# NonLocal Boxes & Communication Complexity

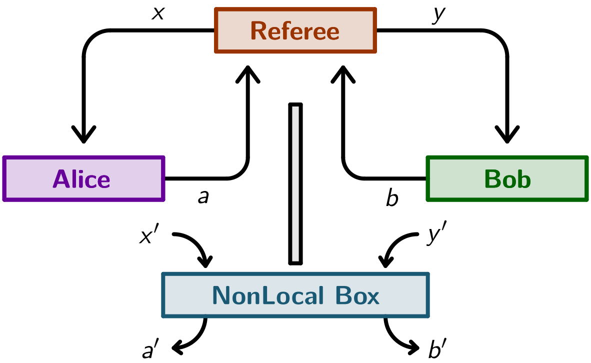
Pierre Botteron, Anne Broadbent,
Ion Nechita, Clément Pellegrini.
(Monday $22^{th}$ of August, 2022.)

# Contents

— *Part* 1 —

# Definitions & Notations

# CHSH Game

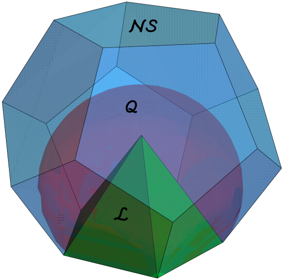



**Win at CHSH.** $a \oplus b = x\,y$.

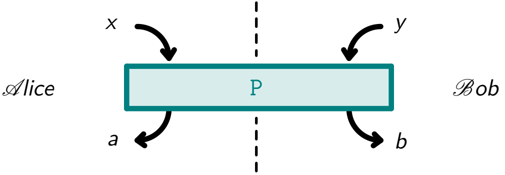
**Win at CHSH'.** $a \oplus b = (x \oplus 1)\,(y \oplus 1)$.

# Strategies

- **Deterministic strategies.** $\rightsquigarrow \max \mathbb{P}(\text{win}) = 75\%$.
- **Classical strategies $\mathcal{L}$.** $\rightsquigarrow \max \mathbb{P}(\text{win}) = 75\%$.
- **Quantum strategies $\mathcal{Q}$.** $\rightsquigarrow \max \mathbb{P}(\text{win}) = \cos^2\left(\frac{\pi}{8}\right) \approx 85\%$.
- **Non-signalling strategies $\mathcal{NS}$.** $\rightsquigarrow \max \mathbb{P}(\text{win}) = 100\%$.



# NonLocal Box

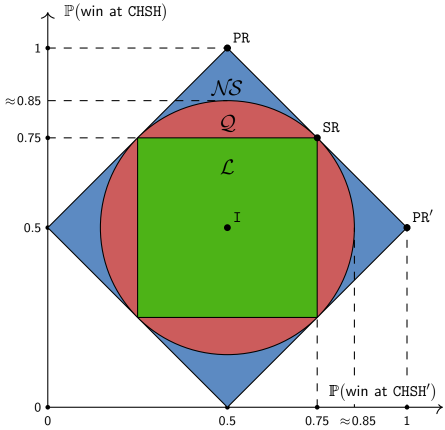



**Definition.** *A* **nonlocal box** *is a function:*

$$\mathtt{P} : \left\{ \begin{array}{ccc} \{0,1\}^4 & \longrightarrow & [0,1] \\ (a,b,x,y) & \longmapsto & \mathtt{P}\big(a,b \,\big|\, x,y\big). \end{array} \right.$$

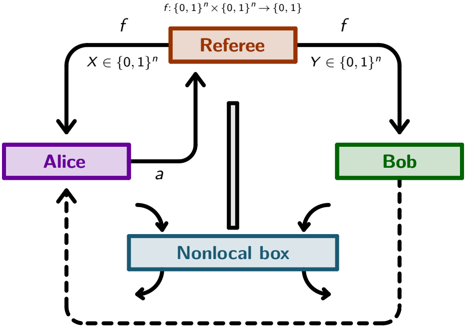
*such that (i)* $\mathtt{P}$ *is a conditional probability distribution and (ii)* $\mathtt{P} \in \mathcal{NS} \backslash \mathcal{L}$.

# Examples




- $\mathtt{PR}\big(a, b \,|\, x, y\big) := \begin{cases} \frac{1}{2} & \text{si } a \oplus b = x\,y, \\ 0 & \text{otherwise.} \end{cases}$
- $\mathtt{PR}'\big(a, b \,|\, x, y\big) := \begin{cases} \frac{1}{2} & \text{si } a \oplus b = (x \oplus 1)\,(y \oplus 1), \\ 0 & \text{otherwise.} \end{cases}$
- $\mathtt{SR}\big(a, b \,|\, x, y\big) := \begin{cases} \frac{1}{2} & \text{si } a = b, \\ 0 & \text{otherwise.} \end{cases}$
- $\mathtt{I}\big(a, b \,|\, x, y\big) := \frac{1}{4}$

# Communication Complexity




Win $\iff a = f(X, Y)$.

**Def.** *A function $f$ is said to be* **trivial** *(in the sense of communication complexity) if Alice knows any value $f(X, Y)$ with only one bit transmitted between Alice and Bob.*

**Ex.** For $n = 2$, $X = (x_1, x_2)$, $Y = (y_1, y_2)$:

- $f := x_1 \oplus y_1 \oplus x_2 \oplus y_2 \oplus 1$ is trivial.
- $g := (x_1\, x_2) \oplus (y_1\, y_2)$ is trivial.
- $h := (x_1\, y_1) \oplus (x_2\, y_2)$ is NOT trivial.

**Def.** *A box* $\mathtt{P}$ *is* **trivial** *(in the sense of communication complexity) if using this box* $\mathtt{P}$ *any Boolean function $f$ is trivial, with probability $\geq q > \frac{1}{2}$.*

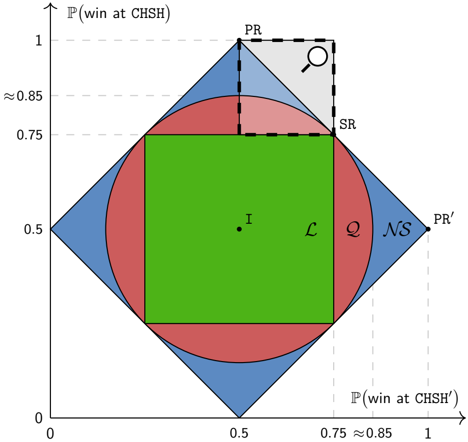
**Ex.** Link with our boxes:

- The boxes $\mathtt{PR}$ and $\mathtt{PR}'$ are trivial.
- The boxes $\mathtt{SR}$ and $\mathtt{I}$ are NOT trivial.

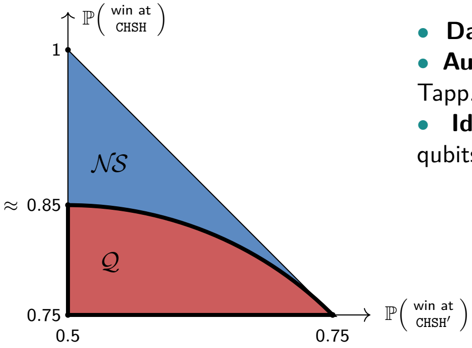
— *Part* 2 —

# Historical Overview

**Goal.** Show that quantum boxes are **non-trivial** but that post-quantum boxes are **trivial**.

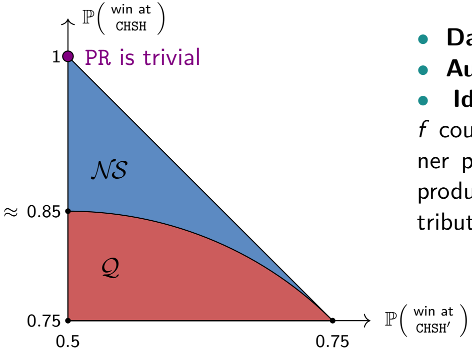


# 1999: Quantum boxes are non-trivial



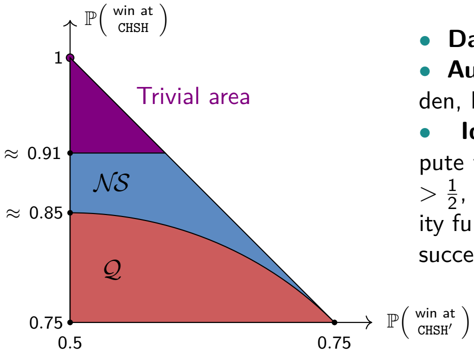

- **Date.** 1999 [1].
- **Authors.** Cleve, van Dam, Nielson, Tapp.
- **Ideas.** (1) Prove the result with qubits, (2) Go back to bits.

# 1999: The PR box is trivial



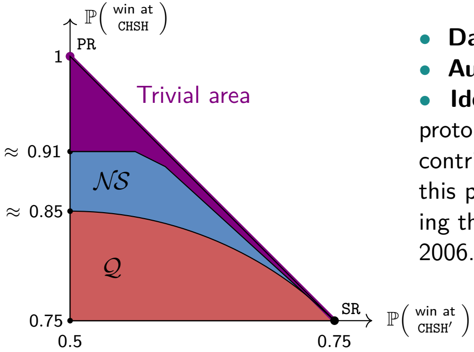

- **Date.** 1999 [2].
- **Author.** van Dam.
- **Idea.** (1) Any Boolean function $f$ could be written in terms of an inner product function, (2) Any inner product function is trivial (using distributed bits).

# 2006: Boxes above $\approx 91\%$ are trivial



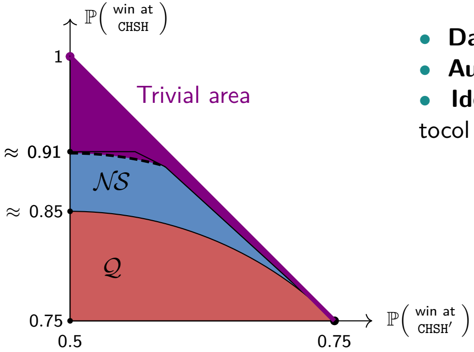

- **Date.** 2006 [3].
- **Authors.** Brassard, Buhrman, Linden, Méthot, Tapp, Unger.
- **Ideas.** (1) Distributively compute the given function $f$ with proba $> \frac{1}{2}$, (2) Inductively apply the majority function `Maj` in order to boost the success probability.

# 2009: Correlated boxes are trivial




- **Date.** 2009 [4].
- **Authors.** Brunner, Skrzypczyk.
- **Ideas.** (1) Introduce a distillation protocol, cf. generalization in “Our contribution”, (2) Inductively apply this protocol many times until reaching the "trivial triangle" discovered in 2006.

# 2018: Boxes above an ellipse are trivial

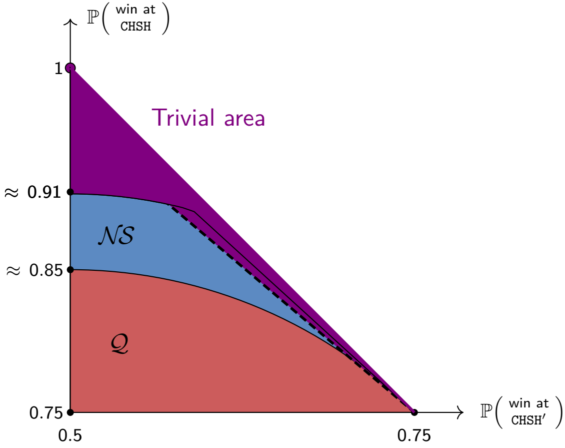



- **Date.** 2018 [5].
- **Author.** Broadbent, Proulx.
- **Idea.** Generalize BBLMTU's protocol (cf. 2006).

— *Part 3* —

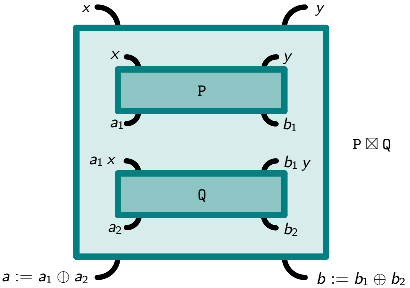
# Our Contribution: Algebra of Boxes

# Our contribution



# Algebra of boxes

**Recall.** *A* nonlocal box $\mathtt{P}$ *is a conditional probability distribution* $(a, b, x, y) \in \{0,1\}^4 \mapsto \mathtt{P}(a, b \,|\, x, y) \in [0,1]$ *such that* $\mathtt{P} \in \mathcal{NS} \backslash \mathcal{L}$.




$$\mathtt{P} \boxtimes \mathtt{Q}\Big(a,\, b \,\Big|\, x,\, y\Big) := \sum_{a_1, b_1 \in \{0,1\}} \mathtt{P}\Big(a_1,\, b_1 \,\Big|\, x,\, y\Big) \times \mathtt{Q}\Big(a \oplus a_1,\, b \oplus b_1 \,\Big|\, a_1 x,\, b_1 y\Big)$$

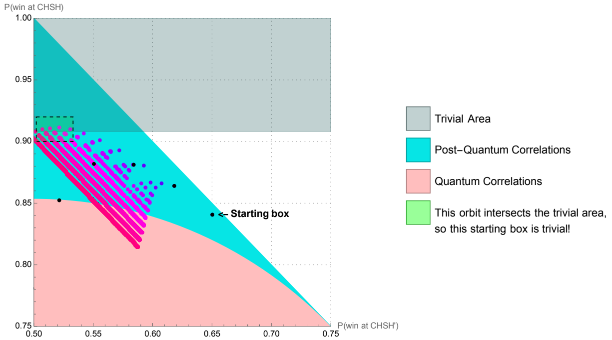
**Algebra of boxes.** The vector space $\mathcal{B} := \mathcal{F}\big(\{0,1\}^4, \mathbb{R}\big)$ endowed with the operations $\{+, \cdot, \boxtimes\}$ defines a non-commutative and non-associative algebra.

# Orbit of a box

**Orbit of order $k$.** $\texttt{Orbit}_k(\mathtt{P}) := \Big\{\text{products of exactly } k \text{ times the term } \mathtt{P}\Big\}$.

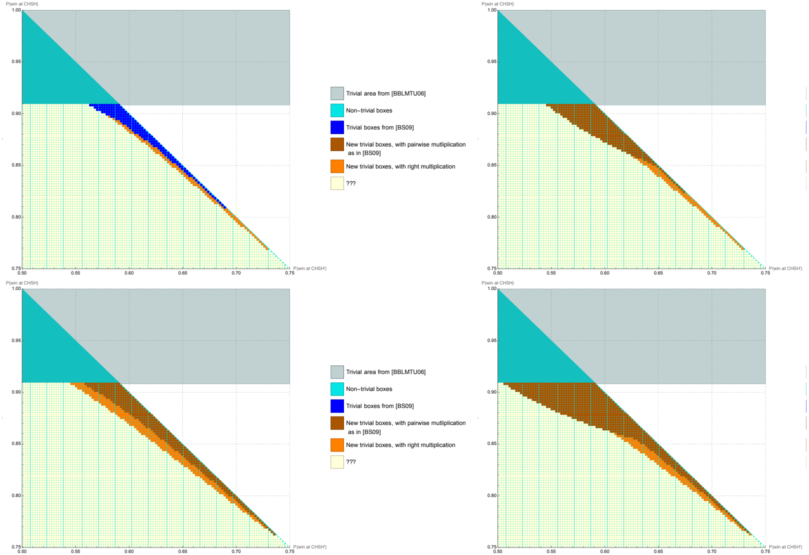
**Examples.** • $\texttt{Orbit}_3(\mathtt{P}) = \Big\{\mathtt{P} \boxtimes (\mathtt{P} \boxtimes \mathtt{P}),\ (\mathtt{P} \boxtimes \mathtt{P}) \boxtimes \mathtt{P}\Big\}$,

• $\texttt{Orbit}_4(\mathtt{P}) = \Big\{\mathtt{P}\boxtimes\big(\mathtt{P}\boxtimes(\mathtt{P}\boxtimes\mathtt{P})\big),\ \mathtt{P}\boxtimes\big((\mathtt{P}\boxtimes\mathtt{P})\boxtimes\mathtt{P}\big),\ \big(\mathtt{P}\boxtimes(\mathtt{P}\boxtimes\mathtt{P})\big)\boxtimes\mathtt{P},\ \big((\mathtt{P}\boxtimes\mathtt{P})\boxtimes\mathtt{P}\big)\boxtimes\mathtt{P},\ \big(\mathtt{P}\boxtimes\mathtt{P}\big)\boxtimes\big(\mathtt{P}\boxtimes\mathtt{P}\big)\Big\}$.




**The "highest" box in each orbit.** $\mathtt{P}_{\max,\,k} \;=\; \Big(\big((\mathtt{P} \boxtimes \mathtt{P}) \boxtimes \mathtt{P}\big) \cdots\Big) \boxtimes \mathtt{P} \;=:\; \mathtt{P}^{\boxtimes k}$.

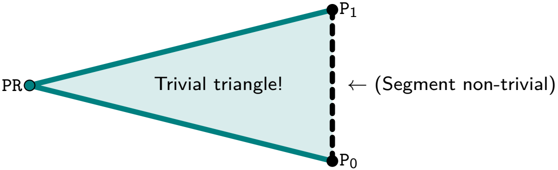
# New trivial boxes: numerically



# New trivial boxes: analytically

**Theorem 1 (New trivial boxes)**

*In the triangle whose vertices are* $\{\mathtt{PR},\ \mathtt{P}_0 := \mathbf{1}_{a=b=0},\ \mathtt{P}_1 := \mathbf{1}_{a=b=1}\}$*, all the points are trivial boxes, except points in the segment* $\mathtt{P}_0$-$\mathtt{P}_1$*.*




*Proof.* **(1)** If we write $\mathtt{SR}_\varepsilon := \varepsilon\,\mathtt{P}_0 + (1-\varepsilon)\,\mathtt{P}_1$ and $(p,\,\varepsilon)$-corNLB $:= p\,\mathtt{PR} + (1-p)\,\mathtt{SR}_\varepsilon$ with $p, \varepsilon \in \mathbb{R}$, then:

$$(p,\,\varepsilon)\text{-corNLB} \boxtimes (p,\,\varepsilon)\text{-corNLB} \;=\; (\widetilde{p},\,\widetilde{\varepsilon})\text{-corNLB},$$

for some $\tilde{p}$ and $\tilde{\varepsilon}$. **(2)** We initialize $p \in ]0,1]$ and $\varepsilon \in [0,1]$, and we inductively apply the multiplication $\boxtimes$. **(3)** We thus obtain a sequence of boxes, and we can show that they converge to PR. **(4)** But, near PR, all boxes are trivial (cf. 2006). **(5)** Hence, the orbit intersects the trivial area and the starting box must be trivial. □

# Bibliography

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

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

[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.*, vol. 96, p. 250401, Jun 2006.

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

[5] M.-O. Proulx, "A limit on quantum nonlocality from an information processing principle," Master's thesis, Department of Physics, University of Ottawa, Canada, 2018. Under the supervision of Anne Broadbent and David Poulin.

[6] P. Botteron, "Nonlocal boxes and communication complexity," Master's thesis, Université Paul Sabatier (Toulouse), 2022. Under the supervision of Anne Broadbent, Ion Nechita and Clément Pellegrini.