On the power of nonlocal boxes

or how nonlocality and entanglement are fundamentally different resources

Anne Broadbent
joint work with André Méthot
quant-ph/0504136
to appear in Theoretical Computer Science
broadbea@iro.umontreal.ca
Nonlocality
Nonlocality

Consider two or more participants that are physically separated and unable to communicate.

- The participants are individually given a challenge. In response, they must each produce an output.
Nonlocality

Consider two or more participants that are physically separated and unable to communicate.

- The participants are individually given a challenge. In response, they must each produce an output.
- We say that the participant’s outputs exhibit *nonlocality* if there is no classical theory that can explain the correlations of their outputs. Nonlocality can be achieved, for example, if the participants share entanglement.
Two examples of nonlocal tasks
Consider a *game*, in which two or more players play as a team, against a *referee*. 
Pseudo-telepathy

- Consider a *game*, in which two or more players play as a team, against a *referee*.
- The players are physically separated and unable to communicate.
Pseudo-telepathy

- Consider a game, in which two or more players play as a team, against a referee.
- The players are physically separated and unable to communicate.
- They each receive an input ($x \in X$ for Alice, $y \in Y$ for Bob).
Pseudo-telepathy

- Consider a *game*, in which two or more players play as a team, against a *referee*.
- The players are physically separated and unable to communicate.
- They each receive an input ($x \in X$ for Alice, $y \in Y$ for Bob).
- They must each produce output ($a \in A$ for Alice, $b \in B$ for Bob) such that a given *winning condition* (a relation $R$ on $X \times Y \times A \times B$) is satisfied. If $R$ is satisfied, we say that the players *win* the game.
Factoid

- According to the Wikipedia, “Alice” and “Bob” were invented by Ron Rivest for the 1978 Communications of the ACM article presenting the RSA cryptosystem.
Factoid

- According to the Wikipedia, “Alice” and “Bob” were invented by Ron Rivest for the 1978 Communications of the ACM article presenting the RSA cryptosystem.

- Rivest denies that these names have any relation with the 1969 movie “Bob & Carol & Ted & Alice” as some suggest.
We say that the players have a *winning strategy* if they can win on all possible inputs. A winning strategy can be *classical* (players share only classical resources), *quantum* (players share entanglement), or *nonlocal* (players share nonlocal boxes, more on this later).
Pseudo-telepathy

- We say that the players have a winning strategy if they can win on all possible inputs. A winning strategy can be classical (players share only classical resources), quantum (players share entanglement), or nonlocal (players share nonlocal boxes, more on this later).

- A game exhibits pseudo-telepathy if it admits a quantum winning strategy and does not admit a classical winning strategy.
Pseudo-telepathy

- **Theorem**: No pseudo-telepathy game exists where the quantum strategy makes use of a single pair of entangled qubits. (Brassard, Méthot, Tapp, 2005)
Entanglement simulation

Entanglement simulation is the exact reproduction of the correlations of quantum entanglement by participants who do not have access to quantum entanglement. An additional resource, such as communication, is usually required.
Simulation and pseudo-telepathy

A protocol *simulates* the correlations of a pseudo-telepathy game if, in addition to yielding a winning strategy, the outputs are indistinguishable from the outputs of the quantum winning strategy.
Simulation and pseudo-telepathy

- A protocol *simulates* the correlations of a pseudo-telepathy game if, in addition to yielding a winning strategy, the outputs are indistinguishable from the outputs of the quantum winning strategy.

- Simulating the entangled state used in the quantum winning strategy cannot be any easier than simulating the correlations of a given pseudo-telepathy game.
Simulation and pseudo-telepathy

- A protocol *simulates* the correlations of a pseudo-telepathy game if, in addition to yielding a winning strategy, the outputs are indistinguishable from the outputs of the quantum winning strategy.

- Simulating the entangled state used in the quantum winning strategy cannot be any easier than simulating the correlations of a given pseudo-telepathy game.

- This gives us a lower bound on the amount of resources required for entanglement simulation.
The nonlocal box
The nonlocal box (NLB)

A virtual device shared between two participants, Alice and Bob. When Alice inputs a bit $x$ and Bob inputs a bit $y$, Alice receives a bit $a$ and Bob a bit $b$ such that:

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

Furthermore, $a$ and $b$ are uniformly distributed among all solutions.
The nonlocal box (NLB)
Properties of the Nonlocal Box

- Cannot be used for signaling
Properties of the Nonlocal Box

- Cannot be used for signaling
  - $a$ and $b$ are uniformly distributed
Properties of the Nonlocal Box

- Cannot be used for signaling
  - $a$ and $b$ are uniformly distributed

- Cannot be reproduced by classical participants
Properties of the Nonlocal Box

- Cannot be used for signaling
  - $a$ and $b$ are uniformly distributed

- Cannot be reproduced by classical participants
  - Alice and Bob can’t communicate
Properties of the Nonlocal Box

- Cannot be used for signaling
  - $a$ and $b$ are uniformly distributed

- Cannot be reproduced by classical participants
  - Alice and Bob can’t communicate

- Cannot be reproduced by quantum participants
Properties of the Nonlocal Box

- Cannot be used for signaling
  - \(a\) and \(b\) are uniformly distributed

- Cannot be reproduced by classical participants
  - Alice and Bob can’t communicate

- Cannot be reproduced by quantum participants
  - Result due to Tsirelson(1980)
Properties of the Nonlocal Box

- The NLB was defined by Popescu and Rohrlich (1994).
Properties of the Nonlocal Box

- The NLB was defined by Popescu and Rohrlich (1994).

- A single use of a NLB is sufficient for the simulation of a maximally-entangled 2-qubit state, for example,

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

(Cerf, Gisin, Massar, Popescu 2004).
Measures of nonlocality

How can we measure the nonlocalness of a specific task?
Measures of nonlocality

How can we measure the nonlocalness of a specific task?
- Dimension of shared entangled state.
Measures of nonlocality

- How can we measure the nonlocalness of a specific task?
  - Dimension of shared entangled state.
  - Ratio of the best classical and quantum success probabilities.
Measures of nonlocality

- How can we measure the nonlocalness of a specific task?
  - Dimension of shared entangled state.
  - Ratio of the best classical and quantum success probabilities.
  - Minimum detector efficiency rate required in order to circumvent the detection loophole.
Measures of nonlocality

- How can we measure the *nonlocalness* of a specific task?
  - Dimension of shared entangled state.
  - Ratio of the best classical and quantum success probabilities.
  - Minimum detector efficiency rate required in order to circumvent the detection loophole.
  - Number of bits of communication required in order for classical players to succeed.
Measures of nonlocality

How can we measure the nonlocalness of a specific task?
- Dimension of shared entangled state.
- Ratio of the best classical and quantum success probabilities.
- Minimum detector efficiency rate required in order to circumvent the detection loophole.
- Number of bits of communication required in order for classical players to succeed.
- *Number of NLB uses required in order for classical players to succeed.*
Non-local Winning Strategies for Pseudo-Telepathy Games
The Magic Square Game
A *magic square* is a $3 \times 3$ matrix with entries in $\{0, 1\}$ such that the sum of each row is even and the sum of each column is odd.
A magic square is a $3 \times 3$ matrix with entries in $\{0, 1\}$ such that the sum of each row is even and the sum of each column is odd.

Can a magic square exist?

<table>
<thead>
<tr>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>
A magic square is a $3 \times 3$ matrix with entries in $\{0, 1\}$ such that the sum of each row is even and the sum of each column is odd.

Can a magic square exist?

A simple parity argument shows that no magic square exists.
The Game

- Alice’s input is row $x \in \{1, 2, 3\}$.
- Bob’s input is column $y \in \{1, 2, 3\}$.
The Game

- Alice’s input is \( row \ x \in \{1, 2, 3\} \).
  Bob’s input is \( column \ y \in \{1, 2, 3\} \).

- Alice outputs \( a \), corresponding to row \( x \) of a magic square.
  Bob outputs \( b \), corresponding to column \( y \) of a magic square.
The Game

- Alice’s input is *row* $x \in \{1, 2, 3\}$. Bob’s input is *column* $y \in \{1, 2, 3\}$.
- Alice outputs $a$, corresponding to row $x$ of a magic square. Bob outputs $b$, corresponding to column $y$ of a magic square.
- The intersection of Alice and Bob’s answers must agree.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Properties

- No classical winning strategy
Properties

- No classical winning strategy
- such a strategy corresponds to a magic square
Properties

- No classical winning strategy
  - such a strategy corresponds to a magic square
- No quantum winning strategy using a 2-qubit entangled state
Properties

- No classical winning strategy
  - such a strategy corresponds to a magic square
- no quantum winning strategy using a 2-qubit entangled state
  - no such pseudo-telepathy game exists
Properties

- No classical winning strategy
  - such a strategy corresponds to a magic square
- No quantum winning strategy using a 2-qubit entangled state
  - no such pseudo-telepathy game exists
- There exists a quantum winning strategy using a 4-qubit entangled state
Properties

- No classical winning strategy
  - such a strategy corresponds to a magic square
- No quantum winning strategy using a 2-qubit entangled state
  - no such pseudo-telepathy game exists
- There exists a quantum winning strategy using a 4-qubit entangled state
  - quantum strategy (Aravind, 2002) using
    $$\frac{1}{2}|0011\rangle - \frac{1}{2}|0110\rangle - \frac{1}{2}|1001\rangle + \frac{1}{2}|1100\rangle$$
Nonlocal players

- There exists a nonlocal winning strategy for the magic square game that makes use of a single NLB.
Nonlocal players

- There exists a nonlocal winning strategy for the magic square game that makes use of a single NLB.

- Proof: Alice and Bob each have two strategies, $A_0$ and $A_1$ for Alice and $B_0$ and $B_1$ for Bob such that:
Nonlocal players

- all strategies respect the parity condition
Nonlocal players

- All strategies respect the parity condition.
- Both pairs of strategies \((A_0, B_0)\) and \((A_1, B_1)\) yield a correct answer for all inputs except \(x = y = 3\).
Nonlocal players

- all strategies respect the parity condition
- Both pairs of strategies \((A_0, B_0)\) and \((A_1, B_1)\) yield a correct answer for all inputs except \(x = y = 3\).
- Both pairs of strategies \((A_0, B_1)\) and \((A_1, B_0)\) yield a correct answer when \(x = y = 3\).
Nonlocal players

- All strategies respect the parity condition.
- Both pairs of strategies \((A_0, B_0)\) and \((A_1, B_1)\) yield a correct answer for all inputs except \(x = y = 3\).
- Both pairs of strategies \((A_0, B_1)\) and \((A_1, B_0)\) yield a correct answer when \(x = y = 3\).
- Now, Alice and Bob each input 1 into the NLB if their input is 3 (and otherwise they input 0). They use the output of the NLB to determine which strategy to use.
Nonlocal players

- In the quantum winning strategy, the outcomes of the players are uniformly distributed.
Nonlocal players

- In the quantum winning strategy, the outcomes of the players are uniformly distributed.
- By randomizing over all possible strategies $A_0, A_1, B_0, B_1$, it is possible to simulate the correlations of the Magic Square game.
Nonlocal players

- In the quantum winning strategy, the outcomes of the players are uniformly distributed.

- By randomizing over all possible strategies $A_0, A_1, B_0, B_1$, it is possible to simulate the correlations of the Magic Square game.

- Corollary: A NLB can simulate bipartite correlations that no 2-qubit entangled state, $\alpha|00\rangle + \beta|11\rangle$, can.
The Mermin-GHZ Game
The Game

- In the Mermin-GHZ pseudo-telepathy game:
The Game

- In the Mermin-GHZ pseudo-telepathy game:
- Alice, Bob and Charlie receive as input a single bit, $x$, $y$ and $z$, respectively.
In the Mermin-GHZ pseudo-telepathy game:

- Alice, Bob and Charlie receive as input a single bit, \( x, y \) and \( z \), respectively.
- There is a promise that \( x \oplus y \oplus z = 0 \).
The Game

- In the Mermin-GHZ pseudo-telepathy game:
  - Alice, Bob and Charlie receive as input a single bit, \( x, y \) and \( z \), respectively.
  - There is a promise that \( x \oplus y \oplus z = 0 \).
  - Alice and Bob must output one bit each, \( a, b \) and \( c \) respectively, such that
    \[
    a \oplus b \oplus c = \frac{x+y+z}{2}.
    \]
The Game

In a classical strategy, suppose Alice, Bob and Charlie output $a_i$, $b_i$ and $c_i$ respectively, on input $i$. This is a winning strategy if and only if the following system of equations is satisfied:

\[
\begin{align*}
    a_0 \oplus b_0 \oplus c_0 &= 0 \\
    a_0 \oplus b_1 \oplus c_1 &= 1 \\
    a_1 \oplus b_0 \oplus c_1 &= 1 \\
    a_1 \oplus b_1 \oplus c_0 &= 1 
\end{align*}
\]
The Game

- In a classical strategy, suppose Alice, Bob and Charlie output $a_i$, $b_i$ and $c_i$ respectively, on input $i$. This is a winning strategy if and only if the following system of equations is satisfied:

\[
\begin{align*}
    a_0 \oplus b_0 \oplus c_0 &= 0 \\
    a_0 \oplus b_1 \oplus c_1 &= 1 \\
    a_1 \oplus b_0 \oplus c_1 &= 1 \\
    a_1 \oplus b_1 \oplus c_0 &= 1
\end{align*}
\]

- Again, a simple parity argument shows that no such strategy exists.
Properties

- no classical winning strategy
Properties

- no classical winning strategy
- simple parity argument
Properties

- no classical winning strategy
  - simple parity argument
- no quantum winning strategy using a 2-qubit entangled state
Properties

- no classical winning strategy
  - simple parity argument

- no quantum winning strategy using a 2-qubit entangled state
  - no such pseudo-telepathy game exists
Properties

- no classical winning strategy
  - simple parity argument
- no quantum winning strategy using a 2-qubit entangled state
  - no such pseudo-telepathy game exists
- there exists a quantum winning strategy using an 3-qubit entangled state
Properties

- no classical winning strategy
  - simple parity argument

- no quantum winning strategy using a 2-qubit entangled state
  - no such pseudo-telepathy game exists

- there exists a quantum winning strategy using an 3-qubit entangled state
  - quantum strategy using \( \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle \)

(Greenberger, Horne, Zeilinger, 1989)
Theorem: There exists a nonlocal winning strategy for the Mermin-GHZ game that makes use of a single NLB.
Theorem

Theorem: There exists a nonlocal winning strategy for the Mermin-GHZ game that makes use of a single NLB.

Proof: Alice and Bob input $\bar{x}$ and $\bar{y}$ into a NLB. They set $a$ and $b$ as their respective outcomes of the NLB. Charlie simply outputs $c = 1$. Taking into account the promise, it is easy to see that this strategy works.
Theorem

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$z$</th>
<th>$\bar{x}$</th>
<th>$\bar{y}$</th>
<th>$a \oplus b$</th>
<th>$c$</th>
<th>$a \oplus b \oplus c$</th>
<th>$\frac{x+y+z}{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Corollary

- In the quantum winning strategy, the outcomes of the players are uniformly distributed.
Corollary

- In the quantum winning strategy, the outcomes of the players are uniformly distributed.

- If Bob and Charlie share a random bit $r$ and they output $b \oplus r$ and $b \oplus r$ respectively, then we have a simulation of the correlations of the Mermin-GHZ game.
In the quantum winning strategy, the outcomes of the players are uniformly distributed.

If Bob and Charlie share a random bit $r$ and they output $b \oplus r$ and $b \oplus r$ respectively, then we have a simulation of the correlations of the Mermin-GHZ game.

Corollary: A NLB can simulate tripartite correlations that no 2-qubit entangled state, $\alpha|00\rangle + \beta|11\rangle$, can.
Nonlocality and Entanglement are different
Previous and new results

Theorem: there exist bipartite entangled states of two qubits that \textit{cannot} be simulated with a single use of a NLB. (Brunner, Gisin, Scarani 2005)
Previous and new results

- Theorem: there exist bipartite entangled states of two qubits that \emph{cannot} be simulated with a single use of a NLB. (Brunner, Gisin, Scarani 2005)

- “entanglement and nonlocality are different resources”…or are they?
Previous and new results

- Theorem: there exist bipartite entangled states of two qubits that cannot be simulated with a single use of a NLB. (Brunner, Gisin, Scarani 2005)

- “entanglement and nonlocality are different resources”...or are they?

- The result is not asymptotic. It does not rule out the possibility that $O(n)$ NLB are sufficient to simulate $n$ bipartite 2-qubit entangled states.
Theorem: there exist bipartite entangled states of two qubits that cannot be simulated with a single use of a NLB. (Brunner, Gisin, Scarani 2005)

“entanglement and nonlocality are different resources”...or are they?

The result is not asymptotic. It does not rule out the possibility that $O(n)$ NLB are sufficient to simulate $n$ bipartite 2-qubit entangled states.

Here, we show that entanglement and nonlocality are asymptotically different.
Distributed Deutsch-Jozsa game

- Alice and Bob each receive a $2^n$-bit string, $x$ and $y$. 
Distributed Deutsch-Jozsa game

- Alice and Bob each receive a $2^n$-bit string, $x$ and $y$.
- There is a promise that $\Delta(x, y) \in \{0, 2^{n-1}\}$. 

Distributed Deutsch-Jozsa game

- Alice and Bob each receive a $2^n$-bit string, $x$ and $y$.
- There is a promise that $\Delta(x, y) \in \{0, 2^{n-1}\}$.
- Alice and Bob must each output an $n$-bit string $a$ and $b$ such that $[a = b] \iff [x = y]$. 
Properties of the game

For all \( n \geq 4 \), this is a pseudo-telepathy game (Newman, 2004).
Properties of the game

- For all $n \geq 4$, this is a pseudo-telepathy game (Newman, 2004).

- The quantum state used for the quantum winning strategy is $\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle |j\rangle$. 
Properties of the game

- For all \( n \geq 4 \), this is a pseudo-telepathy game (Newman, 2004).

- The quantum state used for the quantum winning strategy is
  \[
  \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|j\rangle.
  \]

- A classical winning strategy for the game requires \( \Omega(2^n) \) bits of communication (Brassard, Cleve, Tapp, 1999).
Theorem: For the distributed Deutsch-Jozsa pseudo-telepathy game, $\Omega(2^n)$ NLB uses are required in a nonlocal winning strategy.
Theorem

Theorem: For the distributed Deutsch-Jozsa pseudo-telepathy game, $\Omega(2^n)$ NLB uses are required in a nonlocal winning strategy.

Proof: If we had a nonlocal winning strategy with less than $\Omega(2^n)$ NLB uses, we could use communication to get a classical winning strategy with less than $\Omega(2^n)$ bits of communication, which is a contradiction.
Asymptotic result!

We have shown: there exists a state of \( n \) maximally entangled bipartite states of two qubits that requires at least \( 2^n \) NLB uses to simulate.
Asymptotic result!

- We have shown: there exists a state of \( n \) maximally entangled bipartite states of two qubits that requires at least \( 2^n \) NLB uses to simulate.

- Entanglement and nonlocality are fundamentally different resources after all!
NLB pseudo-telepathy
Recall that a pseudo-telepathy game is one which does not admit a classical winning strategy, whereas a quantum winning strategy does exist.
Recall that a pseudo-telepathy game is one which does not admit a classical winning strategy, whereas a quantum winning strategy does exist.

A NLB pseudo-telepathy game is one which does not admit a quantum winning strategy, whereas a nonlocal winning strategy exists.
Recall that a pseudo-telepathy game is one which does not admit a classical winning strategy, whereas a quantum winning strategy does exist.

A NLB pseudo-telepathy game is one which does not admit a quantum winning strategy, whereas a nonlocal winning strategy exists.

We have already seen an example of a NLB pseudo-telepathy game: the NLB itself!
A new multi-party NLB

What is the generalization of the NLB to a multi-party setting? In our new game:
A new multi-party NLB

- What is the generalization of the NLB to a multi-party setting? In our new game:
- Each of the $n$ participants receives an input bit.
What is the generalization of the NLB to a multi-party setting? In our new game:

Each of the $n$ participants receives an input bit.

They must each produce an output bit such that the $\oplus$ of all the outputs is equal to the *majority* of the input bits.
A new multi-party NLB

What is the generalization of the NLB to a multi-party setting? In our new game:

- Each of the $n$ participants receives an input bit.
- They must each produce an output bit such that the $\oplus$ of all the outputs is equal to the majority of the input bits.

This new multi-party NLB is a generalization of a two-party NLB.
Properties of the new NLB

- no classical winning strategy
Properties of the new NLB

- no classical winning strategy
- the NLB is a special case of this game
Properties of the new NLB

- no classical winning strategy
- the NLB is a special case of this game
- no quantum winning strategy
Properties of the new NLB

- no classical winning strategy
  - the NLB is a special case of this game

- no quantum winning strategy
  - the NLB is a special case of this game
Properties of the new NLB

- no classical winning strategy
  - the NLB is a special case of this game

- no quantum winning strategy
  - the NLB is a special case of this game

- $\Omega(n)$ NLBs are necessary in a nonlocal winning strategy
Properties of the new NLB

- no classical winning strategy
  - the NLB is a special case of this game

- no quantum winning strategy
  - the NLB is a special case of this game

- $\Omega(n)$ NLBs are necessary in a nonlocal winning strategy
  - each player must be linked to another through a NLB
Conclusion and Future Work
Recap

We have made progress towards characterizing the power of the NLB.

- A single NLB can simulate correlations that no entangled pair of qubits can; in the bipartite and in the tri-partite scenario.
Recap

We have made progress towards characterizing the power of the NLB.

- A single NLB can simulate correlations that no entangled pair of qubits can; in the bipartite and in the tri-partite scenario.

- Nonlocality and entanglement are fundamentally different resources: there exists correlation whose simulation requires an exponential amount of NLB uses.
Recap

We have made progress towards characterizing the power of the NLB.

- A single NLB can simulate correlations that no entangled pair of qubits can; in the bipartite and in the tri-partite scenario.

- Nonlocality and entanglement are fundamentally different resources: there exists correlation whose simulation requires an exponential amount of NLB uses.

- We have defined non-local pseudo-telepathy and proposed a multi-party NLB.
Future Work

- Finding nonlocal winning strategies for all pseudo-telepathy games, or showing that such a task is impossible.
Future Work

- Finding nonlocal winning strategies for all pseudo-telepathy games, or showing that such a task is impossible.
- Finding applications for the new multi-party nonlocal box (for instance, in multi-party entanglement simulation).