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†.

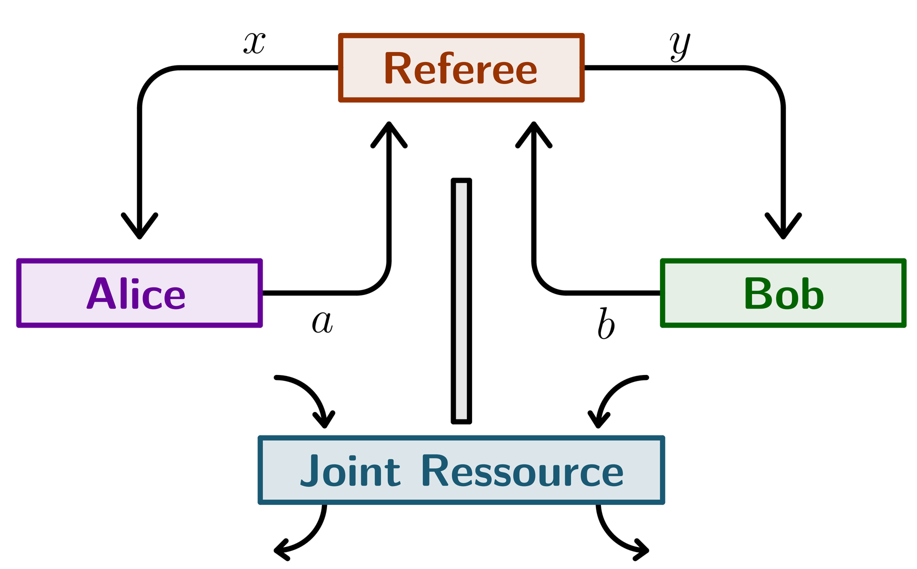
*University of Toulouse (France), †University of Ottawa (Canada).

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 joint ressource they are allowed to use, Alice and Bob have different wining probabilities:

- **Classical Strategy.** $\max \mathrm{P}\left(\begin{smallmatrix}\text{win}\\ \text{CHSH}\end{smallmatrix}\right) = 75\%$.
  ⇝ Joint ressource: *shared randomness.*
- **Quantum Strategy.** $\max \mathrm{P}\left(\begin{smallmatrix}\text{win}\\ \text{CHSH}\end{smallmatrix}\right) = \frac{2+\sqrt{2}}{4} \approx 85\%$.
  ⇝ Joint ressource: *quantum states.*
- **Non-Signaling Strategy.** $\max \mathrm{P}\left(\begin{smallmatrix}\text{win}\\ \text{CHSH}\end{smallmatrix}\right) = 100\,\%$.
  ⇝ Joint ressource: *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. *arXiv preprint arXiv:2302.00488*, 2023.

[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.

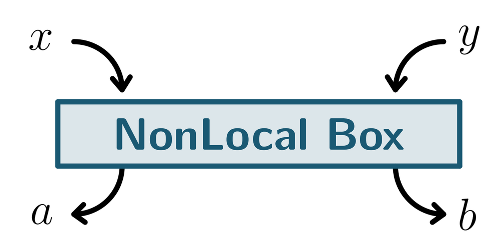
[5] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp. *Quantum Entanglement and the Communication Complexity of the Inner Product Function.* Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

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

[7] 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 $\mathtt{P}(a, b\,|\,x, y)$.

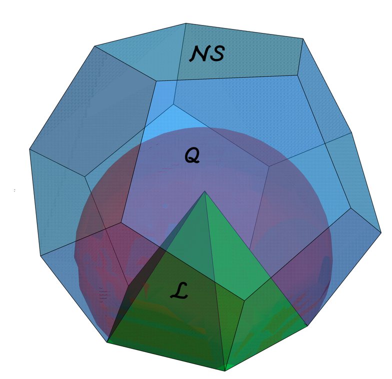


Examples. • $\mathtt{PR}(a,b\,|\,x,y) := \begin{cases} 1/2 & \text{if } a \oplus b = x \times y, \\ 0 & \text{otherwise.} \end{cases}$

• 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 $\mathtt{P}$ *collapses communication complexity* if it allows to compute any Boolean function with only one bit of communication and bounded error:

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

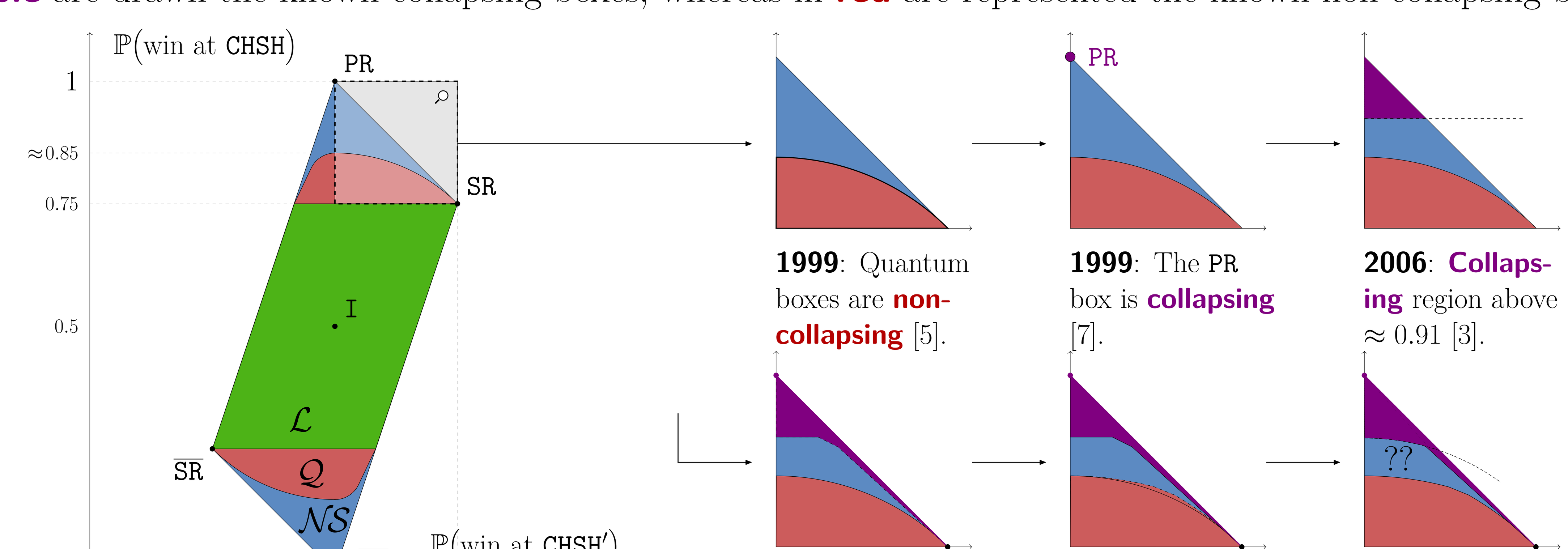
Intuition. It is strongly believed that such a collapsing box could not exist in Nature (it would be too powerful) [7, 3, 4, 1].

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** [7].

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

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

2015: "Almost quantum" boxes are **non-collapsing** [6].

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)

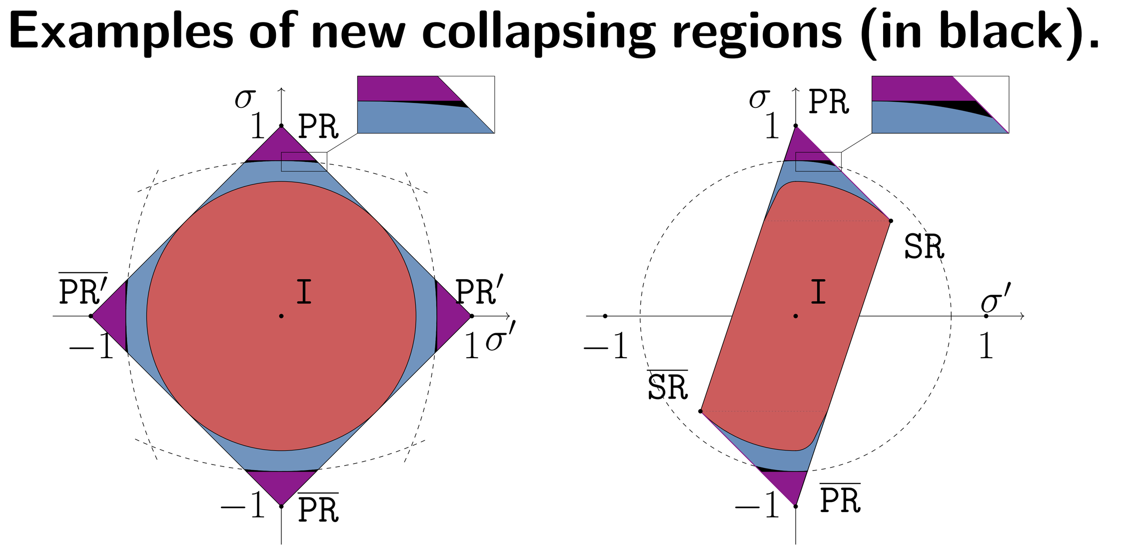
The proof is a generalization of [3] (2006).

- **Setting.** Let $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ a Boolean function, and two strings $X \in \{0,1\}^n$ (known by Alice) and $Y \in \{0,1\}^m$ (known by Bob). Alice and Bob share a nonlocal box $\mathtt{P}$ and infinitely many shared random bits.
- **Protocol $\mathcal{P}_0$.** We define a protocol $\mathcal{P}_0$ in which Alice and Bob smartly guess some bits a_0, b_0 respectively, using only shared random bits, without communication. We show their guess satisfies $a_0 \oplus b_0 = f(X, Y)$ with probability $p_0 > 1/2$.
- **Protocol $\mathcal{P}_1$.** We apply 3 times this protocol $\mathcal{P}_0$, we obtain 3 pairs of guesses $(a_0^1, b_0^1), (a_0^2, b_0^2), (a_0^3, a_0^3)$. Alice and Bob make a majority vote among the three sums $a_0^i \oplus b_0^i$ to keep the most frequent one. Then they use the nonlocal box $\mathtt{P}$ in order to guess a new pair (a_1, b_1) such that $a_1 \oplus b_1 = f(X, Y)$ with better probability $p_1 > p_0$.
- **Protocol $\mathcal{P}_k$.** We repeat the same process inductively to build a protocol $\mathcal{P}_k$ from the protocol $\mathcal{P}_{k-1}$. Alice and Bob guess (a_k, b_k) such that $a_k \oplus b_k = f(X, Y)$ with prob. $p_k > p_{k-1} > \ldots > p_0$.
- **Theorem.** We prove that under some conditions over the box $\mathtt{P}$ (*e.g.* being in the purple area of the last drawing), then $(p_k)_k$ converges to some $p_* > 1/2$, where the limit p_* is independent of f, of X and of Y. So there exists a k large enough for which $p_k > p_* - \varepsilon$; then Bob sends his communication bit b_k to Alice, and Alice knows $a_k \oplus b_k$ which equals $f(X, Y)$ with probability $> p_* - \varepsilon$. Hence:

$$\forall f, \forall X, \forall Y,\ \ \mathbf{CC}_{p_* - \varepsilon}(f, X, Y) \leq 1\,,$$

and communication complexity collapses. □

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



Poster presented at ICMAT (Madrid), on March 21, 2023.