b=xy}\sum_{\lambda}q(\lambda)p_A(a|x,\lambda)p_B(b|y,\lambda), \\
&\leq \frac{1}{4}\max_{p_A(a|x,\lambda),p_B(b|y,\lambda)}\sum_{a\oplus b=xy}p_A(a|x,\lambda)p_B(b|y,\lambda),
\end{aligned}
\tag{11}
$$

so that we can focus on $\sum_{a\oplus b=xy}p_A(a|x,\lambda)p_B(b|y,\lambda)$. Denote $p_A(a|x,\lambda)$ and $p_B(b|y,\lambda)$ by $p_x^A(a)$ and $p_y^B(b)$, respectively, we have

$$
\begin{aligned}
\sum_{a\oplus b=xy}p_A(a|x,\lambda)p_B(b|y,\lambda) &= p_0^A(0)p_0^B(0)+(1-p_0^A(0))(1-p_0^B(0))+p_0^A(0)p_1^B(0)+(1-p_0^A(0))(1-p_1^B(0)), \\
&+p_1^A(0)p_0^B(0)+(1-p_1^A(0))(1-p_0^B(0))+p_1^A(0)(1-p_1^B(0))+(1-p_1^A(0))p_1^B(0), \\
&= \frac{1}{2}\left[2p_0^A(0)-1\right]\left[2p_0^B(0)-1\right]+\frac{1}{2}\left[2p_0^A(0)-1\right]\left[2p_1^B(0)-1\right] \\
&+\frac{1}{2}\left[2p_1^A(0)-1\right]\left[2p_0^B(0)-1\right]-\frac{1}{2}\left[2p_0^A(0)-1\right]\left[2p_1^B(0)-1\right]+2.
\end{aligned}
\tag{12}
$$

Here we have used $p_0^A(0)p_0^B(0)+(1-p_0^A(0))(1-p_0^B(0))=\frac{1}{2}\left[2p_0^A(0)-1\right]\left[2p_0^B(0)-1\right]+\frac{1}{2}$. Denote $O_i^A=2p_i^A(0)-1$ and $O_i^B=2p_i^B(0)-1$, which satisfy $|O_i^A|,|O_i^B|\in[-1,1]$, we have[2]

$$
\begin{aligned}
\sum_{a\oplus b=xy}p_A(a|x,\lambda)p_B(b|y,\lambda) &= \frac{1}{2}[O_0^AO_0^B+O_0^AO_1^B+O_1^AO_0^B-O_1^AO_1^B]+2, \\
&\leq \frac{1}{2}\left[|O_0^A||O_0^B+O_1^B|+|O_1^A||O_0^B-O_1^B|\right]+2, \\
&\leq 3.
\end{aligned}
\tag{13}
$$

Putting everything back to Eq. (11), we thus have

$$
I_{\mathrm{C}}\leq 3/4. \tag{14}
$$

This inequality is usually called the Bell (here CHSH) inequality.

[2] Here the last line could be proved as follow. Let $x=O_0^B+O_1^B$ and $y=O_0^B-O_1^B$, we have $|x+y|\leq 2$ and $|x-y|\leq 2$. Then we can prove it by linear programming.

3.4 Quantum

We can then give an explicit quantum strategy that can beat the LHVM bound. Define a projective measurement as $\{\Pi_0(\theta), \Pi_1(\theta)\}$ with $\Pi_0(\theta) = |\psi_0(\theta)\rangle \langle\psi_0(\theta)|$ and $\Pi_1(\theta) = |\psi_1(\theta)\rangle \langle\psi_1(\theta)|$, and

$$\begin{aligned} |\psi_0(\theta)\rangle &= \cos\theta \,|0\rangle + \sin\theta \,|1\rangle \,, \\ |\psi_1(\theta)\rangle &= -\sin\theta \,|0\rangle + \cos\theta \,|1\rangle \,. \end{aligned} \tag{15}$$

The state Alice and Bob share is the Bell state $|\Phi^+\rangle_{AB} = (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$ and the measurement basis is chosen as

$$M^A_{i|0} = \Pi_i(0), \quad M^A_{i|1} = \Pi_i(\pi/2), \quad M^B_{i|0} = \Pi_i(\pi/8), \quad M^B_{i|1} = \Pi_i(-\pi/8), \tag{16}$$

We can then calculate the average payoff using this strategy as $I = \cos(\pi/8)^2 \approx 0.85 \geq I_{\mathrm{C}}$, which show the violation of the Bell inequality using LHVMs.

Finally, we can show that the above strategy is optimal. Similar to the proof of LHVMs, we first define O^A_i and O^B_i as follows

$$O^A_i = M^A_{0|i} - M^A_{1|i}, \quad O^B_i = M^B_{0|i} - M^B_{1|i}. \tag{17}$$

Then we can show that

$$\begin{aligned} I_{\mathrm{Q}} &= \frac{1}{4} \sum_{a\oplus b = xy} \mathrm{Tr}[\rho_{AB}(M^A_{a|x} \otimes M^B_{b|y})], \\ &= \frac{1}{8}\mathrm{Tr}\left[\rho_{AB}\left(O^A_0 \otimes O^B_0 + O^A_0 \otimes O^B_1 + O^A_1 \otimes O^B_0 - O^A_1 \otimes O^B_1\right)\right] + \frac{1}{2}. \end{aligned} \tag{18}$$

Without loss of generality, we can consider a pure state $\rho_{AB} = |\psi\rangle \langle\psi|_{AB}$ and we show

$$\begin{aligned} \langle\psi|_{AB}\, O^A_0 \otimes O^B_0 + &O^A_0 \otimes O^B_1 + O^A_1 \otimes O^B_0 - O^A_1 \otimes O^B_1 \,|\psi\rangle_{AB} \\ &= \|\left(O^A_0 \otimes O^B_0 + O^A_0 \otimes O^B_1 + O^A_1 \otimes O^B_0 - O^A_1 \otimes O^B_1\right)|\psi\rangle_{AB}\,\|, \\ &\leq \|\left(O^A_0 \otimes O^B_0 + O^A_0 \otimes O^B_1\right)|\psi\rangle_{AB}\,\| + \|\left(O^A_1 \otimes O^B_0 - O^A_1 \otimes O^B_1\right)|\psi\rangle_{AB}\,\|, \\ &\leq \|\left(O^B_0 + O^B_1\right)|\psi\rangle_{AB}\,\| + \|\left(O^B_0 - O^B_1\right)|\psi\rangle_{AB}\,\|. \end{aligned} \tag{19}$$

Denote $|\psi_i\rangle = O^B_i\,|\psi\rangle_{AB}$, we have

$$\begin{aligned} \|\left(O^B_0 + O^B_1\right)|\psi\rangle_{AB}\,\| + \|\left(O^B_0 - O^B_1\right)|\psi\rangle_{AB}\,\| &= \|\,|\psi_0\rangle + |\psi_1\rangle\,\| + \|\,|\psi_0\rangle - |\psi_1\rangle\,\|, \\ &= \sqrt{2 + 2\Re\langle\psi_0|\psi_1\rangle} + \sqrt{2 - 2\Re\langle\psi_0|\psi_1\rangle}, \\ &\leq 2\sqrt{2}. \end{aligned} \tag{20}$$

Finally, we have

$$I_{\mathrm{Q}} \leq \frac{2+\sqrt{2}}{4}. \tag{21}$$

4 Applications

The Bell inequality has wide applications for designing self-testing or device independent quantum information protocols. Recall that a violation of the Bell inequality implies the existence of quantum entanglement. Therefore, the measurement outcomes must have genuine/unpredictable randomness. Such a feature could thus be used to generate randomness. Since the randomness is guaranteed by the violation of the Bell inequality without assuming the realization, it is thus robust to device implementation errors, and hence called device independent. Bell inequality can also be used for quantum key distribution, blind quantum computing, etc. One can read Rev. Mod. Phys. 86, 419 (2014) for more detailed discussions.