Open Question: link between NonLocal Boxes and Communication Complexity?

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

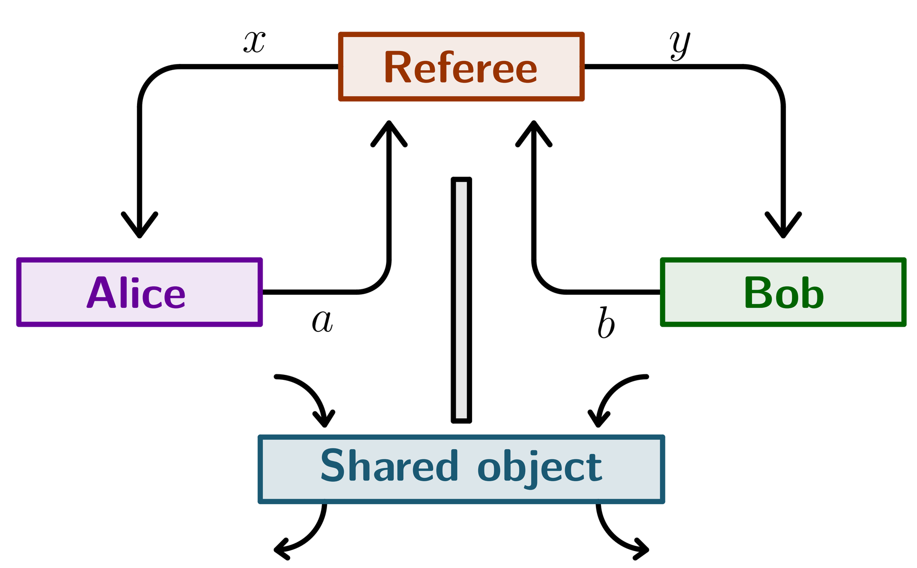
*University of Toulouse (France), †University of Ottawa (Canada).

Goal

Prove that post-quantum boxes collapse communication complexity, and deduce that they are unlikely to exist in Nature.

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** *iff* $a \oplus b = x \times y$.
- **Win at CHSH′** *iff* $a \oplus b = (x \oplus 1) \times (y \oplus 1)$.

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

- **Classical Strategy.** $\max \mathrm{P}\left(\substack{\text{win}\\ \text{CHSH}}\right) = 75\%$.
  ⇝ Shared object: *shared randomness.*
- **Quantum Strategy.** $\max \mathrm{P}\left(\substack{\text{win}\\ \text{CHSH}}\right) = \frac{2+\sqrt{2}}{4} \approx 85\%$.
  ⇝ Shared object: *quantum states.*
- **Non-Signaling Strategy.** $\max \mathrm{P}\left(\substack{\text{win}\\ \text{CHSH}}\right) = 100\,\%$.
  ⇝ Shared object: *nonlocal boxes.*

References

[1] S. Beigi and A. Gohari. Monotone measures for non-local correlations. *IEEE Transactions on Information Theory*, 61(9):5185–5208, 2015.

[2] P. Botteron, A. Broadbent, and M.-O. Proulx. Extending the known region of nonlocal boxes that collapse communication complexity. *Phys. Rev. Lett.*, 132:070201, Feb 2024.

[3] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96:250401, Jun 2006.

[4] N. Brunner and P. Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Physical Review Letters*, 102(16), Apr 2009.

[5] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. *Quantum Entanglement and the Communication Complexity of the Inner Product Function.* Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

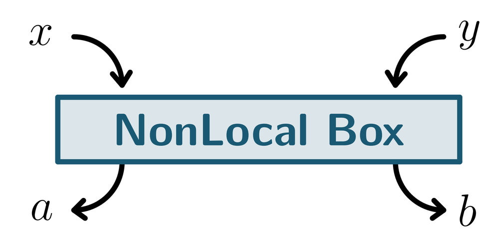
[6] G. Eftaxias, M. Weilenmann, and R. Colbeck. Advantages of multicopy nonlocality distillation and its application to minimizing communication complexity. *Phys. Rev. Lett.*, 130:100201, 03 2023.

[7] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín. Almost quantum correlations. *Nature Communications*, 6(1):6288, 2015.

[8] W. van Dam. *Nonlocality & Communication Complexity.* Ph.d. thesis., University of Oxford, Departement of Physics, 1999.

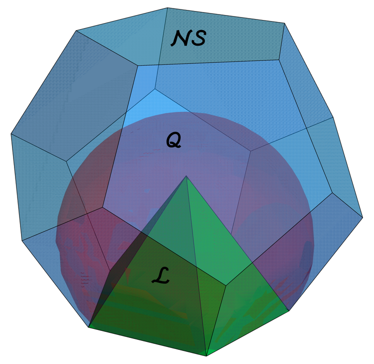
2. NonLocal Boxes

Def. A *nonlocal box* is formalized by a conditional probability distribution $\mathrm{P}(a, b \,|\, x, y)$.



Examples.
- $\mathtt{PR}(a, b \,|\, x, y) := \begin{cases} 1/2 & \text{if } a \oplus b = x \times y, \\ 0 & \text{otherwise.} \end{cases}$
- Shared Randomness: $\mathtt{SR}(a, b \,|\, x, y) := \begin{cases} 1/2 & \text{if } a = b, \\ 0 & \text{otherwise.} \end{cases}$
- Fully mixed box: $\mathtt{I}(a, b \,|\, x, y) := 1/4$.

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



3. Communication Complexity

Let $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$. Assume Alice knows f and $X \in \{0,1\}^n$, and Bob knows f and $Y \in \{0,1\}^m$.

Def. The *communication complexity* of f at (X, Y), denoted $\mathbf{CC}_p(f, X, Y)$, 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:

$$\exists p > \frac{1}{2},\ \ \forall f, \forall X, \forall Y,\ \ \mathbf{CC}_p(f, X, Y) \leq 1\,.$$

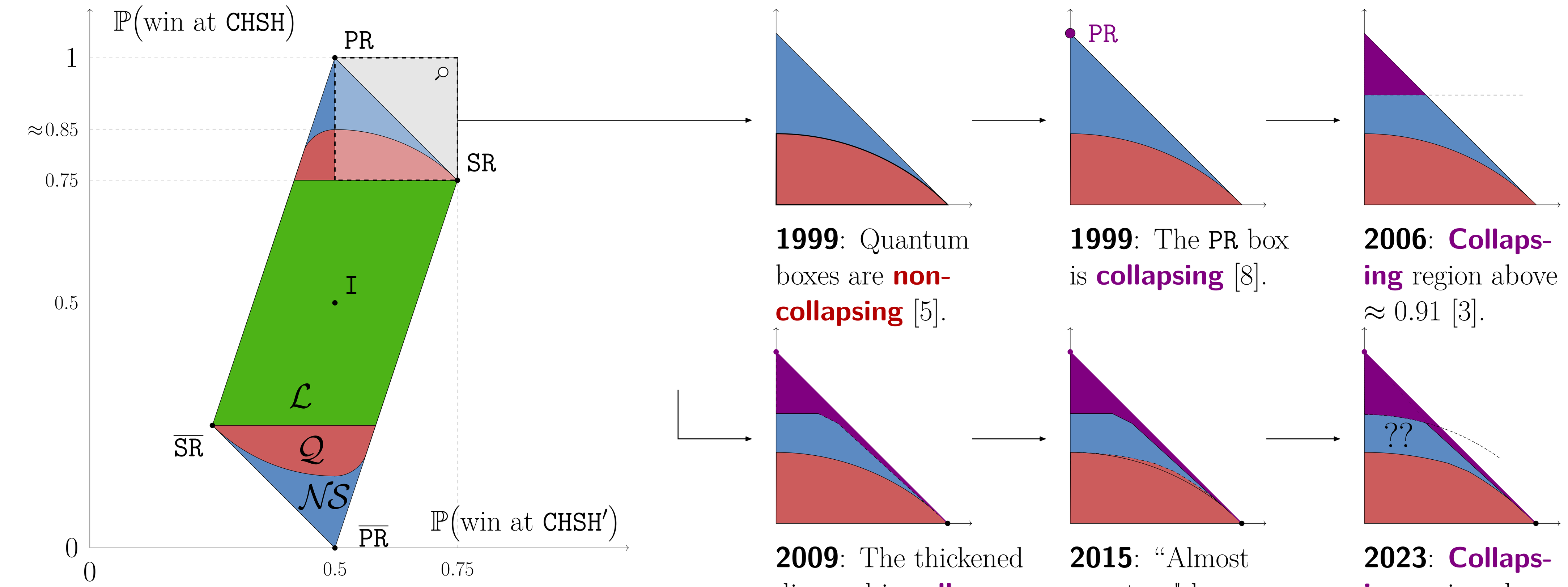
Intuition. It is strongly believed that such a collapsing box could not exist in Nature (it would be too powerful) [8, 3, 4, 1].

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 PR, SR and 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.



1999: Quantum boxes are **non-collapsing** [5].

1999: The PR box is **collapsing** [8].

2006: **Collapsing** region above ≈ 0.91 [3].

2009: The thickened diagonal is **collapsing** (part. numerical result) [4, 6].

2015: "Almost quantum" boxes are **non-collapsing** [7].

2023: **Collapsing** region above an ellipse (analytical result) [2].

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

6. Ideas of our proof [2] (2023)

The proof is a generalization of [3] (2006).

Notations. Let $\mathrm{P} \in \mathcal{NS}$ and consider:

$$\eta_{xy} := -1 + 2\textstyle\sum_c \mathrm{P}(c, c \oplus xy \,|\, x, y)\,;$$
$$A := \big(\eta_{00} + \eta_{01} + \eta_{10} + \eta_{11}\big)^2\,;$$
$$B := 2\,\eta_{00}^2 + 4\eta_{01}\eta_{10} + 2\eta_{11}^2\,.$$

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

Idea of the proof. Let $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ 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 $(\mathcal{P}_k)_k$ such that for each k, Alice is able to produce a bit a that equals $f(X, Y)$ with some probability $p_k > 1/2$ using only 1 bit of communication. Moreover, we show that the sequence $(p_k)_k$ converges to some $p_* > 1/2$:

$$p_k \underset{k\to\infty}{\longrightarrow} p_* > 1/2\,,$$

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 $\mathcal{P}_k$ correctly computes $f(X, Y)$ with probability $p_k > (1 + p_*)/2 > 1/2$ 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).