Fun and games with quantum entanglement

Stephanie Wehner
What to expect

- Quantum Bits
  - What makes them different?
- Entanglement
  - Action at a distance…
  - Why is this so special?
  - Playing games with entanglement
- Applications
  - Why bother?
Quantum Bits

Classical Bits: 0 or 1

Quantum Bits: 0 or 1 at the same time!

\[ \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \]
Quantum Bits

Classical Bits: 0 or 1

Quantum Bits: 0 or 1 at the same time! Cannot be copied.

\[
\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle
\]
Measurements

\[
\frac{1}{\sqrt{2}} \quad + \quad \frac{1}{\sqrt{2}}
\]
Measurements

\[ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \]

State collapses
Different basis...

Basis 1: Vertical and Horizontal

\[ 0 \quad 1 \]

Basis 2: Diagonal

\[ 0 \quad 1 \]

\[
\begin{align*}
\Rightarrow & \quad = \frac{1}{\sqrt{2}} \quad + \quad \frac{1}{\sqrt{2}}
\end{align*}
\]
Measurement in the same basis

0  \downarrow  \rightarrow \uparrow \rightarrow 0

1  \leftarrow \rightarrow \rightarrow \leftarrow 1
Measurement in the same basis
Measurement in the same basis does not change the state.
Measurement in a different basis....

\[ 0 = \frac{1}{\sqrt{2}} \uparrow + \frac{1}{\sqrt{2}} \downarrow \]

\[
\begin{array}{c}
0 \\
\uparrow \\
+ \\
\downarrow \\
50\% \\
\hline
50\% \\
\end{array}
\]

\[
\begin{array}{c}
0 \\
\hline
1 \\
\end{array}
\]
Measurement in a different basis....

\[ l = \frac{1}{\sqrt{2}} \]

50% 50%

0 1
Measurement in a different basis....

\[ l = \frac{1}{\sqrt{2}} \quad \text{and} \quad -\frac{1}{\sqrt{2}} \]

\[ \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \]

\[ 50\% \quad 50\% \]

\[ 0 \quad 1 \]
Measurement in a different basis....

\[ 0 = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \]
Two funny quantum effects

- Interference (see WTH ‘05)
- Entanglement
Entanglement

\[ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \]
Entanglement

\[ \frac{1}{\sqrt{2}} \uparrow \uparrow \downarrow \downarrow + \frac{1}{\sqrt{2}} \leftrightarrow \leftrightarrow \]
Entanglement

\[ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \]
Entanglement

\[ \frac{1}{\sqrt{2}} \uparrow \uparrow + \frac{1}{\sqrt{2}} \downarrow \downarrow \]

50%
Entanglement

\[
\frac{1}{\sqrt{2}} \uparrow \frac{1}{\sqrt{2}} \downarrow + \frac{1}{\sqrt{2}} \uparrow \frac{1}{\sqrt{2}} \downarrow
\]
Perfect correlations

\[
\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}
\]

50%

Always!!
Perfect correlations

\[ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = 50\% \]

Always!!
Perfect correlations

Yet, cannot send information using only entanglement itself.

Always!!
Let’s be more sceptical…
Perhaps there’s communication?

- Cannot communicate faster than light
- Measure immediately, no chance to communicate
Let’s be more sceptical…
Perhaps there’s communication?

- Cannot communicate faster than light
- Measure immediately, no chance to communicate
Let’s be more sceptical… Perhaps there’s communication?

- Cannot communicate faster than light
- Measure immediately, no chance to communicate
Let’s be more sceptical…

Works even without communication

• Cannot communicate faster than light
• Measure immediately, no chance to communicate
Let’s be more sceptical…
What does that mean, “there’s a 50% chance of obtaining an outcome?”

Earth

\[
\frac{1}{\sqrt{2}} \uparrow \downarrow + \frac{1}{\sqrt{2}} \leftrightarrow \leftrightarrow
\]

Mars
Let’s be more sceptical…
What does that mean, “there’s a 50% chance of obtaining an outcome?”

Earth

Mars
Let’s be more sceptical…

Earth

\[ \frac{1}{\sqrt{2}} \uparrow \uparrow + \frac{1}{\sqrt{2}} \]

Always!!

Mars
Let’s be more sceptical…
Let’s be more sceptical...

If \( \text{+} \) then
Output \( \leftrightarrow \)
If \( \text{-} \) then
Output

\( ........ \)

Earth

Not a big deal then.... But how can we be sure this is how it works?

Mars
Let’s play a game of Q & A

- **Measurement settings are the questions:**
  
  ![Measurement symbols](image)

- **Outcomes are the answers:**
  
  ![Outcome symbols](image)

- **Instructions are the strategies of a player:**
  
  ![Instruction symbols](image)
Let’s play a game of Q & A

- Some rules:
  - We tell the players clearly what game we wish to play.
  - Before we start the game, players can communicate and decide on a strategy. This determines their “cheat sheet”.
  - Once the game has started, they are no longer allowed to communicate.
A three person game

• Questions: X, Y, and Z. Always X + Y + Z mod 2 = 0.

• GHZ game (Greenberger, Horne, Zeilinger)
A three person game

• Questions: X Y and Z. Always X + Y + Z mod 2 = 0.
• Players win iff X or Y or Z = A + B + C mod 2

• GHZ game (Greenberger, Horne, Zeilinger)
A three person game

- Questions: X Y and Z. Always $X + Y + Z \mod 2 = 0$.
- Players win iff $X$ or $Y$ or $Z = A + B + C \mod 2$

- If communication is possible, players can easily win.

- GHZ game (Greenberger, Horne, Zeilinger)
A three person game

• Questions: X Y and Z. Always X + Y + Z mod 2 = 0.
• Players win iff X or Y or Z = A + B + C mod 2

• If communication is possible, players can easily win.
• Put players in far away places again, so they have “no time to communicate before we expect answers.

• GHZ game (Greenberger, Horne, Zeilinger)
A three person game

- Questions: X Y and Z. Always $X + Y + Z \mod 2 = 0$.
- Players win iff $X$ or $Y$ or $Z = A + B + C \mod 2$

<table>
<thead>
<tr>
<th>X Y Z</th>
<th>$A + B + C \mod 2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0: 000,011,101,110</td>
</tr>
<tr>
<td>011</td>
<td>1: 001,010,100,111</td>
</tr>
<tr>
<td>101</td>
<td>1:</td>
</tr>
<tr>
<td>110</td>
<td>1:</td>
</tr>
</tbody>
</table>

- GHZ game (Greenberger, Horne, Zeilinger)
A three person game

Questions: X Y and Z. Always X + Y + Z mod 2 = 0.
Players win iff X or Y or Z = A + B + C mod 2

\[ A = X! \]
\[ B = \text{not } Y! \]
\[ C = 1! \]

<table>
<thead>
<tr>
<th>X Y Z</th>
<th>A + B + C mod 2</th>
<th>One strategy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0: 000,011,101,110</td>
<td>011 - Win!</td>
</tr>
<tr>
<td>011</td>
<td>1: 001,010,100,111</td>
<td>001 - Win!</td>
</tr>
<tr>
<td>101</td>
<td>1:</td>
<td>111 - Win!</td>
</tr>
<tr>
<td>110</td>
<td>1:</td>
<td>101 - Loose...</td>
</tr>
</tbody>
</table>

GHZ game (Greenberger, Horne, Zeilinger)
Suppose qubits were like boxes

Questions: X Y and Z. Always X + Y + Z mod 2 = 0.
Players win iff X or Y or Z = A + B + C mod 2

It’s impossible to win all the time with a classical strategy:

\[
\begin{align*}
A(0) + B(0) + C(0) &= 0 \\
A(0) + B(1) + C(1) &= 1 \\
A(1) + B(0) + C(1) &= 1 \\
A(1) + B(1) + C(0) &= 1
\end{align*}
\]

sum all four mod 2: 0 = 1!

GHZ game (Greenberger, Horne, Zeilinger)
Quantumly, things are a little different….

• Questions: X Y and Z. Always $X + Y + Z \mod 2 = 0$.
• Players win iff $X$ or $Y$ or $Z = A + B + C \mod 2$

• But with quantum entanglement, the players can win all the time!
  • Start out with entangled state
  • Just measure with $+$ for 0 and $\times$ for 1
  • Take measurement outcome as answer.

• GHZ game (Greenberger, Horne, Zeilinger)
But if quantum entanglement allows the player to win always

- Qubits are not like boxes with a predetermined instruction sheet (aka hidden variables).
  - Communication was not possible.
  - Neither does entanglement allow us to transfer information by itself.
  - Yet, the players can always win...
Other “games”

- Bell/CHSH ‘game’
- Mermin’s Magic Square (described in an easy way by Aravind)
- ......
Great, so why bother?

- Quantum entanglement can make things possible which are classically only possible with communication. (such as playing the GHZ game)
- Plays an important role in quantum algorithms:
  - Speedup such as in factoring depends crucially on entanglement! (Linden, Josza)
- Quantum Teleportation
- Plays an important role in quantum cryptography.
Quantum Teleportation

- Send an arbitrary quantum bit using
  - One EPR pair
  - 2 bits of classical communication
Quantum Teleportation

- Send an arbitrary quantum bit using
  - One EPR pair
  - 2 bits of classical communication
Quantum Teleportation

- Send an arbitrary quantum bit using
  - One EPR pair
  - 2 bits of classical communication
Applications to cryptography

● Negative: If the security of a protocol depends on the fact that certain parties cannot communicate, the protocol may be compromised if the parties can share entanglement (e.g. in interactive proof systems).

● Positive: Quantum key exchange
  ● An entanglement view on quantum key exchange
The Problem
The Problem
The Problem
Secure Communication

Goal: Hide the message contents from eavesdroppers!
Secure Communication

Goal: Hide the message contents from eavesdroppers!
Secret Key Cryptography

Only Alice and Bob know the key.
Secret Key Cryptography

Problem: Need to communicate the key!
Secret Key Cryptography

Problem: Need to communicate the key!
Secret Key Cryptography

Problem: Need to communicate the key!
Examples:
Secret Key Cryptography

- Algorithms: DES, IDEA, AES (Rijndael),…
  - Advantage: Short keys
- One-time pad (Vernam cipher)
  - Disadvantage: Key as a long as the message itself
  - This is the only system which is secure without imposing any restrictions on the eavesdropper
One time pad

\[ k_i \]

\[ m_i \]

\[ \text{xor} \]

\[ k_i \]

\[ m_i \]
One time pad

Message: 0 1 0 0 1 1 0 0
Key: 0 0 1 0 1 0 0 1
One time pad

Message: 0 1 0 0 1 1 0 0

Key: xor 0 0 1 0 1 0 0 1

Encryption: xor 0 1 1 0 0 1 0 1
One time pad

Message: 0 1 0 0 1 1 0 0
Key: xor 0 0 1 0 1 0 0 1 xor
Encryption: xor 0 1 1 0 0 1 0 1 xor
So…. 

- **Secret Key Cryptography**
  - Needs a secure channel to distribute the key
  - If the key is shorter than the message, security is based on non-proven algorithms (DES, …)

- **Public Key Cryptography**
  - Security based on non-proven assumptions (e.g. factoring is hard)
  - Can be broken with a quantum computer (also retroactively!)

Want: Perfect security from a one time pad, without the need for a secure channel…
• Suppose Alice and Bob shared an EPR pair....
• Suppose Alice and Bob shared an EPR pair....
• Then they could measure to obtain a random bit, of which Eve knows absolutely nothing.
• Use this bit as a key.
• Suppose Alice and Bob shared an EPR pair....
• Then they could measure to obtain a random bit, of which Eve knows absolutely nothing.
• Use this bit as a key.

• But how to get such an EPR pair without Eve interfering ??
Let’s try...

- Alice creates the entire EPR pair, and sends one half to Bob.
Let’s try…

- Alice creates the entire EPR pair, and sends one half to Bob.
Let’s try...

- Alice creates the entire EPR pair, and sends one half to Bob.
- But how can they be sure Eve didn’t interfere?
  - Perhaps Eve captured Alice’s transmission?
Let’s try...

- Alice creates the entire EPR pair, and sends one half to Bob.
- But how can they be sure Eve didn’t interfere?
  - Perhaps Eve captured Alice’s transmission?
  - Perhaps Eve is now entangled with both Alice and Bob herself?
Alice and Bob play a game..

- But how can they be sure Eve didn’t interfere?
  - Perhaps Eve is now entangled with both Alice and Bob herself?
  - Alice and Bob play a two person game, similar to the GHZ game using a random subset of possible EPR pairs.
  - They check all runs of the game: Eve’s presence means they can play it ‘less well’: the win less rounds than they would expect.
  - If they detect Eve’s presence, they abort. Otherwise, they measure.
Summary

- Quantum Computing differs dramatically from classical computing.
- Entanglement is fundamentally different from classical correlations.
- Entanglement plays a central role in quantum computing and cryptography.
- Still many things remain open..