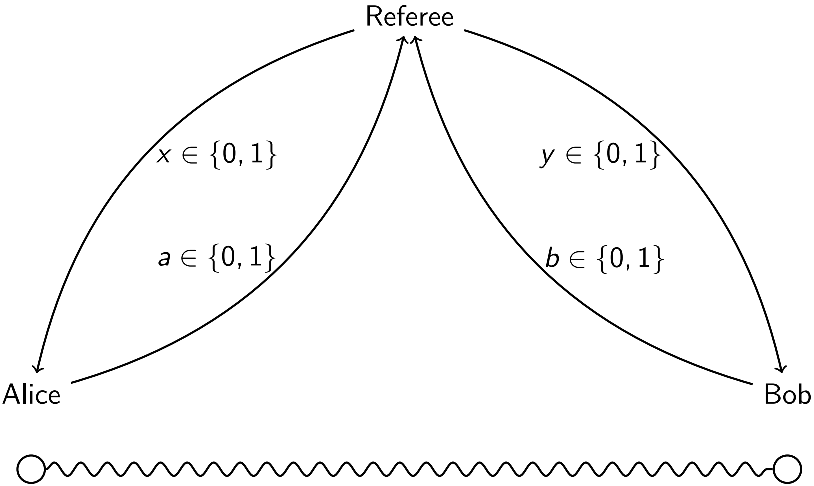
No-signaling polytope and multiplayer XOR games

Ryuhei Mori

Tokyo Institute of Technology

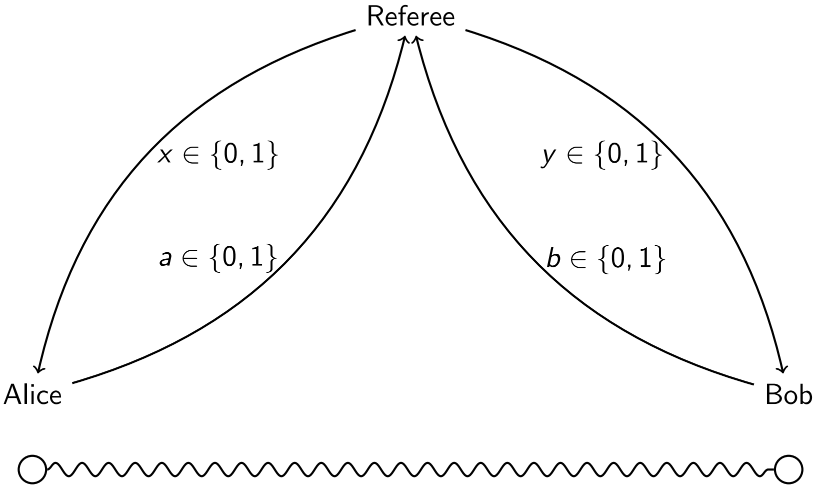
December 20, 2019

Bell test: CHSH game (1964, 1969)



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

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

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

$$\sum_{b\in\{0,1\}} P(0, b \mid 0, 0) = \sum_{b\in\{0,1\}} P(0, b \mid 0, 1)$$

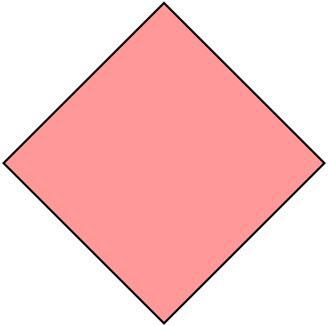
$$\sum_{b\in\{0,1\}} P(0, b \mid 1, 0) = \sum_{b\in\{0,1\}} P(0, b \mid 1, 1)$$

$$\sum_{a\in\{0,1\}} P(a, 0 \mid 0, 0) = \sum_{a\in\{0,1\}} P(a, 0 \mid 1, 0)$$

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

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

No-signaling polytope



Local polytope

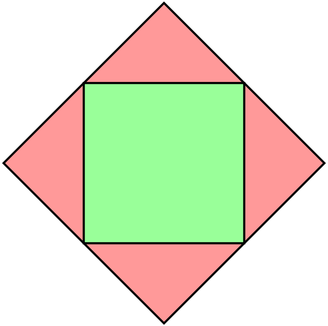
Deterministic choice

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

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

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

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

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

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

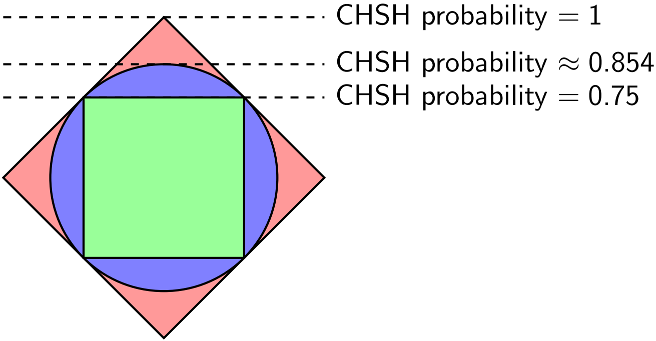
CHSH inequality [Clauser, Horne, Shimony, Holt 1969].
CHSH inequality is the only non-trivial facets [Froissard 1981], [Fine 1982].

No-signaling condition admits CHSH probability 1

$$P(0,0 \mid 0,0) = P(1,1 \mid 0,0) = 1/2$$
$$P(0,0 \mid 0,1) = P(1,1 \mid 0,1) = 1/2$$
$$P(0,0 \mid 1,0) = P(1,1 \mid 1,0) = 1/2$$
$$P(0,1 \mid 1,1) = P(1,0 \mid 1,1) = 1/2$$

PR box
[Popescu and Rohrlich 1994]

No-signaling polytope, local polytope and quantum correlation



Question:

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

Multiplayer XOR game

- n players.
- j-th player are given $x_j \in \mathcal{X}$ according to a probability distribution $p(x_1, \dots, x_n)$.
- j-th player outputs $a^{(j)}$.
- Players win iff $\bigoplus_{j=1}^{n} a^{(j)} = f(x_1, \dots, x_n)$.

Example: Mermin–GHZ game

- 3 players.
- $\mathcal{X} = \{0, 1\}$. $p(x_1, x_2, x_3) = 1/4$ for $x_1 \oplus x_2 \oplus x_3 = 0$.
- $f(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3$.

The winning condition for Mermin–GHZ game

$$
\begin{aligned}
a_0 \oplus b_0 \oplus c_0 &= 0 \\
a_1 \oplus b_0 \oplus c_1 &= 1 \\
a_0 \oplus b_1 \oplus c_1 &= 1 \\
a_1 \oplus b_1 \oplus c_0 &= 1
\end{aligned}
$$

The sum is $0 = 1$ which means that there is no solution in the above system of linear equations. The largest classical winning probability is $3/4$.

Quantum theory allows the winning probability 1 (Mermin–GHZ paradox).

Observables for XOR game

For a single qubit projective measurement $\{|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|\}$, we can define an observable $A := |\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|$. Then, $\mathrm{Tr}(\rho|\psi_x\rangle\langle\psi_x|) = (1 + (-1)^x \mathrm{Tr}(\rho A))/2$. Especially,

$$\mathrm{Tr}(\rho A) = 1 \iff \mathrm{Tr}(\rho|\psi_0\rangle\langle\psi_0|) = 1$$
$$\mathrm{Tr}(\rho A) = -1 \iff \mathrm{Tr}(\rho|\psi_1\rangle\langle\psi_1|) = 1.$$

For multiple qubits,

$$\mathrm{Tr}\left(\rho\bigotimes_{j=1}^{n} A_j\right) = 1 \iff \sum_{x:\,|x| \text{ is even}} \mathrm{Tr}\left(\rho\bigotimes_{j=1}^{n}|\psi_{x_j}\rangle\langle\psi_{x_j}|\right) = 1$$
$$\mathrm{Tr}\left(\rho\bigotimes_{j=1}^{n} A_j\right) = -1 \iff \sum_{x:\,|x| \text{ is odd}} \mathrm{Tr}\left(\rho\bigotimes_{j=1}^{n}|\psi_{x_j}\rangle\langle\psi_{x_j}|\right) = 1$$

since the eigenvectors of $\bigotimes_{j=1}^{n} A_j$ is $|\psi_{x_1}^{(1)}\rangle|\psi_{x_2}^{(2)}\rangle\cdots|\psi_{x_n}^{(n)}\rangle$ with eigenvalue $(-1)^{x_1+\cdots+x_n}$ for $x_1\cdots x_n \in \{0,1\}^n$.

The quantum strategy for Mermin–GHZ game

- The GHZ state is shared.

$$|\mathrm{GHZ}\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

- Alice, Bob and Charlie measure their state by X if the input is 0, and by Y if the input is 1.
- If $x_1 = x_2 = x_3 = 0$, $\langle \mathrm{GHZ}| X^{\otimes 3} |\mathrm{GHZ}\rangle = 1$.
- If $x_1 = x_2 = 1$, $x_3 = 0$, $\langle \mathrm{GHZ}| Y^{\otimes 2} \otimes X |\mathrm{GHZ}\rangle = -1$.
- This means that the winning probability of the Mermin–GHZ game is 1.

The optimal strategy for multiplayer XOR game with binary inptus

In the following, we consider general multiplayer XOR games with binary inptus ($\mathcal{X} = \{0, 1\}$).

- The generalized GHZ state is shared.

$$|\mathrm{GHZ}_n\rangle := \frac{1}{\sqrt{2}}(|0 \cdots 0\rangle + |1 \cdots 1\rangle).$$

- j-th player measures his or her qubit by $\cos\theta_0^{(j)} X + \sin\theta_0^{(j)} Y$ if the input is 0, and by $\cos\theta_1^{(j)} X + \sin\theta_1^{(j)} Y$ if the input is 1.

The winning probability [Werner & Wolf 2001]

$$\mathrm{Tr}\left(|\mathrm{GHZ}_n\rangle \langle \mathrm{GHZ}_n| \bigotimes_{j=1}^{n} (\cos\theta_{x_j}^{(j)} X + \sin\theta_{x_j}^{(j)} Y) \right)$$

$$= \frac{1}{2} \sum_{z\in\{0,1\}} \prod_{j=1}^{n} \left(\cos\theta_{x_j}^{(j)} \langle z| X |\bar{z}\rangle + \sin\theta_{x_j}^{(j)} \langle z| Y |\bar{z}\rangle \right)$$

$$= \frac{1}{2} \sum_{z\in\{0,1\}} \prod_{j=1}^{n} \left(\cos\theta_{x_j}^{(j)} + \sin\theta_{x_j}^{(j)} (-1)^z i \right)$$

$$= \frac{1}{2} \sum_{z\in\{0,1\}} \prod_{j=1}^{n} \exp\left\{ (-1)^z \theta_{x_j}^{(j)} \right\}$$

$$= \frac{1}{2} \left(\exp\left\{ i \sum_{j=1}^{n} \theta_{x_j}^{(j)} \right\} + \exp\left\{ -i \sum_{j=1}^{n} \theta_{x_j}^{(j)} \right\} \right)$$

$$= \cos\left\{ \sum_{j=1}^{n} \theta_{x_j}^{(j)} \right\}$$

Spectral norm

For $A \in L(\mathbb{C}^n, \mathbb{C}^m)$,

$$\|A\| := \max_{|\psi\rangle \in \mathbb{C}^n :\ \langle\psi|\psi\rangle = 1} \sqrt{\langle\psi| A^\dagger A |\psi\rangle}$$

$\|A\|$ is the largest singular value of A.

For any unitary matrices $U \in L(\mathbb{C}^m)$ and $V \in L(\mathbb{C}^n)$,

$$\|UAV\| = \|A\|.$$

The upper bound of the winning probability [Werner & Wolf 2001]

Let $\beta(x_1, \dots, x_n) := p(x_1, \dots, x_n)(-1)^{f(x_1,\dots,x_n)}$ and $U_j = A_j^{(0)} A_j^{(1)}$.

$$\sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \mathrm{Tr}\left(\rho \bigotimes_{j=1}^{n} A_j^{(x_j)}\right) = \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \langle\psi| \bigotimes_{j=1}^{n} A_j^{(x_j)} |\psi\rangle$$

$$= \langle\psi| \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \bigotimes_{j=1}^{n} A_j^{(x_j)} |\psi\rangle \le \left\| \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \bigotimes_{j=1}^{n} A_j^{(x_j)} \right\|$$

$$= \left\| \bigotimes_{j=1}^{n} A_j^{(0)} \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \bigotimes_{j=1}^{n} U_j^{x_j} \right\| = \left\| \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \bigotimes_{j=1}^{n} U_j^{x_j} \right\|$$

$$\le \max_{\theta_1,\dots,\theta_n} \left| \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \exp\left\{ i \sum_{j=1}^{n} x_j \theta_j \right\} \right|$$

$$= \max_{\theta_0,\dots,\theta_n} \sum_{x_1,\dots,x_n} \beta(x_1, \dots, x_n) \cos\left\{ \theta_0 + \sum_{j=1}^{n} x_j \theta_j \right\}.$$

The strategy with $\theta_x^{(j)} := \theta_0/n + x\theta_j$ achieves this bound.

Existence of winning strategies of multiplayer XOR game

A classical winning strategy exists iff there exists $(a_x^{(j)} \in \mathbb{F}_2)_{j=1,\ldots,n,\, x\in\mathcal{X}}$ such that

$$\sum_{j=1}^{n} a_{x_j}^{(j)} = f(x_1, \ldots, x_n) \mod 2$$

for all $x \in \operatorname{supp}(p)$.

When $\mathcal{X} = \{0, 1\}$,
a quantum winning strategy exists iff there exists $(\theta_x^{(j)} \in \mathbb{Q})_{j=1,\ldots,n,\, x\in\mathcal{X}}$ such that

$$\sum_{j=1}^{n} \theta_{x_j}^{(j)} = f(x_1, \ldots, x_n) \mod 2$$

for all $x \in \operatorname{supp}(p)$.

Assignments

1. Show that the PR-box satisfies the no-signaling condition.
2. Show an optimal strategy for the generalized Mermin–GHZ game, defined by

$$
\begin{aligned}
p(x_1, \dots, x_n) &:= \frac{\mathbb{I}\left\{\sum_{j=1}^n x_j \text{ is divisible by } 2^\ell\right\}}{\left|\left\{z \in \{0,1\}^n \mid \sum_{j=1}^n z_j \equiv 0 \mod 2^\ell\right\}\right|}, \\
f(x_1, \dots, x_n) &:= \frac{\sum_{j=1}^n x_j}{2^\ell} \mod 2.
\end{aligned}
$$