Quantum entanglement can be simulated without communication

Nicolas J. Cerf

Centre for Quantum Information and Communication
Université Libre de Bruxelles

(joint work with Nicolas Gisin, Serge Massar, and Sandu Popescu)

Simulation of E.P.R. experiment

Input: $\vec{a}$

Alice

| $\Psi^-$ >

Output: $A \in \{-1, +1\}$

$P(A, B) = \frac{(1 - AB \vec{a} \cdot \vec{b})}{4}$

$P(A) = 1/2 \ \forall \vec{b}$

CAUSALITY

Output: $B \in \{-1, +1\}$

$E(AB) = -\vec{a} \cdot \vec{b}$

$E(AB) = -\vec{a} \cdot \vec{b}$

$P(B) = 1/2 \ \forall \vec{a}$
Local Hidden Variable (LHV) Model

Shared randomness: $\lambda$

Input: $\vec{a}$

Output: $A(\vec{a}, \lambda) \in \{-1, +1\}$

Output: $B(\vec{b}, \lambda) \in \{-1, +1\}$

$E(AB|\vec{a}, \vec{b}) = \int_{\lambda \in \Lambda} p(\lambda) \ A(\vec{a}, \lambda) \ B(\vec{b}, \lambda)$

$\equiv -\vec{a} \cdot \vec{b}$

BUT...
Bell's Theorem:

No Local Hidden Variable model can simulate the quantum correlations of the EPR experiment

Indeed, any LHV model must satisfy the CHSH inequality:

$$|C(\tilde{a}_0, \tilde{a}_1, \tilde{b}_0, \tilde{b}_1)| \leq 2 \quad \forall \tilde{a}_0, \tilde{a}_1, \tilde{b}_0, \tilde{b}_1 \in S_2$$

with

$$C(\tilde{a}_0, \tilde{a}_1, \tilde{b}_0, \tilde{b}_1) = E(AB|\tilde{a}_0, \tilde{b}_0) + E(AB|\tilde{a}_0, \tilde{b}_1) + E(AB|\tilde{a}_1, \tilde{b}_0) - E(AB|\tilde{a}_1, \tilde{b}_1)$$

In quantum mechanics:

$$\exists \tilde{a}_0, \tilde{a}_1, \tilde{b}_0, \tilde{b}_1 \in S_2 \quad such \quad that \quad C(\tilde{a}_0, \tilde{a}_1, \tilde{b}_0, \tilde{b}_1) = 2\sqrt{2}$$

So we need extra resources, in addition to those allowed by any Local Hidden Variable model.

The amount of extra resources that is needed gives us some measure of the non-locality of QM

(Maudlin 92; Brassard, Cleve, Tapp 99)
Additional resources

**Classical communication**: in number of bits (on average or in worst case)

- Allows for superluminal communication

**Freedom to post-select (detection loophole)**: the parties are given the possibility to output “no result”, simulating an imperfect detector

- Does not allow for superluminal communication but probabilistic

**Non-Local Box**: in number of uses

- Remains causal: strictly weaker resource than 1 bit of communication

\[
a \oplus b = x \land y
\]

\[
\begin{align*}
\text{Popescu and Rohrlich 94} \\
\text{van Dam 00} \\
x, y, a, b \in \{0,1\}
\end{align*}
\]
### Outline of the known protocols

<table>
<thead>
<tr>
<th>Resource</th>
<th>Amount</th>
<th>( \vec{a}, \vec{b} )</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>1.17 bit on Average</td>
<td>Equator</td>
<td>Maudlin 92</td>
</tr>
<tr>
<td>Communication</td>
<td>8 bits in Worst Case</td>
<td>Sphere</td>
<td>Brassard, Cleve, Tapp 99</td>
</tr>
<tr>
<td>Communication</td>
<td>1.48 bit on Average</td>
<td>Equator</td>
<td>Steiner 99</td>
</tr>
<tr>
<td>Post-Selection</td>
<td>( P(A_{output}) = P(B_{output}) = \frac{2}{3} )</td>
<td>Sphere</td>
<td>Gisin, Gisin 99</td>
</tr>
<tr>
<td>Communication</td>
<td>1.19 bit on Average</td>
<td>Sphere</td>
<td>NJC, Gisin, Massar 00</td>
</tr>
<tr>
<td>Communication</td>
<td>1 bit in Worst Case</td>
<td>Sphere</td>
<td>Toner, Bacon 03</td>
</tr>
<tr>
<td>Non-Local Box</td>
<td>1 use in Worst Case but no communication</td>
<td>Sphere</td>
<td>(this talk)</td>
</tr>
</tbody>
</table>
Non-Local Box

- Maximally non-local: maximally violates CHSH inequality $C = 4$
- Causal

\[ C(\vec{a}_0, \vec{a}_1, \vec{b}_0, \vec{b}_1) = E(AB|\vec{a}_0, \vec{b}_0) + E(AB|\vec{a}_0, \vec{b}_1) + E(AB|\vec{a}_1, \vec{b}_0) - E(AB|\vec{a}_1, \vec{b}_1) \]

- $x = 0$, $y = 0$
- $x = 1$, $y = 1$

$a$ and $b$ are anticorrelated when $x = 1$ and $y = 1$; otherwise they are correlated.

\[ x \land y = a \oplus b \]

- $A = 1 - 2a$
- $B = 1 - 2b$

\{0, 1\} \rightarrow \{+1, -1\}

\[ p(a = 0|x, y) = p(a = 0|x) = \frac{1}{2} \]

\[ p(b = 0|x, y) = p(b = 0|y) = \frac{1}{2} \]
Is it a **sufficient** resource to simulate any VN measurement on an EPR state?

- It is sufficiently nonlocal (more than QM !)
- It is causal (just like QM !) : does not “spoil” resources
- It admits binary inputs, while there are infinitely many possible VN measurements

**HOW DOES IT WORK?**  Next slide

**WHY DOES IT WORK?**  Next talk
\[
\begin{align*}
\lambda_1, \lambda_2 & \\
x &= \text{sgn}(\vec{a} \cdot \lambda_1) + \text{sgn}(\vec{a} \cdot \lambda_2) \\
y &= \text{sgn}(\vec{b} \cdot \lambda_+) + \text{sgn}(\vec{b} \cdot \lambda_-) \\
x \wedge y &= a \oplus b \\
\end{align*}
\]

with 
\[
\text{sgn}(t) = \begin{cases} 
0 & t > 0 \\
1 & t \leq 0 
\end{cases}
\]

\[
\begin{align*}
A(\vec{a}, \lambda_1, \lambda_2) &= 1 - 2[a + \text{sgn}(\vec{a} \cdot \lambda_1)] \\
B(\vec{b}, \lambda_1, \lambda_2) &= -1 + 2[b + \text{sgn}(\vec{b} \cdot \lambda_+)] \\
\end{align*}
\]

\textbf{RESULT:} 
\[
E(AB) = -\vec{a} \cdot \vec{b}
\]
Monogamy: Non-Local Box cannot be shared

$\forall x \land y = a \oplus b$

$\forall x \land z = a \oplus c$

$x \land (y \oplus z) = (a \oplus b) \oplus (a \oplus c) = b \oplus c$

$y = 0 \land z = 1 \rightarrow b \oplus c = x$  \textbf{Non causal!}

- Exploit monogamy to do QKD (talk by N. Gisin, A. Acin, L. Masanes)
- Characterize monogamy in general (talk by B. Toner)
Conclusion & Perspectives

- Extend to non-maximally entangled states
  
  1 use of Non-Local Box is not sufficient
  N. Brunner, N. Gisin, V. Scarani, 05

  Non-maximally entangled state is "more non-local"

- Extend to POVM measurements (related)

- Extend to multipartite states and/or higher dimensions

**Non-Local Box** appears to be useful conceptual tool
(non-locality characterization, secret key distribution, communication complexity, bit commitment,...)