Operational characterization of quantum nonlocality

Ryuhei Mori

Tokyo Institute of Technology
JST PRESTO

6 Mar. 2019
Motivation

• Quantum physics has a beautiful mathematical representation.

• But, we do not have any “explanation” for the quantum physics.

• We need to find postulates of quantum physics.

Postulate: Similar to axiom in math. But, it must be testable by experiments, e.g.,

• Information cannot be transmitted faster than light.
• A communication complexity is not always equal to 1.
Quantum physics

• There is no concept of “quantum probability”.

• A probability is always expressed by a tuple of non-negative values with sum 1.

• There are concepts of “state” and “measurement”.
  • State: Environment.
  • Measurement: Operation to a state for getting an outcome.
  • Probability of an output $a \in A$ when a measurement $x \in \mathcal{X}$ is chosen is $P(a \mid x)$. 

CHSH game [Bell 1964 12736]
[Clauser, Horne, Shimony, Holt 1969 6564]

Alice and Bob win iff $a \oplus b = x \land y$. 
CHSH winning probability

- The maximum CHSH winning probability in classical physics is $3/4 = 0.75$.

$$b_1 \neq a_1$$

$$\parallel \quad \parallel$$

$$a_0 = b_0$$

- The maximum CHSH winning probability in quantum physics is $(2 + \sqrt{2})/4 \approx 0.854$ [Tsirelson 1980 1380].
Locality (Hidden variable model)

Joint preparation and independent measurements.

Probability distribution $P(a, b \mid x, y)$ is said to be \textbf{local} if

$$P(a, b \mid x, y) = \sum_{\lambda} P(\lambda)P(a \mid x, \lambda)P(b \mid y, \lambda).$$

Equivalently, there exists a joint distribution $P(a_0, a_1, b_0, b_1)$.

Quantum physics allow \textbf{nonlocal} behaviors.

[Einstein, Podolsky, Rosen 1935, \textbf{17516}]
Two-party statistics

$P(a, b \mid x, y), \quad \forall a, b \in \{0, 1\}, x, y \in \{0, 1\}$
No-signaling condition

The marginal distribution of $a$ ($b$) cannot depend on $y$ ($x$), respectively.

$$\sum_{b \in \{0,1\}} P(a, b \mid x, 0) = \sum_{b \in \{0,1\}} P(a, b \mid x, 1), \quad \forall a, x \in \{0,1\}$$

$$\sum_{a \in \{0,1\}} P(a, b \mid 0, y) = \sum_{a \in \{0,1\}} P(a, b \mid 1, y), \quad \forall b, y \in \{0,1\}.$$
The 8-dimensional linear space and no-signaling polytope

\[ \sum_{a \in \{0,1\}, \ b \in \{0,1\}} P(a, b \mid x, y) = 1, \quad x \in \{0,1\}, \ y \in \{0,1\}. \]

\[ \sum_{b \in \{0,1\}} P(0, b \mid 0, 0) = \sum_{b \in \{0,1\}} P(0, b \mid 0, 1) \]
\[ \sum_{b \in \{0,1\}} P(0, b \mid 1, 0) = \sum_{b \in \{0,1\}} P(0, b \mid 1, 1) \]
\[ \sum_{a \in \{0,1\}} P(a, 0 \mid 0, 0) = \sum_{a \in \{0,1\}} P(a, 0 \mid 1, 0) \]
\[ \sum_{a \in \{0,1\}} P(a, 0 \mid 0, 1) = \sum_{a \in \{0,1\}} P(a, 0 \mid 1, 1). \]

16 − 8 = 8-dimensional linear space.
No-signaling polytope
Local polytope

Deterministic choice

\[ a = A(x), \quad b = B(y). \]

Local polytope

\[
\text{conv} \left( \left\{ P(a, b \mid x, y) = \delta_{(a, b), (A(x), B(y))} \right\}_{a, b, x, y} \mid A, B \in \{0, 1\}^{0, 1} \right). 
\]
No-signaling polytope and local polytope
CHSH inequality: Facets of the local polytope

\[
\sum_{a \oplus b = x \wedge y} P(a, b \mid x, y) \leq 3,
\sum_{a \oplus b \neq x \wedge y} P(a, b \mid x, y) \leq 3
\]

\[
\sum_{a \oplus b = \overline{x} \wedge y} P(a, b \mid x, y) \leq 3,
\sum_{a \oplus b \neq \overline{x} \wedge y} P(a, b \mid x, y) \leq 3
\]

\[
\sum_{a \oplus b = x \wedge \overline{y}} P(a, b \mid x, y) \leq 3,
\sum_{a \oplus b \neq x \wedge \overline{y}} P(a, b \mid x, y) \leq 3
\]

CHSH inequality [Clauser, Horne, Shimony, Holt 1969 6564].
CHSH inequality is the only non-trivial facets [Froissard 1981 111], [Fine 1982 991].
No-signaling condition admits CHSH probability 1

\[ P(0, 0 \mid 0, 0) = P(1, 1 \mid 0, 0) = 1/2 \]
\[ P(0, 0 \mid 0, 1) = P(1, 1 \mid 0, 1) = 1/2 \]
\[ P(0, 0 \mid 1, 0) = P(1, 1 \mid 1, 0) = 1/2 \]
\[ P(0, 1 \mid 1, 1) = P(1, 0 \mid 1, 1) = 1/2 \]

[Popescu and Rohrlich 1994 1122]
No-signaling polytope, local polytope and quantum correlation

- CHSH probability = 1
- CHSH probability ≈ 0.854
- CHSH probability = 0.75

Question:

Why does quantum physics prohibits CHSH probability greater than \((2 + \sqrt{2})/4 \approx 0.854\) ?
• $p_{\text{CHSH}} = 1 \implies$ Communication complexity (CC) of arbitrary function is 1 bit.

• $p_{\text{CHSH}} > (3 + \sqrt{6})/6 \approx 0.908 \implies$ CC of arbitrary function is 1 bit.
  [Brassard, Buhrman, Linden, Méthot, Tapp, Unger 2006 291]

• $p_{\text{CHSH}} > (2 + \sqrt{2})/4 \approx 0.854 \implies$ Information causality is violated.
  [Pawłowski, Paterek, Kaszlikowski, Scarani, Winter, Zukowki 2009 462]

• Brassard et al.’s result cannot be improved by generalizations of their techniques [Mori 2016].
Abstract device with two input ports and two output ports.

Nonlocal box

\[ P(a, b \mid x, y) = \begin{cases} \frac{p_{\text{CHSH}}}{2}, & \text{if } a \oplus b = x \land y \\ \frac{1-p_{\text{CHSH}}}{2}, & \text{if } a \oplus b \neq x \land y. \end{cases} \]

This does not lose generality since

\[ x \land y = (x \oplus r_1) \land (y \oplus r_2) \oplus x \land r_2 \oplus r_1 \land y \oplus r_1 \land r_2 \]

\[ = a \oplus b \oplus e \oplus x \land r_2 \oplus r_1 \land y \oplus r_1 \land r_2 \]

\[ = (a \oplus x \land r_2 \oplus r_1 \land r_2) \oplus (b \oplus r_1 \land y) \oplus e \]
Alice and Bob win iff $a \oplus b = f(x, y)$.
PR box gives a winning probability 1


If the CHSH probability is 1, a winning probability of any XOR game is 1!

Any boolean function can be represented by a $\mathbb{F}_2$-polynomial.

$$f(x, y) = \bigoplus_i A_i(x) \land B_i(y).$$

Recall Alice and Bob have nonlocal boxes with

$$\Pr(a \oplus b = x \land y) = 1$$

for any $(x, y) \in \{0, 1\}^2$,

$$\bigoplus_i A_i(x) \land B_i(y) = \bigoplus_i (a_i \oplus b_i)$$

$$= \left( \bigoplus_i a_i \right) \oplus \left( \bigoplus_i b_i \right).$$
Bias

For a probability $p \in [1/2, 1]$, $\beta := 2p - 1 \in [0, 1]$ is called a bias. In other word,

$$p = \frac{1 + \beta}{2}.$$

Let $\beta$ be a bias of the CHSH probability $p_{\text{CHSH}}$.

- $p_{\text{CHSH}} = 3/4 \iff \beta = 1/2$.
- $p_{\text{CHSH}} = (2 + \sqrt{2})/4 \iff \beta = 1/\sqrt{2}$.
- $p_{\text{CHSH}} = 1 \iff \beta = 1$.

- If $X$ is $\pm 1$ random variable, the bias (for a prob. of 1) is $\mathbb{E}[X] = \frac{1+\beta}{2} - \frac{1-\beta}{2} = \beta$.
- If $X$ and $Y$ are independent 0-1 random variables with bias (for a prob. of 0) $\beta_X$ and $\beta_Y$, respectively, the bias of $X \oplus Y$ is $\beta_X \beta_Y$. 
Constant winning probability

[Brassard, Buhrman, Linden, Méthot, Tapp, Unger 2006]

\( \rho_{\text{CHSH}} > \frac{3+\sqrt{6}}{6} \approx 0.908 \iff \beta > \sqrt{\frac{2}{3}} \)

\( \implies \) A winning probability of any XOR game is constant (\( > \frac{1}{2} \)).

By using shared random bits \( r \in \{0, 1\}^n \) and Bob’s private random bit \( r' \in \{0, 1\} \),

\[
a = f(x, r) \\
b = \begin{cases} 
0, & \text{if } y = r \\
r', & \text{otherwise.}
\end{cases}
\]

\( a \oplus b = f(x, y) \) with probability

\[
\frac{1}{2^n} + \left( 1 - \frac{1}{2^n} \right) \frac{1}{2} = \frac{1 + 2^{-n}}{2}.
\]
Bias amplification by Maj₃

\[ \text{Maj}_3(z_1, z_2, z_3) = \frac{1}{2} \left( z_1 + z_2 + z_3 - z_1 z_2 z_3 \right) \]

\[ \mathbb{E}[\text{Maj}_3(z_1, z_2, z_3)] = \frac{3}{2} \epsilon - \frac{1}{2} \epsilon^3 \]
Bias amplification by noisy Maj$_3$

[von Neumann 1956 2708]

\[ \text{Maj}_3(z_1, z_2, z_3) = \frac{1}{2} (z_1 + z_2 + z_3 - z_1 z_2 z_3) \]

\[ \mathbb{E} [y \text{Maj}_3(z_1, z_2, z_3)] = \rho \left( \frac{3}{2} \epsilon - \frac{1}{2} \epsilon^3 \right) \]

\[ \rho > \frac{2}{3} \]
Probability of succeeding of computation of Maj_3

\[ \text{Maj}_3(z_1, z_2, z_3) = z_1z_2 \oplus z_2z_3 \oplus z_3z_1 \]

\[ \text{Maj}_3(a_1 \oplus b_1, a_2 \oplus b_2, a_3 \oplus b_3) \]
\[ = (a_1 \oplus b_1)(a_2 \oplus b_2) \oplus (a_2 \oplus b_2)(a_3 \oplus b_3) \oplus (a_3 \oplus b_3)(a_1 \oplus b_1) \]
\[ = (a_1 \oplus a_2)(b_2 \oplus b_3) \oplus (a_2 \oplus a_3)(b_1 \oplus b_2) \]
\[ \quad \oplus a_1a_2 \oplus a_2a_3 \oplus a_3a_1 \]
\[ \quad \oplus b_1b_2 \oplus b_2b_3 \oplus b_3b_1 \]
\[ = (\alpha_0 \oplus \beta_0 \oplus e_0) \oplus (\alpha_1 \oplus \beta_1 \oplus e_1) \]
\[ \quad \oplus a_1a_2 \oplus a_2a_3 \oplus a_3a_1 \]
\[ \quad \oplus b_1b_2 \oplus b_2b_3 \oplus b_3b_1 \]
\[ = (\alpha_0 \oplus \alpha_1 \oplus a_1a_2 \oplus a_2a_3 \oplus a_3a_1) \oplus (\beta_0 \oplus \beta_1 \oplus b_1b_2 \oplus b_2b_3 \oplus b_3b_1) \oplus e_0 \oplus e_1. \]

\[ \beta^2 > \frac{2}{3} \iff \beta > \sqrt{\frac{2}{3}} \iff p > \frac{1 + \sqrt{\frac{2}{3}}}{2} = \frac{3 + \sqrt{6}}{6} \approx 0.908. \]
Generalization of Brassard et al’s protocol

• Why $\text{Maj}_3$ ?

• Replace $\text{Maj}_3$ with arbitrary boolean function.

• Two important parameters:
  • 2: Number of nonlocal boxes for the computation.
  • $2/3$: Threshold for the bias amplification.

• We showed that the $\text{Maj}_3$ is the unique optimal function in a simple generalization [Mori, Phys. Rev. A 94, 052130, 2016].
Information causality:

If Alice communicates $m$ bits to Bob, the total information obtainable by Bob cannot be greater than $m$.

Alice has $2^n$ bits. Bob wants to know one of Alice’s $2^n$ bits. Alice doesn’t know which bit Bob wants to know.

IC says that Alice has to send $2^n$ bits.

Above the quantum limit $0.854$, Alice only has to send $1.99^n$ bits.
Address function

\[ \text{Addr}_n(x_0, \ldots, x_{2^n-1}, y_1, \ldots, y_n) := x_y \]

where \( y := \sum_{i=1}^{n} y_i 2^{i-1} \).

**Theorem** ([Pawłowski, Paterek, Kaszlikowski, Scarani, Winter, Zukowski 2009 462])

There is an adaptive protocol of the XOR game for the address function with bias \( \beta^n \).

**Proof**

Induction.

For \( n = 1 \), from

\[ \text{Addr}_1(x_0, x_1, y_1) = x_0 \oplus y_1(x_0 \oplus x_1) \]

there is a non-adaptive protocol with bias \( \beta \).
Address function

Proof (Cont’d).

\[ \text{Addr}_n(x_0, \ldots, x_{2^n-1}, y_1, \ldots, y_n) = \text{Addr}_1(z_0, z_1, y_n) \]

where

\[ z_0 := \text{Addr}_{n-1}(x_0, \ldots, x_{2^{n-1}-1}, y_1, \ldots, y_{n-1}) \]
\[ z_1 := \text{Addr}_{n-1}(x_{2^{n-1}}, \ldots, x_{2^n-1}, y_1, \ldots, y_{n-1}) \].

\[ \text{Addr}_1(z_0, z_1, y_n) = \text{Addr}_1(a_0 \oplus b_0 \oplus e_0, a_1 \oplus b_1 \oplus e_1, y_n) \]
\[ = \text{Addr}_1(a_0, a_1, y_n) \oplus b_{y_n} \oplus e_{y_n} \]
\[ = a' \oplus b' \oplus e' \oplus b_{y_n} \oplus e_{y_n} \]
\[ = a' \oplus (b' \oplus b_{y_n}) \oplus (e' \oplus e_{y_n}) \].

This protocol has bias \( \beta^n \). \qed
Repetition

The 1 bit communication has error probability $\epsilon := \frac{1 - \beta^n}{2}$.
The $m$ bits communication has error probability $\leq \left(2\sqrt{\epsilon(1 - \epsilon)}\right)^m$.

From
\[
\left(2\sqrt{\epsilon(1 - \epsilon)}\right)^m = (1 - \beta^{2n})^{m/2}
\]
error probability goes to zero if
\[
m \gg \beta^{-2n}.
\]

If $\beta > 1/\sqrt{2}$, then $\beta^{-2} < 2$.

If CHSH probability is greater than the quantum limit, 

1.99$^n$ bits communication allows Bob to select arbitrary one bit from Alice’s 2$^n$ bits.
Macroscopic locality

Nature should not exhibit nonlocal behaviour in macroscopic setting.

\[ a = 0 \quad \rightarrow \quad b = 0 \]
\[ \begin{array}{c}
\text{1 photon pair} \\
\end{array} \]
\[ a = 1 \quad \rightarrow \quad b = 1 \]

Microscopic experiment of nonlocality.

\[ a = 0 \quad \rightarrow \quad b = 0 \]
\[ \begin{array}{c}
\text{N photon pairs} \\
\end{array} \]
\[ a = 1 \quad \rightarrow \quad b = 1 \]

Macroscopic experiment of nonlocality (with precision \( O(\sqrt{N}) \)).

[Navascués, Wunderlich, 2009, 219]
Central limit theorem

For fixed $x$ and $y$,
\[
\{ (N(a; x) - \mathbb{E}[N(a; x)])/\sqrt{N}, (N(b; y) - \mathbb{E}[N(b; y)])/\sqrt{N} \}_{a,b}
\]
weakly converges to the normal distribution. Assume
\[
\mathbb{E}[a_x] = 0, \quad \mathbb{E}[b_y] = 0, \quad \mathbb{E}[a_x b_y] = (-1)^{x \wedge y} \beta.
\]

Then, the nonlocal box is macroscopically local if and only if
\[
\exists \lambda \in [-1, +1] \text{ such that }
\]
\[
\Gamma(\lambda) := \begin{bmatrix}
1 & \lambda & \beta & \beta \\
\lambda & 1 & \beta & -\beta \\
\beta & \beta & 1 & \lambda \\
\beta & -\beta & \lambda & 1
\end{bmatrix} \succeq 0
\]

This condition shows $\beta \leq \frac{1}{\sqrt{2}}$. 

Toward characterizing the quantum correlation

**Theorem ([Navascués and Wunderlich 2009, 219])**
Quantum physics satisfies the macroscopic locality.

**Theorem ([Navascués and Wunderlich 2009, 219])**
There exists a macroscopically local distribution with biased marginals attaining the Tsirelson bound. Hence, the macroscopic locality alone cannot characterize the quantum correlation.

**Theorem**
Macroscopic locality completely characterizes the bipartite quantum correlation with binary outputs with unbiased marginals.