Quantum Entanglement, Quantum Cryptography, Beyond Quantum Mechanics, and Why Quantum Mechanics

Brad Christensen

Advisor: Paul G. Kwiat

Physics 403 talk: December 2, 2014
Entanglement is a feature of compound quantum systems

- States that can be written \( |\Psi\rangle_{AB} = |\varphi^1\rangle_A |\varphi^2\rangle_B \) are separable
- States that cannot be written this way are entangled

Example: the Bell states are inseparable

\[
|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|0\rangle |0\rangle \pm |1\rangle |1\rangle)
\]

\[
|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} (|0\rangle |1\rangle \pm |1\rangle |0\rangle)
\]

\[
|\Phi'\rangle = (\alpha |0\rangle + \beta |1\rangle) (\gamma |0\rangle + \delta |1\rangle)
= \alpha \gamma |0\rangle |0\rangle + \alpha \delta |0\rangle |1\rangle + \beta \gamma |1\rangle |0\rangle + \beta \delta |1\rangle |1\rangle
\]

No solution!

Measurement outcomes are random and correlated
Classical “entanglement”? 

- Classical things can be random and correlated, too…

- … but not entangled!

How is this different from an entangled state?

- Each marble has a defined color from the beginning (local hidden variable)
- The processes are distinguishable in principle
- There is no conjugate measurement basis

Entangled systems give random and correlated measurement outcomes in every measurement basis!
Downconversion

(a) Pump
Nonlinear Crystal

(b) Momentum conservation

(c) Energy conservation

\[ \omega_p, \omega_i, \omega_s \]

\[ K_i, K_s, K_p \]
Polarization Entanglement

\[ |\psi_i\rangle \langle \psi_i| = |V\rangle \langle V| + |H\rangle \langle H| \]

\( \text{“Fast”} \)

\[ |H\rangle + R e^{i\phi} |V\rangle \]

\( K_i \)

\( K_p \)

\( K_s \)

\( \text{“Slow”} \)

\[ |\psi_s\rangle \langle \psi_s| = |V\rangle \langle V| + |H\rangle \langle H| \]

\( \text{“Slow”} \)

\[ |\psi_{\text{system}}\rangle = |VV\rangle + R e^{i\phi} |HH\rangle \]
$|HH\rangle + |VV\rangle \rightarrow |H\rangle = |D\rangle + |A\rangle$

$|V\rangle = |D\rangle - |A\rangle \rightarrow |DD\rangle + |AA\rangle$
Hidden-Variables

\[ |DD\rangle + |AA\rangle \\
|VV\rangle + |HH\rangle \]

Requires speeds > c

“If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.”

If measured in the Θ basis, then the outcome is determined by \( f(\Theta) = \{0,1\} \)

Problem:

Device independent QRNG

Very hard to do (75% efficiency)! 8700 bits/3 hours

Not ideal for every system, can we do something different?

Assume control of the source: >1,000,000,000 bits/s
Classical Cryptography

One-Time Pad

Alice uses a one-time pad that she shares with Bob to encode a message.

Bob uses his identical one-time pad to decode Alice’s string.

Without access to the completely random key, it is impossible for Eve to decode the string.

Y 0 1 1 1 1 0 0 1
+ 1 0 0 0 1 1 1 0
= 1 1 1 1 0 1 1 1

- 1 0 0 0 1 1 1 0
= 0 1 1 1 1 0 0 1

Message + Secret key = Completely random

Not random + Completely random = Completely random

Message + Secret key - Secret Key = Message

Without access to the completely random key, it is impossible for Eve to decode the string.
Alice uses a one-time pad that she shares with Bob to encode a message.

Bob uses his identical one-time pad to decode Alice’s string.

Without access to the completely random key, it is impossible for Eve to decode the string.

\[
\begin{align*}
Y & \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \\
+ & \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \\
= & \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \\
\end{align*}
\]

\[
\begin{align*}
Y & \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \\
- & \quad 1 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \\
= & \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \\
\end{align*}
\]

Quantum Key Distribution

Alice's Basis Choice: H/V H/V
Alice's Measurements: H V

Bob's Basis Choice: D/A H/V
Bob's Measurements: D V

Eve's Basis Choice: D/A D/A D/A H/V D/A D/A D/A H/V
Eve's Measurements: D A D H A D D V

HWP + PBS

\[ |DD\rangle + |AA\rangle \]
\[ |VV\rangle + |HH\rangle \]

Quantifying a “nonlocal resource”

• Consider the CHSH Bell inequality:
  \[ S = E(a,b) - E(a,b') + E(a',b) + E(a',b') \]
  – Classically, \( S \leq 2 \)
  – Quantum mechanically, \( S \leq 2\sqrt{2} \)
  – Algebraically, \( S \leq 4 \)

• What sort of theory could achieve the algebraic bound?
  – A theory only limited by causality!
Quantifying a “nonlocal resource”

• For QM, $S = 2\sqrt{2}$ by using maximally entangled particles

$S = 4$ is achieved using “PR Boxes”

• $S = 4$ is achieved using “PR Boxes”

$S = E(0,0) - E(1,1) + E(1,0) + E(0,1) = 4$

PR Box as a nonlocal resource

• A PR box could simulate the QM maximum CHSH value

• If a PR box is used, it is completely nonlocal and cannot be predicted

• If a local model is used, it is a classical result and can be predicted perfectly

• Beyond-QM theories could predict the outcomes of a CHSH Bell test with a $41%/2 + 59% = 79\%$ probability

• Can we design a Bell inequality where nature would need to use a PR box 100% of the time?
Chained Bell Inequality

\[ I_N = \sum_{a,b} P(a = b|0, 2N - 1) + \sum_{|x-y|=1} (1 - \sum_{a,b} P(a = b|x, y)) \]

\[ I_{\infty} = 0 \text{ (i.e., the maximal nonlocal value)} \]

\[ I_2 \text{ is the CHSH Bell inequality} \]

\[ I_{18} = 0.126 \pm 0.001 \]

\[ I_{45} = 0.180 \pm 0.001 \]

Requires 360 measurements!

Limiting the Predictive Power

\[ \delta_N = \frac{\sum_{a,b} P(a = b|0, 2N - 1) + \sum|_{x-y}=1 (1 - \sum_{a,b} P(a = b|x, y))}{2} \]

Bias term = 0.007

(Alice sees 0.5035|HH><HH| + 4.965|VV><VV|)

\[ I_N = 0.126 \rightarrow \text{Predictive power} = 0.126 + 0.874/2 + 0.007 \]

Any further theory could only predict the results with 57% probability

\[ \delta_{18}=0.070\pm0.0005 \]
\[ \delta_{45}=0.098\pm0.001 \]
Quantum postulates aren’t clean

Postulates of quantum mechanics

• Each physical system is associated with a separable complex Hilbert Space $H$ with inner product. Rays (one-dimensional subspaces) in $H$ are associated with states of the system.
• The Hilbert space of a composite system is the Hilbert space tensor product of the state spaces associated with the component systems.
• Physical symmetries act on the Hilbert space of quantum states unitarily or anti-unitarily due to Wigner’s theorem.
• Physical observables are represented by Hermitian matrices on $H$. The expectation value of the observable $A$ for the system in state represented by the unit vector $|\psi\rangle \in H$ is $\langle \psi | A | \psi \rangle$.

Postulates of special relativity

• The laws of physics are the same in all inertial frames of reference.
• The speed of light in free space has the same value $c$ in all inertial frames of reference.
Can we re-derive quantum mechanics?

- **Causality**
  - A1 to Q1
  - A2 to Q2
  - 1 bit
  - Learns
  - A2 or A1

- **????????**

- **Currently we can only do a maximum bound**
  - Quantum Mechanics has **Information causality**
    - Answering multiple one bit questions with one bit (but only one question can be found the answer to).
  - Quantum Mechanics has **Communication redundancy**
    - One bit answers only require one bit input