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`

Université de Montréal

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.

Université de Montréal

Two examples of nonlocal tasks

Pseudo-telepathy

- Consider a *game*, in which two or more players play as a team, against a *referee*.

Université de Montréal

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.

Université de Montréal

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).

Université de Montréal

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.

Université de Montréal

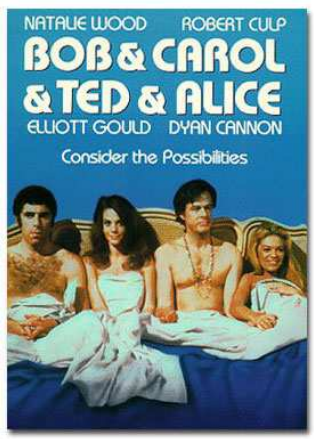
Factoid

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

Université de Montréal

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.



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).

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.

Université de Montréal

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.

Université de Montréal

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.

Université de Montréal

The nonlocal box

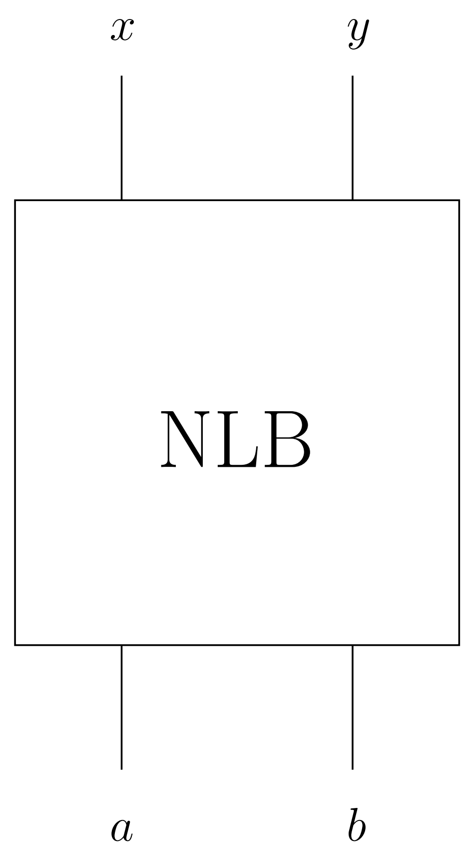
The nonlocal box (NLB)

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:

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

- Furthermore, a and b are uniformly distributed among all solutions.

The nonlocal box (NLB)



Properties of the Nonlocal Box

- Cannot be used for signaling

Université de Montréal

Properties of the Nonlocal Box

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

Université de Montréal

Properties of the Nonlocal Box

- Cannot be used for signaling
  - a and b are uniformly distributed
- Cannot be reproduced by classical participants

Université de Montréal

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

Université de Montréal

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

Université de Montréal

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)

Université de Montréal

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).

Université de Montréal

Measures of nonlocality

- How can we measure the *nonlocalness* of a specific task?

Université de Montréal

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.

Université de Montréal

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.

Université de Montréal

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.

Université de Montréal

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.*

Université de Montréal

Non-local Winning Strategies for Pseudo-Telepathy Games

Université de Montréal

The Magic Square Game

Université de Montréal

Magic Square

- A *magic square* is a 3×3 matrix with entries in $\{0, 1\}$ such that the sum of each row is even and the sum of each column is odd.

Magic Square

- A *magic square* is a 3×3 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?

0	0	0
0	1	1
1	0	?

Université de Montréal

Magic Square

- A *magic square* is a 3×3 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?

0	0	0
0	1	1
1	0	?

- A simple parity argument shows that no magic square exists.

Université de Montréal

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.

		0
		1
1	1	1

Université de Montréal

Properties

- No classical winning strategy

Properties

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

Université de Montréal

Properties

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

Université de Montréal

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

Université de Montréal

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

Université de Montréal

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 $\frac{1}{2}|0011\rangle - \frac{1}{2}|0110\rangle - \frac{1}{2}|1001\rangle + \frac{1}{2}|1100\rangle$

Université de Montréal

Nonlocal players

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

Université de Montréal

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, $A0$ and $A1$ for Alice and $B0$ and $B1$ for Bob such that:

Université de Montréal

Nonlocal players

- all strategies respect the parity condition

Nonlocal players

- all strategies respect the parity condition
- Both pairs of strategies $(A0, B0)$ and $(A1, B1)$ yield a correct answer for all inputs except $x = y = 3$.

Université de Montréal

Nonlocal players

- all strategies respect the parity condition
- Both pairs of strategies $(A0, B0)$ and $(A1, B1)$ yield a correct answer for all inputs except $x = y = 3$.
- Both pairs of strategies $(A0, B1)$ and $(A1, B0)$ yield a correct answer when $x = y = 3$.

Université de Montréal

Nonlocal players

- all strategies respect the parity condition
- Both pairs of strategies $(A0, B0)$ and $(A1, B1)$ yield a correct answer for all inputs except $x = y = 3$.
- Both pairs of strategies $(A0, B1)$ and $(A1, B0)$ 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.

Université de Montréal

Nonlocal players

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

Université de Montréal

Nonlocal players

- In the quantum winning strategy, the outcomes of the players are uniformly distributed.
- By randomizing over all possible strategies $A0, A1, B0, B1$, 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 $A0, A1, B0, B1$, 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.

Université de Montréal

The Mermin-GHZ Game

Université de Montréal

The Game

- In the Mermin-GHZ pseudo-telepathy game:

Université de Montréal

The Game

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

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 $x \oplus y \oplus z = 0$.

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:

$$a_0 \oplus b_0 \oplus c_0 = 0$$
$$a_0 \oplus b_1 \oplus c_1 = 1$$
$$a_1 \oplus b_0 \oplus c_1 = 1$$
$$a_1 \oplus b_1 \oplus c_0 = 1$$

Université de Montréal

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:

$$\begin{aligned} a_0 \oplus b_0 \oplus c_0 &= 0 \\ a_0 \oplus b_1 \oplus c_1 &= 1 \\ a_1 \oplus b_0 \oplus c_1 &= 1 \\ a_1 \oplus b_1 \oplus c_0 &= 1 \end{aligned}$$

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

Université de Montréal

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

Université de Montréal

Properties

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

Université de Montréal

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

Université de Montréal

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

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

Université de Montréal

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 $\overline{x}$ and $\overline{y}$ 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.

Université de Montréal

Theorem

x	y	z	$\bar{x}$	$\bar{y}$	$a \oplus b$	c	$a \oplus b \oplus c$	$\frac{x+y+z}{2}$
0	0	0	1	1	1	1	0	0
0	1	1	1	0	0	1	1	1
1	0	1	0	1	0	1	1	1
1	1	0	0	0	0	1	1	1

Université de Montréal

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.

Université de Montréal

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

Université de Montréal

Nonlocality and Entanglement are different

Université de Montréal

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)

Université de Montréal

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?

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.

Université de Montréal

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.
- Here, we show that entanglement and nonlocality are *asymptotically* different.

Université de Montréal

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 $\Delta(x, y) \in \{0, 2^{n-1}\}$.

Université de Montréal

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 $[a = b] \Leftrightarrow [x = y]$.

Université de Montréal

Properties of the game

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

Université de Montréal

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).

Université de Montréal

Theorem

- 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.

Université de Montréal

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.

Université de Montréal

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!

Université de Montréal

NLB pseudo-telepathy

Université de Montréal

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.

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

Université de Montréal

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.
- 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!

Université de Montréal

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.

Université de Montréal

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.

Université de Montréal

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.

Université de Montréal

Properties of the new NLB

- no classical winning strategy

Université de Montréal

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

Université de Montréal

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

Université de Montréal

Conclusion and Future Work

Université de Montréal

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.

Université de Montréal

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.

Université de Montréal

Future Work

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

Université de Montréal

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).

Université de Montréal