Open Question: link between NonLocal Boxes and Communication Complexity?

Pierre Botteron† (PhD student under A. Broadbent, I. Nechita and C. Pellegrin), Anne Broadbent‡, Marc-Olivier Proulx†.

†University of Toulouse (France), ‡University of Ottawa (Canada).

1. CHSH game

Alice and Bob receive some bits \( x, y \in \{0, 1\} \), and they answer some bits \( a, b \in \{0, 1\} \) to the referee.

- **Win at CHSH** if \( a \oplus b = x \land y \).
- **Win at CHSH'** if \( a \oplus b = (x \lor 1) \land (y \lor 1) \).

Depending on the type of the shared object, Alice and Bob can reach different winning probabilities:

- **Classical Strategy**: \( \max \left( P(\text{win} | \text{CHSH}) \right) = 75\% \).
- **Shared Randomness**: \( \max \left( P(\text{win} | \text{CHSH}’) \right) = 87\% \).
- **Quantum Strategy**: \( \max \left( P(\text{win} | \text{CHSH}’’) \right) = 91\% \).
- **Non-Signalling Strategy**: \( \max \left( P(\text{win} | \text{NS}) \right) = 100\% \).

2. NonLocal Boxes

**Def.** A nonlocal box is formalized by a conditional probability distribution \( P(a, b \mid x, y) \).

**Examples.** \( \begin{align*}
\Pr(a \mid b, x, y) &= \frac{1/2}{1/2} = 1/2, \\
&\text{if } a \oplus b = x \land y, \\
&\text{otherwise.}
\end{align*} \)

- **Shared Randomness**: \( \mathbf{SR}(a, b \mid x, y) = \begin{cases} 
1/2, & \text{if } a = b, \\
0, & \text{otherwise.}
\end{cases} \)
- **Fully mixed box**: \( \{a, b \mid x, y\} = 1/4. \)

**Non-signalling boxes.** The set \( \mathcal{NS} := \{\text{non-signalling boxes}\} \) is an \( 8 \)-dimensional convex set, containing \( Q := \{\text{quantum boxes}\} \).

3. Communication Complexity

Let \( f : \{0, 1\}^n \rightarrow \{0, 1\} \), Assume Alice knows \( f \) and \( X \in \{0, 1\}^n \), and Bob knows \( f \) and \( Y \in \{0, 1\}^n \).

**Def.** The communication complexity of \( f \) at \((X, Y)\), denoted \( \mathbf{CC}_f(X, Y) \), is the minimal number of communication bits between Alice and Bob so that Alice knows the value \( f(X, Y) \) with probability \( p \).

**Def.** A box \( P \) collapses communication complexity if it allows to compute any Boolean function with only one bit of communication and bounded error:

\[ \exists p > \frac{1}{2}, \forall f : \mathcal{X} \times \mathcal{Y}, \mathbf{CC}_f(X, Y) \leq 1. \]

**Intuition.** It is strongly believed that such a collapsing box could not exist in Nature (it would be too powerful) [8, 3, 4, 1].

4. Open Question

Which nonlocal boxes collapse communication complexity?

5. Partial Answers

**Historical Overview of Partial Answers.** This overview is presented in the slice of \( \mathcal{NS} \) passing through the boxes \( \mathcal{PR} \), \( \mathcal{SR} \) and \( \mathcal{I} \), and we zoom in the top-right corner of the diagram. The open question consists in determining what portion of the **blue** area (the ‘post-quantum boxes’) is collapsing, and what portion is not collapsing. 

In **purple** are drawn the known collapsing boxes, whereas in **red** are represented the known non-collapsing boxes.


**Notations.** Let \( P \in \mathcal{NS} \) and consider:

\[ \eta_y := 1 + 2 \sum_x P(c \mid x, y) ; \]

\[ A := (y_0 + y_1 + \eta_1)^2 ; \]

\[ B := 2 \eta_0 + 4y_0 y_1 + 2\eta_1. \]

**Theorem (Sufficient condition).** If the box \( P \) satisfies \( A + B > 16 \), then \( P \) is collapsing.

**Idea of the proof.** Let \( f : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\} \) a Boolean function known by both Alice and Bob, and let two strings \( X \in \{0, 1\}^n \) and \( Y \in \{0, 1\}^m \) known by Alice and Bob respectively. Alice and Bob share infinitely many copies of a certain nonlocal box \( P \) and infinitely many shared random bits.

If the condition \( A + B > 16 \) is valid, then we exhibit a sequence of protocols \( \mathcal{PR}_\infty \) such that for each \( k \), Alice is able to produce a bit of Alice such that equals \( f(X, Y) \) with some probability \( p_k > 1/2 \) using only 1 bit of communication. Moreover, we show that the sequence \( \{p_k\} \) converges to some \( p > 1/2 \), and that \( p \) does not depend on \( f \) nor \( X \) nor \( Y \) (it only depends on \( p \)).

Hence, for any \( f \), there exists a \( k \) large enough such that the protocol \( \mathcal{PR}_\infty \) correctly computes \( f(X, Y) \) with probability \( p > (1 + p_k)/2 > 1/2 \) and only 1 bit of communication, and as the constant \( p := (1 + p)/2 \) is independent of \( f, X, Y \), we indeed obtain that \( P \) collapses communication complexity by definition.

**Examples of new collapsing regions (in black).**

The question is still open today: there is still a **blue** gap to be filled!