Operational characterization of quantum nonlocality

Ryuhei Mori

Tokyo Institute of Technology

Motivation

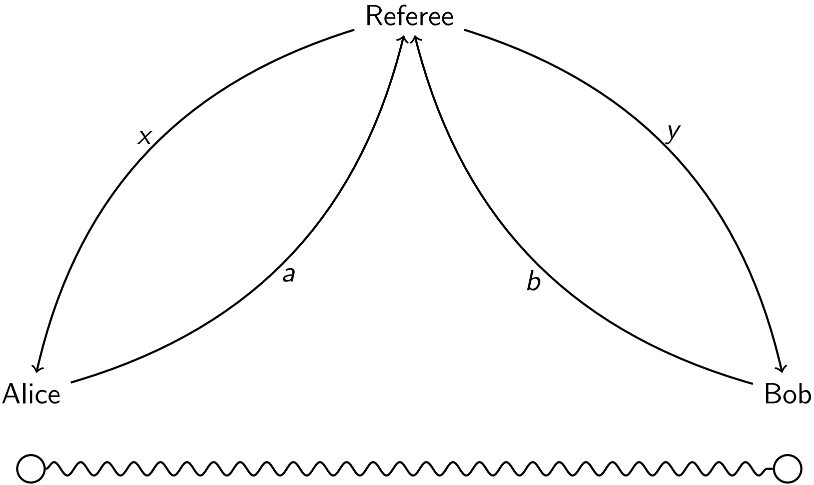
- Quantum physics has a beautiful mathematical representation.
- But, we do not have any "explanation" for the quantum physics.
- We need to find postulates of quantum physics.

  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.

CHSH game [Bell 1964 **11353**]

[Clauser, Horne, Shimony, Holt 1969 **5779**]



Alice and Bob win iff $a \oplus b = x \wedge y$.

CHSH winning probability

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

$$
\begin{aligned}
a_0 \oplus b_0 &= 0 \\
a_0 \oplus b_1 &= 0 \\
a_1 \oplus b_0 &= 0 \\
a_1 \oplus b_1 &= 1
\end{aligned}
$$

- The maximum CHSH winning probability in quantum physics is $(2+\sqrt{2})/4 \approx 0.854$ [Tsirelson 1980 **1195**].

Locality (Hidden variable model)

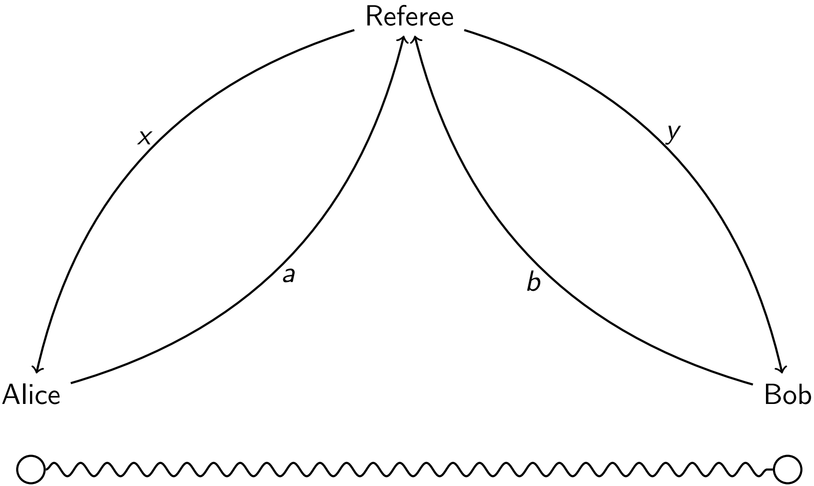
Joint preparation and independent measurements.

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

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

Quantum physics allow nonlocal behaviors.

Two-party statistics



$$P(a, b \mid x, y), \qquad \forall a, b \in \{0, 1\}, x, y \in \{0, 1\}$$

No-signaling condition

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

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

$$\sum_{a\in\{0,1\}} P(a, b \mid 0, y) = \sum_{a\in\{0,1\}} P(a, b \mid 1, y), \qquad \forall b,\ y \in \{0, 1\}.$$

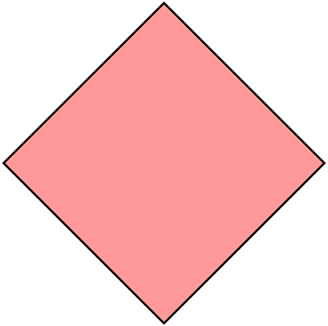
The 8-dimensional linear space and no-signaling polytope

$$\sum_{a\in\{0,1\},\, b\in\{0,1\}} P(a,b \mid x,y) = 1, \qquad x\in\{0,1\},\ y\in\{0,1\}.$$

$$\begin{aligned}
\sum_{b\in\{0,1\}} P(0,b \mid 0,0) &= \sum_{b\in\{0,1\}} P(0,b \mid 0,1)\\
\sum_{b\in\{0,1\}} P(0,b \mid 1,0) &= \sum_{b\in\{0,1\}} P(0,b \mid 1,1)\\
\sum_{a\in\{0,1\}} P(a,0 \mid 0,0) &= \sum_{a\in\{0,1\}} P(a,0 \mid 1,0)\\
\sum_{a\in\{0,1\}} P(a,0 \mid 0,1) &= \sum_{a\in\{0,1\}} P(a,0 \mid 1,1).
\end{aligned}$$

$16 - 8 = 8$-dimensional linear space.

No-signaling polytope



Local polytope

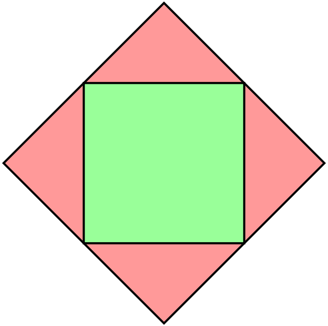
Deterministic choice

$$a = A(x), \qquad\qquad b = B(y).$$

Local polytope

$$\operatorname{conv}\left(\left\{\left\{P(a, b \mid x, y) = \delta_{(a,b),(A(x),B(y))}\right\}_{a,b,x,y} \mid A, B \in \{0,1\}^{\{0,1\}}\right\}\right).$$

No-signaling polytope and local polytope



CHSH inequality: Facets of the local polytope

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

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

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

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

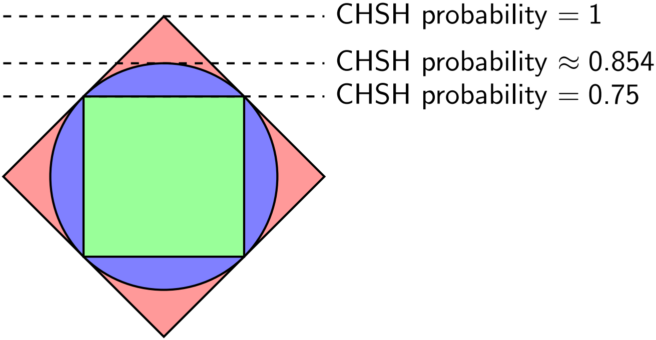
CHSH inequality [Clauser, Horne, Shimony, Holt 1969 **5779**].
CHSH inequality is the only non-trivial facets [Froissard 1981 **81**], [Fine 1982 **845**].

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 **955**]

No-signaling polytope, local polytope and quantum correlation



Question:

Why does quantum physics prohibits CHSH probability greater than $(2+\sqrt{2})/4 \approx 0.854$?

Topics

- $p_{\text{CHSH}} = 1 \quad \Longrightarrow$ Communication complexity (CC) of arbitrary function is 1 bit.
  [van Dam 2013 (quant-ph/0501159) (Ph.D. thesis 1999) **168**]

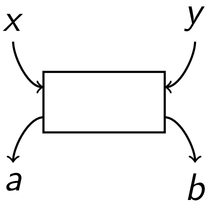
- $p_{\text{CHSH}} > (3+\sqrt{6})/6 \approx 0.908 \quad \Longrightarrow$ CC of arbitrary function is 1 bit.
  [Brassard, Buhrman, Linden, Méthot, Tapp, Unger 2006 **250**]

- $p_{\text{CHSH}} > (2+\sqrt{2})/4 \approx 0.854 \quad \Longrightarrow$ Information causality is violated.
  [Pawłowki, Paterek, Kaszlikowski, Scarani, Winter, Zukowki 2009 **375**]

- Brassard et al.'s result cannot be improved by generalizations of their techniques [Mori 2016].

Nonlocal box

Abstract device with two input ports and two output ports.



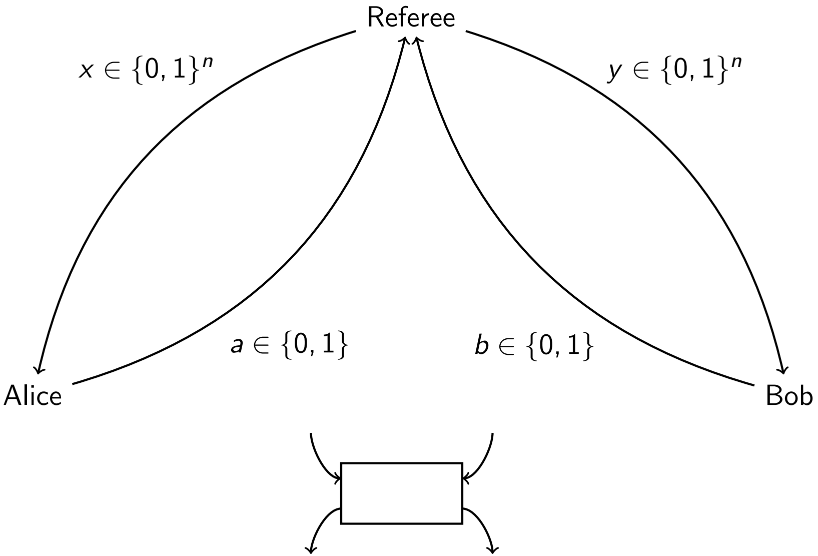
Isotropic nonlocal box

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

This does not lose generality since

$$\begin{aligned} x \wedge y &= (x \oplus r_1) \wedge (y \oplus r_2) \oplus x \wedge r_2 \oplus r_1 \wedge y \oplus r_1 \wedge r_2 \\ &= a \oplus b \oplus e \oplus x \wedge r_2 \oplus r_1 \wedge y \oplus r_1 \wedge r_2 \\ &= (a \oplus x \wedge r_2 \oplus r_1 \wedge r_2) \oplus (b \oplus r_1 \wedge y) \oplus e \end{aligned}$$

XOR game



Alice and Bob win iff $a \oplus b = f(x, y)$.

PR box gives a winning probability 1

[van Dam 2013 (arXiv 2005) (PhD. thesis 1999) **168**]

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.

$$f(x, y) = \bigoplus_z \mathbb{I}\{x = z\} \wedge f(z, y).$$

Recall Alice and Bob have nonlocal boxes with

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

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

$$\begin{aligned} \bigoplus_z \mathbb{I}\{x = z\} \wedge f(z, y) &= \bigoplus_z (a_z \oplus b_z) \\ &= \left(\bigoplus_z a_z \right) \oplus \left(\bigoplus_z b_z \right). \end{aligned}$$

Bias

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

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

Let δ be a bias of the CHSH probability p_{CHSH}.

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

- If X is ± 1 random variable, the bias (for a prob. of 1) is $\mathbb{E}[X] = \frac{1+\delta}{2} - \frac{1-\delta}{2} = \delta$.
- If X and Y are independent 0-1 random variables with bias (for a prob. of 0) δ_X and δ_Y, respectively, the bias of $X \oplus Y$ is $\delta_X \delta_Y$.

Constant winning probability

[Brassard, Buhrman, Linden, Méthot, Tapp, Unger 2006 **250**]

$p_{\mathrm{CHSH}} > \frac{3+\sqrt{6}}{6} \approx 0.908 \iff \delta > \sqrt{\frac{2}{3}}$
$\implies$ 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 $r' \in \{0,1\}$,

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

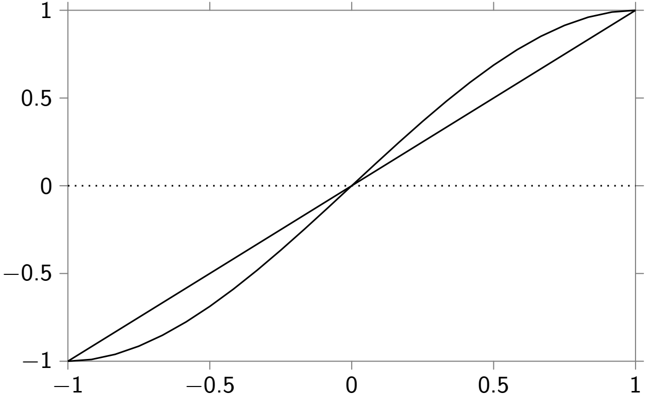
$a \oplus b = f(x, y)$ with probability

$$\frac{1}{2^n} + \left(1 - \frac{1}{2^n}\right)\frac{1}{2} = \frac{1 + 2^{-n}}{2}.$$

Bias amplification by Maj_3

$$\mathrm{Maj}_3(z_1, z_2, z_3) = \frac{1}{2}\left(z_1 + z_2 + z_3 - z_1 z_2 z_3\right)$$

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

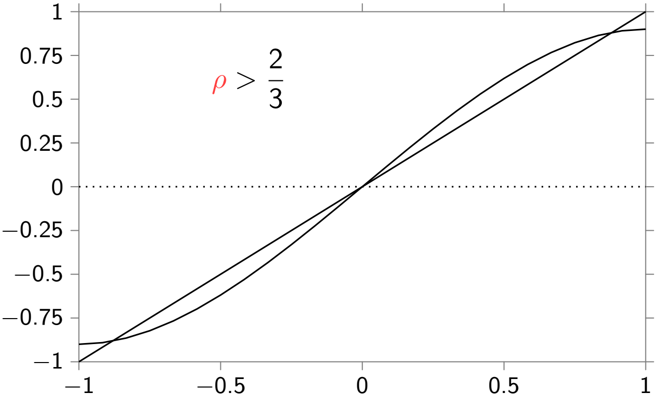


Bias amplification by noisy Maj_3

[von Neumann 1956 **2588**]

$$\mathrm{Maj}_3(z_1, z_2, z_3) = \frac{1}{2}\left(z_1 + z_2 + z_3 - z_1 z_2 z_3\right)$$

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



Probability of succeeding of computation of Maj_3

$$\mathrm{Maj}_3(z_1, z_2, z_3) = z_1 z_2 \oplus z_2 z_3 \oplus z_3 z_1$$

$$\begin{aligned}
&\mathrm{Maj}_3(a_1 \oplus b_1, a_2 \oplus b_2, a_3 \oplus b_3)\\
&= (a_1 \oplus b_1)(a_2 \oplus b_2) \oplus (a_2 \oplus b_2)(a_3 \oplus b_3) \oplus (a_3 \oplus b_3)(a_1 \oplus b_1)\\
&= (a_1 \oplus a_2)(b_2 \oplus b_3) \oplus (a_2 \oplus a_3)(b_1 \oplus b_2)\\
&\qquad \oplus a_1 a_2 \oplus a_2 a_3 \oplus a_3 a_1\\
&\qquad \oplus b_1 b_2 \oplus b_2 b_3 \oplus b_3 b_1\\
&= (\alpha_0 \oplus \beta_0 \oplus e_0) \oplus (\alpha_1 \oplus \beta_1 \oplus e_1)\\
&\qquad \oplus a_1 a_2 \oplus a_2 a_3 \oplus a_3 a_1\\
&\qquad \oplus b_1 b_2 \oplus b_2 b_3 \oplus b_3 b_1\\
&= (\alpha_0 \oplus \alpha_1 \oplus a_1 a_2 \oplus a_2 a_3 \oplus a_3 a_1) \oplus (\beta_0 \oplus \beta_1 \oplus b_1 b_2 \oplus b_2 b_3 \oplus b_3 b_1) \oplus e_0 \oplus e_1.
\end{aligned}$$

$$\delta^2 > \frac{2}{3} \iff \delta > \sqrt{\frac{2}{3}} \iff p > \frac{1 + \sqrt{\frac{2}{3}}}{2} = \frac{3 + \sqrt{6}}{6} \approx 0.908.$$

Generalization of Brassard et al's protocol

- Why Maj_3 ?

- Replace 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 Maj_3 is the unique optimal function in a simple generalization [Mori, Phys. Rev. A 94, 052130, 2016].

Information causality

[Pawłowki, Paterek, Kaszlikowski, Scarani, Winter, Zukowki 2009 **375**]

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

$$\mathrm{Addr}_n(x_0, \dots, x_{2^n-1}, y_1, \dots, y_n) := x_y$$

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

Theorem ([Pawłowski, Paterek, Kaszlikowski, Scarani, Winter, Zukowski 2009 **375**])

There is an adaptive protocol of the XOR game for the address function with bias δ^n.

Proof

Induction.
For $n = 1$, from

$$\mathrm{Addr}_1(x_0, x_1, y_1) = x_0 \oplus y_1(x_0 \oplus x_1)$$

there is a non-adaptive protocol with bias δ.

Proof (Cont'd).

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

where

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

$$\begin{aligned}
&\mathrm{Addr}_1(z_0, z_1, y_n) = \mathrm{Addr}_1(a_0 \oplus b_0 \oplus e_0, a_1 \oplus b_1 \oplus e_1, y_n) \\
&= \mathrm{Addr}_1(a_0, a_1, y_n) \oplus b_{y_n} \oplus e_{y_n} \\
&= a' \oplus b' \oplus e' \oplus b_{y_n} \oplus e_{y_n} \\
&= a' \oplus (b' \oplus b_{y_n}) \oplus (e' \oplus e_{y_n}).
\end{aligned}$$

This protocol has bias δ^n. $\square$

Repetition

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

From

$$\left(2\sqrt{\epsilon(1-\epsilon)}\right)^m = (1-\delta^{2n})^{\frac{m}{2}}$$

error probability goes to zero if

$$m \gg \delta^{-2n}.$$

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

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.