NON-LOCALITY
AND
CONTEXTUALITY
IN
QUANTUM
MECHANICS

Lecture - II

GURUPRASAD KAR
INDIAN STATISTICAL INSTITUTE
KOLKATA
Bell Locality condition:

\[ p(a, b | x, y, \lambda) = p(a | x, \lambda) \ p(b | y, \lambda) \]

Parameter independence condition:

\[ p(a | x, y, \lambda) = p(a | x, \lambda) \]
\[ p(b | x, y, \lambda) = p(b | y, \lambda) \]

which does not necessarily imply;

\[ p(a | x, y, \lambda) = p(a | x, y, b, \lambda) \]

Parameter independence implies;

\[ p(a | x, y, \lambda) = \sum_b p(a | x, y, b, \lambda) = p(a | x, \lambda) \]

for all \( y \), with outcomes \( b \).

This is actually no-signaling condition respecting relativity principle.
Now the question is whether QM can be reproduced by a theory obeying only the parameter independence. But it is trivially true as QM is itself such a theory.

\[ p(x|a, b, \psi) = p(x|a, \psi) \text{ for all } \psi. \]

Next question:

Can quantum mechanical correlation be reproduced by some other (non-local) correlation (satisfying parameter independence) which is qualitatively different from quantum correlation?

The answer is 'yes'.

There is a non-local correlation (known as P-R correlation) which reproduces singlet statistics.
**Popescu-Rorlich Correlation**

\[
x \downarrow \quad y \downarrow
\]

\[
a \downarrow \quad b \downarrow
\]

<table>
<thead>
<tr>
<th>Input ((x))</th>
<th>Input ((y))</th>
<th>output ((a))</th>
<th>output ((b))</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>(x_1)</td>
<td>(y_1)</td>
<td>+1</td>
<td>+1</td>
<td>1/2</td>
</tr>
<tr>
<td></td>
<td>-1</td>
<td></td>
<td>-1</td>
<td>1/2</td>
</tr>
<tr>
<td>(x_1)</td>
<td>(y_2)</td>
<td>+1</td>
<td>+1</td>
<td>1/2</td>
</tr>
<tr>
<td></td>
<td>-1</td>
<td></td>
<td>-1</td>
<td>1/2</td>
</tr>
<tr>
<td>(x_2)</td>
<td>(y_1)</td>
<td>+1</td>
<td>+1</td>
<td>1/2</td>
</tr>
<tr>
<td></td>
<td>-1</td>
<td></td>
<td>-1</td>
<td>1/2</td>
</tr>
<tr>
<td>(x_2)</td>
<td>(y_2)</td>
<td>+1</td>
<td>-1</td>
<td>1/2</td>
</tr>
<tr>
<td></td>
<td>-1</td>
<td></td>
<td>+1</td>
<td>1/2</td>
</tr>
</tbody>
</table>

\[
< x_1 y_1 > + < x_1 y_2 > + < x_2 y_1 > - < x_2 y_2 > = 4
\]

\[
x_1 \rightarrow x = 0, \quad x_2 \rightarrow x = 1, \quad y_1 \rightarrow y = 0, \quad y_2 \rightarrow y = 1
\]

\[
+1 \rightarrow 0 \quad -1 \rightarrow 1
\]

\[
a \oplus b = xy
\]
Simulating singlet statistics

Alice and Bob share two set of shared randomness $\lambda_1$ and $\lambda_2$ which are unit vectors randomly and independently distributed on Poincare sphere.

$$sgn(m.\lambda_1) + sgn(m.\lambda_2) = x$$

$$y = sgn(n.\lambda_+) + sgn(n.\lambda_-)$$

\[
\begin{array}{c}
\downarrow \\
P-R \text{ Box} \\
\downarrow \\
\downarrow \\
a \\
\downarrow \\
b \\
\end{array}
\]

Alice outputs

$$A = a + sgn(m.\lambda_1)$$

Bob outputs

$$B = b + sgn(n.\lambda_+) + 1$$

where

$$\lambda_\pm = \lambda_1 \pm \lambda_2$$

$$sgn(x) = 1 \text{ if } x \geq 0 \text{ and } sgn(x) = 0 \text{ if } x < 0$$

This strategy reproduces singlet statistics.

For a given direction $m$ and $\lambda_1$, $a$ being completely random $A$ is also completely random.
Leggett suggested a different local statistics at Nonlocal Hidden Variable level
and showed that such theory fails to reproduce singlet statistics.

Polarized along $u$

Polarized along $v$

Leggett puts the following condition;

$$p(x = +1|a, \lambda) = \frac{1}{2} (1 + a \cdot u)$$

$$p(y = +1|b, \lambda) = \frac{1}{2} (1 + b \cdot v)$$

$a, b, u$ and $v$ are unit vectors.

as if the local particles are polarized along $u$ and $v$.

and shows that this (nonlocal) hidden variable theory can not
reproduce singlet statistics.
Now we consider a hidden variable theory which satisfy parameter independence.

\[ p(x|a, b, \lambda) = p(x|a, \lambda) \]
\[ p(y|a, b, \lambda) = p(y|b, \lambda) \]

\[
\int p(x, y|a, b, \lambda) \rho(\lambda) d\lambda = p(x, y|a, b, \psi_{AB})
\]
\[
\int p(x|a, \lambda) \rho(\lambda) d\lambda = p(x|a, \rho_A)
\]
\[
\int p(y|b, \lambda) \rho(\lambda) d\lambda = p(y|b, \rho_B)
\]

But \[ p(x|a, \lambda) \neq p(x|a, \rho_A) \]

Singlet statistics can not be reproduced by such theory.

(Colbeck & Renner, PRL, 2008 and Liefer, Quanta, 2014.)
Sketch of the proof:

Distance between two probability distribution $P(X)$ and $Q(Y)$:

$$D(P(X), Q(Y)) = \frac{1}{2} \sum_{j=0}^{1} |P(X = j) - Q(Y = j)|$$

* $P''(X) = pP(X) + (1 - p)P'(X)$  \quad $Q''(Y) = pQ(Y) + (1 - p)Q'(Y)$

$$D(P''(X), Q''(Y)) \leq pD(P(X), P(Y)) + (1 - p)D(P'(X), Q'(Y))$$

* $P(X, Y)$ is a joint distribution with the following marginals;

$$P(X) = \sum_{k} P(X, Y = k)$$  \quad $$P(Y) = \sum_{j} P(X = j, Y)$$

Then \quad $D(P(X), P(Y)) \leq P(X \neq Y)$

* The distance satisfies triangle inequality;

$$D(P(X), Q(Y)) \leq D(P(X), R(Z)) + D(Q(Y), R(Z))$$
where $a$ refers to some measurement on Alice's side and $b$ on Bob's side. The outcome $X$ and $Y$ can be either 0 or 1.

A correlation measure:

$$I_N(\lambda) = P(X = Y|0, 2N - 1, \lambda) + \sum_{a,b,|a-b|=1} P(X \neq Y|a, b, \lambda)$$

All local realistic correlations: $I_N = \int I_N(\lambda)\rho(\lambda) d\lambda \geq 1$
\[ \bar{X} = X + 1 \mod 2 \]

so that when \( X = 1 \), \( \bar{X} = 0 \) and vice-versa.

\[
I_N(\lambda) = P(\bar{X} \neq Y|0, 2N - 1, \lambda) + \sum_{a,b,|a-b|=1} P(X \neq Y|a, b, \lambda)
\]

\[
\geq D(P(\bar{X}|0, 2N - 1, \lambda), P(Y|0, 2N - 1, \lambda)) + \sum_{a,b,|a-b|=1} D(P(X|a, \lambda), P(Y|a, \lambda), P(Y|b, \lambda)) \quad \text{(parameter independence)}
\]

\[
= D(P(\bar{X}|0, \lambda), P(Y|2N - 1, \lambda)) + \sum_{a,b,|a-b|=1} D(P(X|a, \lambda), P(Y|b, \lambda))
\]

\[
= D(P(\bar{X}|0, \lambda), P(Y|2N - 1, \lambda)) + D(P(X|2N - 2, \lambda), P(Y|2N - 1, \lambda))
\]

\[
+ D(P(X|2N - 2, \lambda), P(Y|2N - 3, \lambda)) + D(P(X|2N - 4, \lambda), P(Y|2N - 3, \lambda))
\]

\[
+ D(P(X|2, \lambda), P(Y|1, \lambda)) + D(P(X|0, \lambda), P(Y|1, \lambda))
\]

\[
\geq D(P(\bar{X}|0, \lambda), P(X|2N - 2, \lambda)) + D(P(X|2N - 2, \lambda), P(Y|2N - 3, \lambda))
\]

\[
+ D(P(X|2N - 4, \lambda), P(Y|2N - 3, \lambda)) + D(P(X|2, \lambda), P(Y|1, \lambda)) + D(P(X|0, \lambda), P(Y|1, \lambda)) \geq D(P(\bar{X}|0, \lambda), P(X|0, \lambda)
\]

\{ \text{Triangle inequality in each step.} \}
\[ |\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}} \left[ |0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B \right] \]

Alice's measurement basis

\[ M_a \rightarrow |\psi^a_j\rangle_A = \cos \frac{\theta^a_j}{2} |0\rangle_A + \sin \frac{\theta^a_j}{2} |1\rangle_A \]

\[ \theta^a_j = \left( \frac{a}{2N} + j \right) \pi, \quad j = 0, 1 \]

Bob's measurement basis

\[ M_b \rightarrow |\psi^b_k\rangle_B = \cos \frac{\theta^b_k}{2} |0\rangle_B + \sin \frac{\theta^b_k}{2} |1\rangle_B \]

\[ \theta^b_k = \left( \frac{b}{2N} + k \right) \pi, \quad k = 0, 1 \]
Quantum mechanical results for the singlet

\[ P(X = j, Y = k | a, b, \phi^+) = \frac{1}{2} \cos^2 \left( \left( \frac{a - b}{2N} + j - k \right) \frac{\pi}{2} \right) \]

\[ P(X = Y | a = 0, b = 2N - 1, \phi^+) = \sin^2 \frac{\pi}{4N} \]

\[ P(X \neq Y | a, b, |a - b| = 1, \phi^+) = \sin^2 \frac{\pi}{4N} \]

\[ I_N^{QM}(\phi^+) = 2NS\sin^2 \frac{\pi}{4N} \leq \frac{\pi^2}{8N} \rightarrow 0 \]

for large \( N \)
Quantum reproducibility condition:

\[
\int I_N(\lambda) \rho(\lambda) d\lambda = I_{N}^{Q_{M}}(\phi^+)
\]

We have seen \( I_{N}^{Q_{M}}(\phi^+) = 0 \) for \( N \to \infty \)

which implies;

\[
I_N(\lambda) \to 0
\]

\[
D(P(\bar{X}|0, \lambda), P(X|0, \lambda)) = 0
\]

\[
p(0|M_0, \lambda) = p(1|M_0, \lambda)
\]

Normalization for probability;

\[
p(0|M_0, \lambda) + p(1|M_0, \lambda) = 1
\]

\[
p(0|M_0, \lambda) = p(1|M_0, \lambda) = \frac{1}{2}, \text{ for all } \lambda
\]
Perfect Security with P-R Box

\[ x = 0, 1 \]
\[ y = 0, 1 \]
\[ a = 0, 1 \]
\[ b = 0, 1 \]

\[ P_{PR}(ab|xy) = \begin{cases} 
\frac{1}{2} & \text{if } a \oplus b = x \cdot y \\
0 & \text{otherwise}
\end{cases} \]

This correlation is a vertex of the bipartite no-signaling polytope.

Protocol:

* Alice and Bob inputs their bits randomly and collect the output datas.

* By revealing some of their results, they check whether the correlation supplied to them is OK.

* Alice reveals her inputs and Bob flips his bit when both of their inputs is 1.
P-R correlation is completely uncorrelated with the rest of the world.

\[ P_{abe/XYZ} = P_{ab/XY}P_{e/Z} \]

Hypothetical correlation with large no of observables

Hence for large no. of observables quantum correlation becomes monogamous. Hence device independent cryptography.
For PR correlation: \( I(B: E) = 0 \),
Can this be achieved for quantum correlation?

\[
<\text{Chain}> = \sum_{i=1}^{N} [p(a_i \neq b_i) + p(a_i = b_i)]
\]

For proper choice of observables:

\[
<\text{Chain}> = N[1 - p\cos\left(\frac{\pi}{2N}\right)] \quad \text{for Werner state.}
\]

\[
I(B: E) \leq <\text{chain}>
\]

For maximally entangled state \((p = 1)\) and for large \(N\)

\[
<\text{chain}> = 2N \sin^2\left(\frac{\pi}{4N}\right) = \frac{\pi^2}{8N} \approx 0
\]

Key rate will be 1 like PR correlation.

Kochen-Specker Game

The local but contextual model can not reproduce quantum correlation.

Rename the 18 vectors

\[ S_1 = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\} \equiv \{S^1_i, i = 1, 2, 3, 4\} \]

\[ S_2 = \{\varphi_1, \varphi_5, \varphi_6, \varphi_7\} \equiv \{S^2_i, i = 1, 2, 3, 4\} \]

\[ S_3 = \{\varphi_8, \varphi_{18}, \varphi_3, \varphi_9\} \equiv \{S^3_i, i = 1, 2, 3, 4\} \]

\[ S_4 = \{\varphi_8, \varphi_{10}, \varphi_7, \varphi_{11}\} \equiv \{S^4_i, i = 1, 2, 3, 4\} \]

\[ S_5 = \{\varphi_2, \varphi_5, \varphi_{12}, \varphi_{13}\} \equiv \{S^5_i, i = 1, 2, 3, 4\} \]

\[ S_6 = \{\varphi_{18}, \varphi_{10}, \varphi_{13}, \varphi_{14}\} \equiv \{S^6_i, i = 1, 2, 3, 4\} \]

\[ S_7 = \{\varphi_{15}, \varphi_{16}, \varphi_4, \varphi_9\} \equiv \{S^7_i, i = 1, 2, 3, 4\} \]

\[ S_8 = \{\varphi_{15}, \varphi_{17}, \varphi_6, \varphi_{11}\} \equiv \{S^8_i, i = 1, 2, 3, 4\} \]

\[ S_9 = \{\varphi_{16}, \varphi_{17}, \varphi_{12}, \varphi_{14}\} \equiv \{S^9_i, i = 1, 2, 3, 4\} \]
Consider a game:

They are not allowed to communicate after the game starts.

Alice has to assign 1 to one of the vector and 0 to other three vectors.

Bob has to assign 1 or 0 to his single vector.

Winning condition:

\[ v_{Alice}(S'_k) = v_{Bob}(S'_k) \]

in each turn.
\[ |\varphi>_{AB} = \frac{1}{4} [ |\varphi_1>_{A} |\varphi_1>_{B} + |\varphi_2>_{A} |\varphi_2>_{B} + |\varphi_3>_{A} |\varphi_3>_{B} + |\varphi_4>_{A} |\varphi_4>_{B} ] \]

\[ |\varphi^+> = \frac{1}{\sqrt{d}} \sum |i>_{A} |i>_{B} \]

\[ U_A \otimes U_B |\varphi^+> = |\varphi^+> \]

For real vectors: \[ U_B^* = U_B \]

\[ |\varphi>_{AB} = \frac{1}{4} \sum_i |S^i_1>_{A} \otimes |S^i_1>_{B} \]

\[ |\varphi>_{AB} = \frac{1}{4} \sum_i |S^i_k>_{A} \otimes |S^i_k>_{B} \quad k = 1, 2, 3, 4, 5, 6, 7, 8, 9 \]

Let \( S_r \) be the set given to Alice.

Alice measures in the basis \( \{|S^i_r>\} \).

Let the state collapses to \( |S^i_r> \):

\[ v(S^i_r) = 1, \text{ for } i = j \]

\[ = 0, \text{ for } i \neq j \]

Bob is given the vector \( S^m_r \).

He measures in a basis having a vector \( |S^m_r> \).

If he collapses on \( |S^m_r> \), he assigns;

\[ v(S^m_r) = 1 \]

\[ = 0, \text{ otherwise.} \]

Due to correlation of the state;

\[ v_{Alice}(S^m_r) = v_{Bob}(S^m_r) \]
Magic square game

A $3 \times 3$ matrix

$$
\begin{bmatrix}
a_{11} & a_{12} & a_{13} \\
a_{21} & a_{22} & a_{23} \\
a_{31} & a_{32} & a_{33} \\
\end{bmatrix}
$$
with $a_{ij} = 0$ or $1$

For row:
- $a_{11} + a_{12} + a_{13} = \text{even}$
- $a_{21} + a_{22} + a_{23} = \text{even}$
- $a_{31} + a_{32} + a_{33} = \text{even}$

Such matrix does not exist

For column:
- $a_{11} + a_{21} + a_{31} = \text{odd}$
- $a_{12} + a_{22} + a_{32} = \text{odd}$
- $a_{13} + a_{23} + a_{33} = \text{odd}$

- The game -

Alice is given a row and Bob is given a column. They are asked to give the entries.

The sum of Alice’s entries should be even.

The sum of Bob’s entries should be odd.

Winning condition:
They should assign same value to the common element in each turn.
A deterministic classical strategy can not exist. A deterministic classical strategy would have to assign definite binary values to each nine entries of the magic square which is impossible.

Quantum winning strategy

\[
|\psi^-_{AB} = \frac{1}{\sqrt{2}} |01_{AB} - 10_{AB}\]

\[
|\psi^-_{CD} = \frac{1}{\sqrt{2}} |01_{CD} - 10_{CD}\]

\[
|\phi^-_{ACBD} = |\psi^-_{AB} \otimes |\psi^-_{CD}\]

Write the state in the AC:BD cut.

\[
|\phi^-_{AC:BD} = \frac{1}{2} [00_{AC} |11_{BD} + 01_{AC} |10_{BD} + 10_{AC} |01_{BD} + 11_{AC} |00_{BD}]
\]
Alice: Row Unitary operation

1
\[ U_1 = \begin{bmatrix}
  i & 0 & 0 & 1 \\
  0 & -i & 1 & 0 \\
  0 & i & 1 & 0 \\
  1 & 0 & 0 & i
\end{bmatrix} \]

2
\[ U_2 = \begin{bmatrix}
  i & 1 & 1 & i \\
  -i & 1 & -1 & i \\
  i & -1 & 1 & -i \\
  -i & 1 & 1 & -i
\end{bmatrix} \]

3
\[ U_3 = \begin{bmatrix}
  -1 & -1 & -1 & 1 \\
  1 & 1 & -1 & 1 \\
  1 & -1 & 1 & 1 \\
  1 & -1 & -1 & -1
\end{bmatrix} \]

Bob: Column Unitary operation

1
\[ V_1 = \begin{bmatrix}
  i & -i & 1 & 1 \\
  -i & -i & 1 & -1 \\
  1 & 1 & -i & i \\
  -i & i & 1 & 1
\end{bmatrix} \]

2
\[ V_2 = \begin{bmatrix}
  -1 & i & 1 & i \\
  1 & i & 1 & -i \\
  1 & -i & 1 & i \\
  -1 & -i & 1 & -i
\end{bmatrix} \]

3
\[ V_3 = \begin{bmatrix}
  1 & 0 & 0 & 1 \\
  0 & 1 & 0 & 1 \\
  0 & 0 & 1 & 0 \\
  0 & 0 & -1 & 0
\end{bmatrix} \]

After the unitary operation Alice and Bob measure their qubits in the basis \(|00>, |01>, |10>, |11>\).

If Alice collapses on \(|a_1 a_2 >_{AC}\)

she outputs \((a_1, a_2, a_1 \oplus a_2)\)

If Bob collapses on \(|b_1 b_2 >_{BD}\)

he outputs \((b_1, b_2, b_1 \oplus b_2 \oplus 1)^T\)
Quantum correlation reduces communication

\[ x = (x_1, x_2, x_2 \ldots \ldots x_n), x_i \in \{0, 1\} \]

Similarly for \( y \) and \( z \)

There is a constraint on the inputs:

\[ x_i + y_i + z_i = 1 \]

for all \( i \).

The task for Alice is to compute the function

\[ f(x, y, z) = x_1 \cdot y_1 \cdot z_1 + x_2 \cdot y_2 \cdot z_2 + \ldots + x_n \cdot y_n \cdot z_n \]

(Cleve & Buhrman, In Arxiv 1997)
In classical world, it has been shown that more than 2 bits of communication are necessary. 3 bits of communication is sufficient.

Let $n = 3$.

If $x_i \cdot y_i \cdot z_i = 1$, then none of them can be zero.

If $x_i \cdot y_i \cdot z_i = 0$, then two of them have to be zero. $(x_i + y_i + z_i = 1 \text{ for all } i.)$

$r_A, r_B, r_C$ be the no. of zeros for Alice's, Bob's and Charie's input respectively.

Total no. of zeros among all their inputs is even and let it be equal to $2k$. $r_A + r_B + r_C = 2k$

$k$ no. of terms in $x_1 \cdot y_1 \cdot z_1 + x_2 \cdot y_2 \cdot z_2 + \ldots + x_n \cdot y_n \cdot z_n$ are zero.

$$f(x, y, z) = (n - k) \text{mod} 2$$

To compute $k$, Alice has to learn $r_B$ and $r_C$.

Possible values of $r_B$ and $r_C$ are 0,1,2,3 which can be communicated by 2 bits 00, 01, 10, 11.

But one of them (say Charlie) can communicate just one bit (first bit) as Alice can determine $r_C$ as

$$r_A + r_B + r_C = \text{even}$$
Quantum protocol needs two bits of communication

They share $n$ copies of the following 3 qubits state.

$$|\psi >_{ABC}^k = \frac{1}{2} [ |001> + |010> + |001> - |111> | ] \quad k = 1, 2, ..., n$$

- If the $i$th bit $x_i = 1$, Alice measures in the $\{|0>, |1>\}$ basis and notes down the output $S_i^A$.
- If the $i$th bit $x_i = 0$, Alice first applies Hadamard transform on the respective qubit and then follows the same procedure.

Bob and Charlie do the same.

Alice computes $S_A = \sum S_i^A$

Bob computes $S_B = \sum S_i^B$ and communicate to Alice by 1 bit.

Charlie computes $S_C = \sum S_i^C$ and communicate to Alice by 1 bit.

Alice outputs $S_A + S_B + S_C$ as $f(x, y, z)$. 
The protocol works as follows;

First observe that \( S_i^A + S_i^B + S_i^C = x_i \cdot y_i \cdot z_i \) for all \( i \).

Possible values of \( x_i \ y_i \ z_i \) are \((100, 010, 001, 111)\)

**Case:** \( x_i \ y_i \ z_i = 111 \)

then all possible measurement results \((S_i^A, S_i^B, S_i^C)\) satisfy

\[
S_i^A + S_i^B + S_i^C = x_i \cdot y_i \cdot z_i
\]

**Case:** \( x_i \ y_i \ z_i = 001 \)

\[
H \otimes H \otimes I \ |\psi\rangle_{ABC} = \frac{1}{2} [ |011\rangle + |101\rangle + |000\rangle - |110\rangle ]
\]

In this case also measurements results \((S_i^A, S_i^B, S_i^C)\) satisfy

\[
S_i^A + S_i^B + S_i^C = x_i \cdot y_i \cdot z_i
\]

This thing works in other two cases \((x_i \ y_i \ z_i = 100, 010)\) due to symmetry of the entangled state.

\[
S_A + S_B + S_C = \sum S_i^A + \sum S_i^B + \sum S_i^C = \sum (S_i^A + S_i^B + S_i^C) = \sum x_i \cdot y_i \cdot z_i = f(x, y, z).
\]