NonLocal Boxes and Communication Complexity

Pierre BOTTERON[1] – *Master's thesis*

Supervisors: *Anne* BROADBENT[2] (Ottawa), *Ion* NECHITA[3] and *Clément* PELLEGRINI[4] (Toulouse).

Abstract. The famous CHSH game displays strict demarcations between three canonical families of correlations known as classical, quantum and non-signalling. Although Alice and Bob cannot win more than 75% of the time in the classical case (Bell's Inequality), they can outperform this limit as long as they are provided with quantum correlations and thereby reach Tsirelson's Bound ≈ 85%. Doing even better, post-quantum strategies, formalized with *non-local boxes*, can win with up to 100% probability, yet without violating non-signalling axiom (no faster-than-light communication). This tells that Quantum Mechanics is not fully singled out by (1) the non-signalling axiom and (2) nonlocality, which led Popescu and Rohrlich to raise a question in 1994: what could be missing axioms?[5] Among many attempts, *communication complexity* is conjectured to provide an answer: as opposed to quantum correlations which are known to induce *non-trivial* communication complexity, some post-quantum boxes are shown to render it *trivial*. To this day, the question is still open, and in the present report, after making a detailed historical overview, we provide a new partial answer. We propose a new approach to *distillation* with what we call *algebra of boxes* and *orbit* of a box, which leads to disclosing new trivial areas, some numerically and others explicitly.

Keywords. CHSH game, non-signalling correlations, nonlocal box, trivial communication complexity.

Table of Contents

[1] Pierre Botteron: Université Paul Sabatier (Toulouse). Last edition: Tuesday 28th June, 2022.
[2] Anne Broadbent: Département de Mathématiques et Statistiques, Ottawa, Canada.
[3] Ion Nechita: CNRS - Laboratoire de Physique Théorique, Toulouse, France.
[4] Clément Pellegrini: Institut de Mathématiques de Toulouse, Toulouse, France.

[5] The original discussion was more precisely: "*For quantum correlations, the CHSH sum of correlations is bounded in absolute value by* $2\sqrt{2}$. *Where does this bound come from? [...] Why do they not violate it more? [...] We have proposed two axioms for quantum theory, nonlocality and relativistic causality, which together imply quantum indeterminacy. From our brief exercise with nonlocal correlations, however, we learn that our two axioms do not determine quantum theory, [...] our two axioms are not enough. [...] We hope then to find a logically simple quantum theory.*" [PR94].

Introduction

> « *Do you really believe that the moon exists only when you look at it?* » (Einstein) [Pai79]

In the early twentieth century, although Albert Einstein contributed a lot to the establishment of quantum theory, especially with his Nobel price winning paper [Ein05a], he did not approve the way it was evolving in and he described *quantum entanglement* as "spooky actions at a distance". Quantum entanglement is the essential idea that makes two entangled particles behaving like *one* big system: particules are a superposition of states, and if we measure the state of only one of the particles, then we automatically and *instantly* learn the state on the other as well, *no matter how far they are from each other*. According to Einstein, this scenario involves instantaneous transmission of information between particles, so it implies faster-than-light communication and is therefore in contradiction with his Special Relativity theory. This is the reason why he came up in 1935 with his famous *EPR paradox* [EPR35] together with Podolsky and Rosen.

In EPR paradox, the authors assumed Local Realism, as it was a standard in all fields of physics by that time. In this report, we will denote $\mathcal{L}$ the set of local correlations. On the one hand, *locality* is the idea that, at short time scale, a particle is only influenced by its nearby neighbor particles, called "local beables" [GNTZ11]. On the other hand, *realism* is the idea that a particle's behavior is determined by its properties (mass, position, spin...) and its environment. A lack of knowledge could cause unpredictable measurement outcomes, meaning that there are *local hidden variables* which are unknown but which impact the outcome of the measurement, but if we knew all the properties of the object and the interactions with its environment then measurements would be predictable. So according to EPR, quantum mechanics could not be a complete theory, it should be supplemented by additional variables and it is impossible to have quantum superposition, as the one in Schrodinger's cat experiment [Sch35].

But later, in 1964, John S. Bell made a breakthrough: he showed that local realism is actually incompatible with quantum mechanics [Bel64]. He disclosed some inequalities, known as Bell's inequalities, that single out the local set $\mathcal{L}$ and he found a quantum state violating one of those inequalities. A few years after, Clauser, Horne, Shimony and Holt derived a simpler Bell's inequality, called `CHSH` inequality [CHSH69]. So the set $\mathcal{Q}$ of quantum correlations happens to be strictly bigger than the local set $\mathcal{L}$. In order to verify that Nature really violates local realism, many experiements have been conduced, [CS78, AGR82, RKM+01] to name but a few, but loopholes were found [BCP+14] until recent experiments [HBD+15, SMSC+15] which are hopefully loophole-free. Good recent reviews of Bell nonlocality and its applications are found in [BCP+14, Sca19].

> « *When the Queen dies in London—may it long be delayed—the Prince of Wales, lecturing on modern architecture in Australia, becomes instantaneously King.* » (Bell) [Bel90]

Then, in 1980, taking part in this new enthusiasm to learn more about nonlocality, Tsirelson (*a.k.a.* Cirel'son) showed that nonlocality is limited and that entangled particles need to satisfy a new inequality, called Tsirelson's Bound [Cir80].

Often in Physics, limitations observed in Nature emerge from physical principles, as it is the case for Special Relativity theory. This led Popescu and Rohrlich in 1994 to search for such a physical principle. They put to the try the two axioms of (1) no faster-than-light communication (a.k.a. *non-signalling axiom*) and (2) nonlocality [PR94]. Their conclusion was that those two axioms are not enough to perfectly single out Quantum Mechanics, *i.e.* at least an axiom is missing to fully characterize $\mathcal{Q}$, because they found a theoretical post-quantum correlation, called `PR` box, which is not in the quantum set $\mathcal{Q}$ but which respects both axioms. This is why we might wonder: what could be missing axioms?[6]

Many attempts to finding the remaining axioms have been listed and reviewed by Popescu (one of the co-authors of the `PR` box) in [Pop14]: *nonlocal computation* [LPSW07], *information causality* [PPK+09], *macroscopic locality* [NW09], *local orthogonality* [FSA+13], *nonlocality swapping* [SBP09], *many-box locality*

[6] Barrett as well wondered about that question: "Aside from Hardy's derivation, what different ways are there of uniquely identifying quantum theory from the other theories in the framework by adding as few extra assumptions as possible?" [Bar07, Section VIII.E]

[ZCB+17], and last but not least, *communication complexity* [vD99, BBL+06, BS09, BCMdW10]. However, none of them has been shown to perfectly single out $\mathcal{Q}$. In this report, we choose to focus on communication complexity because this criterion seems the most promising one due to its precision near the SR box [BS09], see Subsection II.(4).

This report is organized as follows. First, for the sake of completeness, we introduce all the necessary material in Section I. More particularly, we define CHSH game in order to illustrate the difference between the local set $\mathcal{L}$, the quantum set $\mathcal{Q}$ and the non-signalling set $\mathcal{NS}$. We introduce as well the key notions of *nonlocal box* and of *communication complexity*, which are at the heart of this report. Next, in Section II. we make an historical overview of the main proofs trying to determine a clear split between quantum and post-quantum correlations, using communication complexity. Eventually in Section III. we present our contribution with what we call *algebra of boxes*, and we disclose some new trivial post-quantum boxes. This report finds a large part of its inspiration in Marc-Olivier Proulx's Master's thesis [Pro18].

I. Basics and Notations

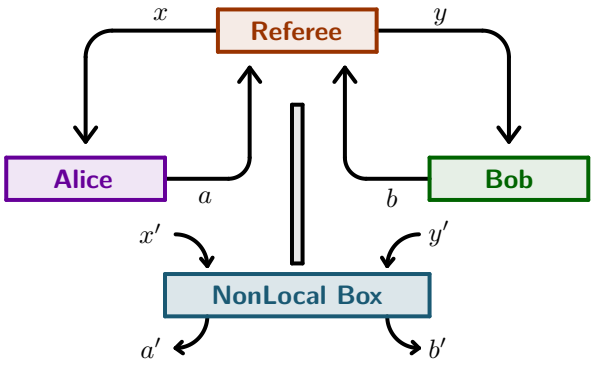
In this section, we introduce all the necessary materials for a good appreciation of the next two sections. First in Subsection I.(1), we introduce CHSH game which is a convenient introduction in order to visualize some differences between the sets of correlations $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$. As well, we add some details about the geometry of those sets, as it will be useful in Section III. Then in Subsection I.(2), we define nonlocal boxes, we provide plenty of examples and we draw a famous slice of boxes. Eventually, we define the notion of communication complexity in Subsection I.(3), which leads to the definition of *trivial box*.

I.(1) Context: CHSH Game

> « *Each answer raises new questions, completely different in nature from the ones one started with; this, more than anything else, indicates that finally we might be on the right track.* » [Pop14]

The most well-known Bell's inequality is CHSH inequality [CHSH69], named after the authors John Clauser, Michael Horne, Abner Shimony and Richard Holt. Here we study CHSH game, which illustrates well both violation of CHSH inequality with $\mathcal{Q}$, and of Tsirelson's bound with $\mathcal{NS}$.

CHSH Game. The CHSH game is a hypothetical scenario presented in a form of game between two parties, often called Alice and Bob, who are geographically separated far enough from each other so that direct communication is impossible. A third person is involved, the referee, who can communicate with each player and whose role is to verify whether Alice and Bob win or not. As shown in Drawing I.(a) below, the game begins when the referee provides the players Alice and Bob with respective classical bits $x, y \in \{0, 1\}$ called *questions*.



Drawing I.(a) — CHSH game scenario, where Alice and Bob share a nonlocal box that they can use as a ressource in their strategy.

Then, without inter-communication, Alice and Bob send back respective bits $a, b \in \{0,1\}$ to the referee, named *answers*, computed according to the strategy the have established together before being space-wise separated. Note that Alice do not have any idea of the value of y, nor does Bob concerning x. Eventually, the referee declares that the players win CHSH game if and only if the mod-2 sum $a \oplus b$ of the answers equals the product $x \wedge y$ of the questions:

$$\text{Alice and Bob win at CHSH} \quad \Longleftrightarrow \quad a \oplus b = x \wedge y. \tag{1}$$

This equality is the *rule* of the game. Equivalently, we say that Alice and Bob win at CHSH if they output the same answer $a = b$ (without inter-communicating) when $x = 0$ or $y = 0$, or if they output different answers $a \neq b$ when $x = y = 1$, without inter-communicating neither. There exists as well a similar game named CHSH′ (derived from [Bra11]), whose procedures for questions and answers are the same, but whose rule slightly differs from the one of CHSH:

$$\text{Alice and Bob win at CHSH}' \quad \Longleftrightarrow \quad a \oplus b = (x \oplus 1) \wedge (y \oplus 1). \tag{2}$$

Actually, in this game, Alice and Bob play the same game as before but with flipped questions, in the sense that x and $x \oplus 1$ are always opposed bits, and similarly for y and $y \oplus 1$. In this thesis, we will always assume x and y to be independent and uniformly randomly distributed in $\{0,1\}$.

Remark I.1 (Logic Gates). In logic gate terms, the mod-2 sum $\oplus$ is actually the XOR gate: $a \oplus b = 1$ whenever $a = 1$ or $b = 1$ but not both; the product $\wedge$ is the AND gate: $x \wedge y = 1$ whenever both $x = 1$ and $y = 1$; and the flip $\oplus 1$ is the NOT gate: $x \oplus 1 = 1$ whenever a is not 1. So in some sense, the purpose of CHSH game is to turn an AND gate into an XOR gate.

Deterministic Strategy. As mentioned hereinabove, before moving apart from each other, Alice and Bob can prepare in advance a strategy so that they maximise their probability of winning. A strategy is as well frequently called *correlation*. There exist different types of strategies, conditional on the ressources that are allowed to Alice and Bob to share during the game—even though they cannot communicate. The most basic one is the *deterministic strategy*, where Alice and Bob do not share anything. More explicitly, they choose beforehand a behavior $g : \{0,1\} \to \{0,1\}$ for Alice depending on the question x she will receive, so that she will answer $a = g(x)$, and similarly for Bob answering $b = h(y)$ for some $h : \{0,1\} \to \{0,1\}$. With such a strategy, they will with the following probability:

$$\mathbb{P}\Big(\text{win at CHSH}\Big) \;=\; \sum_{x,y\in\{0,1\}} \tfrac{1}{4}\, \mathbb{1}_{g(x)\oplus h(y)=x\wedge y},$$

where the $\frac{1}{4}$ comes from the uniform distribution of x and y in $\{0,1\}$, and where $\mathbb{1}_A$ stands for the indicator function taking value 1 *if, and only if,* condition A is satisfied. For instance, if their strategy is to always answer 0 no matter what they receive, *i.e.* $g \equiv h \equiv 0$, then they win at CHSH with $\boxed{75\%}$ of probability. And actually, we can show that this value is optimal for deterministic strategies. Indeed, otherwise they would win with probability 100%, which would mean $g(x) \oplus h(y) = x \wedge y$ for all $x, y \in \{0,1\}$ and which would give rise to the following contradiction:

$$1 \;=\; g(1) \oplus h(1) \;=\; \Big(g(1) \oplus h(0)\Big) \oplus \Big(h(0) \oplus g(0)\Big) \oplus \Big(g(0) \oplus h(1)\Big) \;=\; 0 \oplus 0 \oplus 0 \;=\; 0.$$

Classical Strategies $\mathcal{L}$. In this second type of strategy, Alice and Bob have access to a *shared randomness*: they can share the outcome a common dice, or they can have access to a list of random numbers, or they can use the first journal page to generate numbers, *etc...* The symbol $\mathcal{L}$ stands for the set *local strategies*, an other name of classical strategies because they are the exact ones that are consistent with theories of causality and locality [Bel64] (see the terminology differences in [WW01]). This strategy involves a random variable λ, often called *local hidden variable*. In this case, Alice and Bob win with the following probability:

$$\mathbb{P}\Big(\text{win at CHSH}\Big) \;=\; \sum_{x,y\in\{0,1\}} \frac{1}{4} \int_{\lambda\in\Lambda} \sum_{a,b\in\{0,1\}} \mathbb{1}_{a\oplus b=x\wedge y}\, \mathbb{P}_A(a \,|\, x, \lambda)\, \mathbb{P}_B(b \,|\, y, \lambda)\, \mu(\lambda),$$

for some probability space (Λ, μ) and some conditional probability measures $\mathbb{P}_A$ and $\mathbb{P}_B$, which are Alice's and Bob's respective strategies. For the sake of generalization to nonlocal boxes (see later), we may write

$\mathtt{P}(a,b\,|\,x,y) := \int_\lambda \mathbb{P}_A(a\,|\,x,\lambda)\,\mathbb{P}_B(b\,|\,y,\lambda)\,\mu(\lambda)$ their joint strategy from the referee's point of view, and we simply obtain:

$$\mathbb{P}\Big(\text{win at } \mathtt{CHSH}\Big) = \sum_{x,y,a,b\in\{0,1\}} \underbrace{\tfrac{1}{4}}_{\substack{\text{proba. of}\\ \text{questions}}} \underbrace{\mathtt{P}(a,b\,|\,x,y)}_{\text{strategy}} \underbrace{\mathbb{1}_{a\oplus b=x\wedge y}}_{\text{rule}}. \tag{3}$$

Obviously, the set of classical strategies contains the one of deterministic strategies, so the maximal probability is at least as well as before. But is can be shown that those strategies are limited by the same bound $\boxed{75\%}$ at CHSH as before: indeed $\mathcal{L}$ is the convex hull of deterministic strategies, so the maximal probability of winning must be the same as in the deterministic case since this maximum is attained at an extremal point. This limitation is called CHSH inequality [CHSH69], it is one of Bell's inequalities limiting locality.

Quantum Strategies $\mathcal{Q}$. Going even further, Alice and Bob can make quantum strategies by sharing an entangled state. The set $\mathcal{Q}_{\text{finite}}$ is defined as strategies for which Alice and Bob are respectively allowed to perform a local measurement on some finite-dimensional state, so that the outcomes of their measurement may be part of their strategy. Then $\mathcal{Q}$ is defined as the topological closure of $\mathcal{Q}_{\text{finite}}$, making $\mathcal{Q}$ compact, see [GKW+18, Appendix B] for a precise construction. Although $\mathcal{Q}_{\text{finite}}$ and its closure $\mathcal{Q}$ are known to be different [SLO19, DPP19], in our scenario with two binary measurement we actually have $\mathcal{Q} = \mathcal{Q}_{\text{finite}}$ [GKW+18], which makes it much simpler to understand. The existence in Nature of those quantum correlations has been tested in many experiments, [CS78, AGR82, RKM+01] to name but a few, but many loopholes were found [BCP+14], until recent experiments [HBD+15, SMSC+15] which are hopefully loophole-free. Note that to determine whether a probability distribution is quantum or not, it is also possible to test a hierarchy of semidefinite programming conditions [Weh06, NPA08, DLTW08]. Let us see an example of quantum strategy. Say that Alice and Bob share the following maximally entangled pair:

$$\Omega := \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \in \mathbb{C}\otimes\mathbb{C},$$

denoted with Dirac's notations of kets [Dir39], where $\big\{|0\rangle, |1\rangle\big\}$ is an orthonormal basis of $\mathbb{C}$ (seen as a real vector space). Here is a possible strategy for Alice and Bob using this state. If Alice receives the question $x = 0$, then she measures her share of the state on the canonical basis $\big\{|0\rangle, |1\rangle\big\}$, and if she otherwise receives $x = 1$, then she measures it in the rotated basis $B_\theta := \big\{\cos(\theta)|0\rangle + \sin(\theta)|1\rangle,\, -\sin(\theta)|0\rangle + \cos(\theta)|1\rangle\big\}$ with the angle $\theta = \frac{\pi}{4}$. Similarly, if Bob gets a question $y = 0$, then he measures his share of the state in the basis B_θ with the angle $\theta = \frac{\pi}{8}$, or with the angle $\theta = -\frac{\pi}{8}$ if $y = 1$. After some computations, we obtain the following probabilities:

x	y	$\mathbb{P}(a = b\,\|\,x,y)$	$\mathbb{P}(a \neq b\,\|\,x,y)$
0	0	$\cos^2\left(\frac{\pi}{8}\right)$	(not important)
1	0	$\cos^2\left(\frac{\pi}{8}\right)$	(not important)
0	1	$\cos^2\left(\frac{\pi}{8}\right)$	(not important)
1	1	(not important)	$\cos^2\left(\frac{\pi}{8}\right)$

Then applying the general formula (3) to this strategy, we eventually obtain $\mathbb{P}\big(\text{win at } \mathtt{CHSH}\big) = \cos^2\left(\frac{\pi}{8}\right) \boxed{\approx 85\%.}$ Actually, this value is optimal over all quantum strategies, this is the famous Tsirelson's Bound [Cir80].

Non-Signalling Strategies $\mathcal{NS}$. Those strategies are the most general ones respecting the axiom of *non-signalement*: we authorize Alice and Bob to perform any trick in their strategy as long as causality of information is not violated, *i.e.* they cannot use a faster-than-light communication device [Sha61]. More formally, Alice and Bob are allowed to establish any joint strategy $\mathbb{P}(a,b\,|\,x,y)$ that satisfies the following equations [PR94, Equation (5)]:

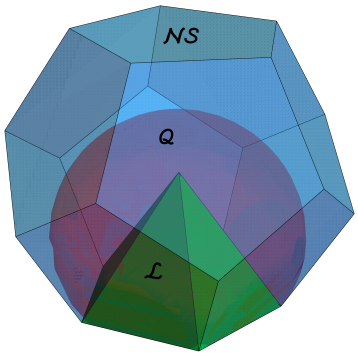
$$\forall a,b,x,y \in \{0,1\}, \qquad \mathbb{P}(a,b\,|\,x,y) \geq 0 \qquad \text{and} \qquad \sum_{a,b} \mathbb{P}(a,b\,|\,x,y) = 1 \tag{4}$$

$$\forall a,x \in \{0,1\}, \qquad \sum_{b\in\{0,1\}} \mathbb{P}(a,b\,|\,x,0) = \sum_{b\in\{0,1\}} \mathbb{P}(a,b\,|\,x,1) \tag{5}$$

$$\forall b,y \in \{0,1\}, \qquad \sum_{a\in\{0,1\}} \mathbb{P}(a,b\,|\,0,y) = \sum_{a\in\{0,1\}} \mathbb{P}(a,b\,|\,1,y). \tag{6}$$

The two equations in (4) are respectively non-negativity and normalization constraints, which are necessary conditions in order to have a well-defined probability measure $\mathbb{P}$, and equations (5) and (6) are the non-signalling contraints, meaning that one party's strategy cannot depend on the question asked to the other party. Later on, we will formalize those general non-signalling strategies with *nonlocal boxes*, and we will observe that they are so powerful that they can reach $\boxed{100\%}$ of victory at CHSH game using the famous PR box. It is known that quantum strategies satisfy this non-signalement axiom (in order to have compatibility between Quantum Mechanics and Special Relativity [PR94, BLM+05]), so that the strict inclusions $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$ hold. Strategies in $\mathcal{NS}\backslash\mathcal{Q}$ are called *post-quantum strategies*. A motivation to study this more general set $\mathcal{NS}$ is that it could provide a better understanding of the nature of quantum correlations $\mathcal{Q}$ as part of a wider set.

Geometry of $\mathcal{L}$ and $\mathcal{Q}$ and $\mathcal{NS}$. The geometry of the non-signalling set $\mathcal{NS}$ has been widely studied in [BLM+05, RDBC19] in many more general cases than ours, not only in the two-party scenario but also in the multi-party scenario, and as well in the case of more than two outputs. In our bipartite case with only two outputs, it is shown that $\mathcal{NS}$ is an 8-dimensional convex polytope, where "dimension" is meant in the sense of the underlying affine space. Indeed $\mathcal{NS}$ is defined by equations (4) and (5) and (6), which are stable under convex combinaison, so $\mathcal{NS}$ is convex. Moreover, those equations tell us that $\mathcal{NS}$ is bounded, closed, and defined by finitely many affine inequalities, so it is a polytope. Finally, the idea for finding the dimension is that $\mathbb{P}(a,b\,|\,x,y)$ could be seen as a $2\times2\times2\times2$ tensor $(\mathtt{T}_{a,b,x,y})$ with real entries, so $\mathcal{NS}$ is included in a vector space $\mathcal{B}$ of dimension 16. But from equations (5) and (6) we can extract $4+4=8$ linearly independent constraints, so that $\mathcal{NS}$ actually lies in a vector space of dimension at most $16-8=8$. Moreover, we can show that its affine dimension could not be lower than 8 by exhibiting nine points that are affinely independent from each other, so that $\mathcal{NS}$ is well of affine dimension 8.



Graphic I.(b) — This is a sketch of how one could think of the sets $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$. Both $\mathcal{L}$ and $\mathcal{NS}$ are convex polytopes, and $\mathcal{Q}$ is convex but not a polytope (since it has an infinite number of extremal points). Sixteen of the twenty-four extremal points of $\mathcal{NS}$ are as well in $\mathcal{L}$. A more faithful representation of these sets would have been in dimension 8 though...

As well as $\mathcal{NS}$, the local set $\mathcal{L}$ is a convex polytope [Pit89, Thm 2-5], [WW01, Section 8]. Indeed, for the same reasons as for $\mathcal{NS}$, the set $\mathcal{L}$ is a polytope whose boundary could be found using the non-negativity constraint (4) and Bell-type inequalities, and $\mathcal{L}$ is convex since it is the convex hull of the deterministic strategies, which are finitely many [GKW+18]. The quantum set $\mathcal{Q}$ was investigated in many references [Cir80, Tsi87, Lan88, WW01, Mas03, Mas06, NPA07], and although it is a fundamental set, surprisingly little is known about its general geometry [Tsi93]. For instance, we know that $\mathcal{Q}$ is convex but not a polytope since it has an infinite amount of extremal points [Pit89]. In [Cab05], "volumes" of $\mathcal{L}$, $\mathcal{Q}$ and $\mathcal{NS}$ are compared, showing that $\mathcal{Q}$ is $(\frac{3\pi}{8})^2 \approx 1.39$ times larger than $\mathcal{L}$ and that $\mathcal{NS}$ is $\frac{32}{3\pi^2} \approx 1.08$ times larger than $\mathcal{Q}$. As for *extremal points*, the convex polytopes $\mathcal{L}$ and $\mathcal{NS}$ share 16 communal extremal points, denoted $\mathtt{P}_{\mathrm{L}}^{\mu,\nu,\sigma,\tau}$, and $\mathcal{NS}$ has 8 additional extremal points $\mathtt{P}_{\mathrm{NL}}^{\mu,\nu,\sigma}$, with parameters $\mu,\nu,\sigma,\tau \in \{0,1\}$, defined as follows [BLM+05, Section 2.B.1], [ABPS09]:

$$\begin{aligned}
&\bullet \text{ Local extremal points:} && \mathtt{P}_{\mathrm{L}}^{\mu,\nu,\sigma,\tau}(a,b\,|\,x,y) &&:= \begin{cases} 1 & \text{if } a=\mu\,x\oplus\nu \text{ and } b=\sigma\,y\oplus\tau, \\ 0 & \text{otherwise,} \end{cases} \\
&\bullet \text{ Nonlocal extremal points:} && \mathtt{P}_{\mathrm{NL}}^{\mu,\nu,\sigma}(a,b\,|\,x,y) &&:= \begin{cases} 1/2 & \text{if } a\oplus b = x\wedge y\oplus\mu\,x\oplus\nu\,y\ \oplus\sigma, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned} \tag{7}$$

Note that in the expression of $\mathtt{P}_{\mathrm{NL}}$ there is no parameter before xy, so that the bit $x\wedge y = (a\oplus\mu\,x\oplus\sigma)\oplus\big(b\oplus\nu\,y\big)$ is of the form of what we will call *distributed bit*, see Subsection II.(2). The correlations $\mathtt{P}_{\mathrm{NL}}$ will be good

examples of *nonlocal boxes*, and this property will be the reason why those nonlocal boxes are so powerful: they turn multiplications into sums, which will cause communication complexity to collapse!

I.(2) NonLocal Boxes

> « *Quantum mechanics is, without any doubt, our best theory of nature.* » [Pop14]

The theoretical notion of *nonlocal boxes* generalizes the notion of strategies or correlations in a convenient way so that they may be efficiently represented in a circuit as gates and therefore they may be easily combined in order to obtain a better strategy. Popescu and Rohrlich were the first to formally introduce this concept with their famous PR box [PR94], see details below.

Definition I.2 (Nonlocal box). *A* box $\mathtt{P}$ *is a function* $\{0,1\}^4 \to \mathbb{R}$ *whose image is denoted* $\mathtt{P}(a,b\,|\,x,y) \in \mathbb{R}$ *for bits* $a,b,x,y \in \{0,1\}$. *We write* $\mathcal{B} = \mathcal{F}\big(\{0,1\}^4, \mathbb{R}\big)$ *the vector space of all boxes. When referring to the case of conditional probabilities as in equations* (3) *to* (6)*, a box* $\mathtt{P}$ *is said* nonlocal *when* $\mathtt{P} \in \mathcal{NS}\backslash\mathcal{L}$*, i.e. it is a non-local non-signalling correlation.*

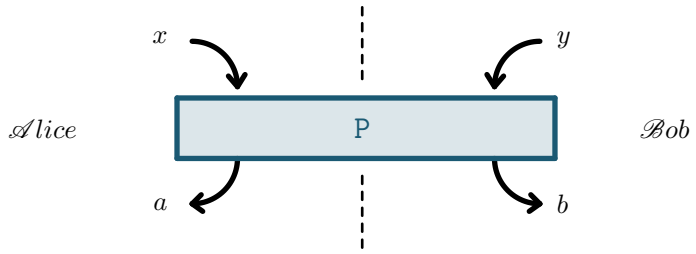


Figure I.(c) — Drawing of a nonlocal box P. Alice has exclusively access to the left side of the box, and Bob exclusively to the right side. If Alice and Bob input respective bits x and y into the box, then the box outputs two bits a and b with probability $\mathtt{P}(a,b\,|\,x,y)$, as if pairs of bits (a,b) were superposed. This model of nonlocal box mimics an entangled state, in the sense that Alice instantly receives her output a right after inputing x, whether or not Bob already inputed his bit y, and from her point of view, her output bit a is uniformly random, locally uncorrelated to anything else, including her own input bit x! [BBL+06]

Find some examples of nonlocal boxes thereafter. We will almost exclusively focus our study on nonlocal boxes, and by abusing the notation we will not always precise "nonlocal" and only say "box" although we will generally mean "nonlocal box".

Advantages of NonLocal Boxes. The benefit of considering boxes is twofold. On the one hand, we may view a nonlocal box as a strategy [Bra11, BCP+14]: in this case, we make the box playing at CHSH (or another game) and we may study its probability of winning at this game. For instance, a quantum state provides a particular box, for which entries determine measurement choices and outputs correspond to measurement outcomes. On the other hand, a nonlocal box can be view as a ressource [BLM+05, Bro16]: in this case, Alice and Bob may have access to arbitrarily many copies of a nonlocal box and use them in their strategy. It is useful to understand boxes as ressources because they have technological application, *e.g.* for device-independent cryptography. For instance, we allow Alice and Bob to connect their boxes with *deterministic wirings* [BS09, ABL+09, LVN14, NGHA15, BG15, GA17, Kar21, EWC22], which will be at the heart of the algebra of boxes that we will introduce in Section III.

Remark I.3 (Link with tensors). Recall that a *tensor* is simply a multi-dimensional array of numbers, whose "dimension" is called *order* of the tensor. For instance, order 1 tensors are vectors (*i.e.* arrays of dimension 1), and order 2 tensors are matrices (*i.e.* arrays of dimension 2). Now, as briefly mentioned earlier, although a box $\mathtt{P}$ is defined as a function above, we may as well see it as an order 4 tensor since it has a finite number of possibility on each of the four entries. More precisely, a box $\mathtt{P}$ may be naturally associated to a $2\times2\times2\times2$ real-valued tensor $\mathtt{T} = \big(\mathtt{T}_{abxy}\big)$ using the relation $\mathtt{T}_{abxy} := \mathtt{P}(a,b\,|\,x,y)$. This point of view based on tensors will be useful to make efficient computations on boxes, see Subsection III.(6).

PR Box. The PR box is undoubtedly the most famous box. It was named after Popescu and Rohrlich who introduced this idea in [PR94, Equation (7)]. They knew that quantum correlations violate CHSH inequality to some extent, but they also knew that this violation was limited from above by Tsirelson's Bound [Cir80]. So their goal was to determine if a stronger violation of CHSH inequality was possible, yet respecting Relativity Theory, *i.e.* considering non-signalling strategies. And this is indeed what they found: the PR box induces a maximal violation of CHSH inequality, or in other words this box wins with 100% of probability at CHSH game. It is defined as follows:

$$\mathtt{PR}(a,b\,|\,x,y) \;:=\; \tfrac{1}{2}\mathbb{1}_{a\oplus b=x\wedge y} \;=\; \begin{cases} \frac{1}{2} & \text{if } a\oplus b = x\wedge y,\\ 0 & \text{otherwise.}\end{cases}$$

Viewing this box as a strategy, we verify that PR satisfying the non-signalling axioms (4) and (5) and (6), so we deduce that $\mathtt{PR}\in\mathcal{NS}$. Moreover, from the definition of the PR box and relation (3), it is straightforward to see that PR wins at CHSH with $\boxed{100\%}$, since the rule of CHSH game is that Alice and Bob win *if, and only if,* $a\oplus b = x\wedge y$. Hence they proved the existence of *post-quantum* correlations, also known as *superquantum* correlations with their own words. A first consequence is that Quantum Mechanics could *not* be deduced solely from the two axioms of (1) relativistic causality and of (2) the existence of a nonlocal correlation. We will see that this box is so powerful that it turns multiplication of entries $x\wedge y$ into sum of the outputs $a\oplus b$, which will cause communication complexity to collapse! Furthermore, it was shown in [BM06] that the PR can simulate some quantum correlations that no entangled pair of qubits can, in our bipartite scenario or more generally even in a multi-party scenario. Note that Tsirelson was already aware of the fact that maximal violation of CHSH inequality is consistent with relativity [KT92].

Remark I.4 (Uniqueness of PR). Besides its existence, it is also possible to show that PR is the *unique* box of $\mathcal{NS}$ that perfectly wins at CHSH game. Indeed, on the one hand, a sharp eye would have noticed that PR is an extremal point of $\mathcal{NS}$ since $\mathtt{PR} = \mathtt{P}_{\mathrm{NL}}^{0,0,0}$, see equation (7) for definitions. Moreover, direct computations lead to the fact that all the other extremal points of $\mathcal{NS}$ win at CHSH with $< 100\%$ of probability. On the other hand, observe that the function $\mathtt{P}\mapsto\mathbb{P}(\mathtt{P}\text{ wins at }\mathtt{CHSH})$ defined in (3) is linear so affine. But an affine map preserves convex combinaisons by definition, so any box of $\mathcal{NS}$ being a convex combinaison of the extremal points must have probability $< 100\%$ at CHSH, except for PR. Thus the uniqueness.

Other Outstanding Boxes. Likewise, we define PR′ as the box that always win at CHSH′ game, whose rule is defined in equation (2). In addition, we define $\overline{\mathtt{PR}}$ and $\overline{\mathtt{PR}'}$ as the boxes that always lose at respectively CHSH and CHSH′. It gives:

$$\begin{aligned}
\mathtt{PR}'(a,b\,|\,x,y) \;&:=\; \tfrac{1}{2}\mathbb{1}_{a\oplus b=(x\oplus 1)\wedge(y\oplus 1)} \;=\; \begin{cases} \frac{1}{2} & \text{if } a\oplus b = (x\oplus 1)\wedge(y\oplus 1),\\ 0 & \text{otherwise.}\end{cases}\\
\overline{\mathtt{PR}}(a,b\,|\,x,y) \;&:=\; \tfrac{1}{2}\mathbb{1}_{a\oplus b=(x\wedge y)\oplus 1} \;=\; \begin{cases} \frac{1}{2} & \text{if } a\oplus b = (x\wedge y)\oplus 1,\\ 0 & \text{otherwise.}\end{cases}\\
\overline{\mathtt{PR}'}(a,b\,|\,x,y) \;&:=\; \tfrac{1}{2}\mathbb{1}_{a\oplus b=(x\oplus 1)\wedge(y\oplus 1)\oplus 1} \;=\; \begin{cases} \frac{1}{2} & \text{if } a\oplus b = (x\oplus 1)\wedge(y\oplus 1)\oplus 1,\\ 0 & \text{otherwise.}\end{cases}
\end{aligned}$$

Next, there are boxes that do not depend on the inputs x and y. First, the *fully mixed* box I [BCP+14] outputs purely random bits a and b. Then consider the *shared randomness* box SR that always answers bits a and b such that $a=b$ [BS09], and its complementary $\overline{\mathtt{SR}}$ that always outputs $a\neq b$. More formally:

$$\begin{aligned}
\mathtt{I}(a,b\,|\,x,y) \;&:=\; \tfrac{1}{4}\\
\mathtt{SR}(a,b\,|\,x,y) \;&:=\; \tfrac{1}{2}\mathbb{1}_{a=b} \;=\; \begin{cases} \frac{1}{2} & \text{if } a=b,\\ 0 & \text{otherwise.}\end{cases}\\
\overline{\mathtt{SR}}(a,b\,|\,x,y) \;&:=\; \tfrac{1}{2}\mathbb{1}_{a\neq b} \;=\; \begin{cases} \frac{1}{2} & \text{if } a\neq b,\\ 0 & \text{otherwise.}\end{cases}
\end{aligned}$$

Finally, here are the two last categories of boxes that will interest us. The *isotropic box* [MAG06, BS09, BG15] of parameter $p\in[0,1]$, denoted p-isoNLB, is defined as the convex combinaison $p\,\mathtt{PR} + (1-p)\,\overline{\mathtt{PR}}$. This is in some sense a noisy version of the perfect box PR, and it wins at CHSH with probability p. The study of those boxes for $p\geq\frac{1}{2}$ will lead us to the open question at the heart of this thesis: we will see in Section II. that communication complexity is nontrivial for $p\leq\cos^2(\frac{\pi}{8})\approx 0.85$ and it is trivial for $p>\frac{3+\sqrt{6}}{6}\approx 0.91$, but we do not know yet what occurs when p is in between. Another kind of noise is given by *correlated boxes* [BS09], denoted p-corNLB and defined as the convex combinaison $p\,\mathtt{PR} + (1-p)\,\mathtt{SR}$, and we will see that these boxes

always make communication complexity to be trivial except when $p = 0$.

$$p\text{-isoNLB} := p\,\mathtt{PR} + (1-p)\,\overline{\mathtt{PR}},$$
$$p\text{-corNLB} := p\,\mathtt{PR} + (1-p)\,\mathtt{SR}.$$

Then, computing the probability of winning at CHSH of each of these boxes with (3), and likely for CHSH′, it yields:

Box P	$\mathtt{P}(a,b\,\vert\,x,y)$	$\mathbb{P}(\mathtt{P}$ wins at CHSH$)$	$\mathbb{P}(\mathtt{P}$ wins at CHSH′$)$
I	$1/4$	$1/2$	$1/2$
SR	$\frac{1}{2}\mathbb{1}_{a=b}$	$3/4$	$3/4$
$\overline{\mathtt{SR}}$	$\frac{1}{2}\mathbb{1}_{a\neq b}$	$1/4$	$1/4$
PR	$\frac{1}{2}\mathbb{1}_{a\oplus b=x\wedge y}$	1	$1/2$
$\overline{\mathtt{PR}}$	$\frac{1}{2}\mathbb{1}_{a\oplus b=xy\oplus 1}$	0	$1/2$
PR′	$\frac{1}{2}\mathbb{1}_{a\oplus b=(x\oplus 1)\wedge(y\oplus 1)}$	$1/2$	1
$\overline{\mathtt{PR}'}$	$\frac{1}{2}\mathbb{1}_{a\oplus b=(x\oplus 1)\wedge(y\oplus 1)\oplus 1}$	$1/2$	0
p-isoNLB	$p\,\mathtt{PR} + (1-p)\,\overline{\mathtt{PR}}$	p	$1/2$
p-corNLB	$p\,\mathtt{PR} + (1-p)\,\mathtt{SR}$	$(p+3)/4$	$(-p+3)/4$

Table I.(d) — Summary of the definition and probabilities at CHSH and CHSH′ games for some outstanding boxes.

Remark I.5 (Extremal points of $\mathcal{NS}$). We saw in Remark I.4 that PR is an extremal point of $\mathcal{NS}$. Similarly, the boxes PR′, $\overline{\mathtt{PR}}$ and $\overline{\mathtt{PR}'}$ are a well an extremal points of $\mathcal{NS}$ since we have $\mathtt{PR}' = \mathtt{P}_{\mathrm{NL}}^{1,1,1}$ and $\overline{\mathtt{PR}} = \mathtt{P}_{\mathrm{NL}}^{0,0,1}$ and $\overline{\mathtt{PR}'} = \mathtt{P}_{\mathrm{NL}}^{1,1,0}$. Nevertheless, observe that SR is not an extremal point since it could be written as the non-trivial convex combinaison $\mathtt{SR} = \frac{1}{2}\mathtt{P}_0 + \frac{1}{2}\mathtt{P}_1$ with $\mathtt{P}_0 = \mathtt{P}_{\mathrm{L}}^{0000}, \mathtt{P}_1 = \mathtt{P}_{\mathrm{L}}^{0101} \in \mathcal{L} \subseteq \mathcal{NS}$.

Example I.6 (Signalling box). The box that always give a and b such that $a \wedge b = x \wedge y$ uniformly is not in $\mathcal{NS}$ since it does not satisfies (5).

The CHSH–CHSH′ Slice. Recall that $\mathcal{NS}$ is a convex polytope of dimension 8 (see page 6), so it does admit a very convenient representation in drawings, but we can study some of its slices. By "slice" we mean an affine plane of the vector space $\mathcal{B}$ of boxes (or the intersection of $\mathcal{NS}$ with this affine plane). More particularly, we call CHSH–CHSH′ slice the slice containing the three non-aligned points PR, PR′ and I. This slice has been investigated in [Bra11, BCP+14, CLB+15], and in this slice it shown that the sets $\mathcal{L} \subseteq \mathcal{Q} \subseteq \mathcal{NS}$ have appealing shapes: $\mathcal{Q}$ is a disk sandwiched between the squares $\mathcal{L}$ and $\mathcal{NS}$, see Diagram I.(e). Additionally, we projected some boxes into the CHSH–CHSH′ although they do not belong to this slice. For instance the box SR is projected to the point of coordinates $\left(\frac{3}{4}, \frac{3}{4}\right)$, which corresponds to its probability of winning at respectively CHSH′ and CHSH (see Table I.(d)), although PR $\notin$CHSH–CHSH′ slice. Note that many other slices have been studied in [GKW+18].

Remark I.7 (Noteworthy local boxes). As we can see on Diagram I.(e), although PR and PR′ are not local, their middle point, which has coordinates $\left(\frac{3}{4}, \frac{3}{4}\right)$, is local. Indeed, when we compute its expression, we obtain that it is the iso-barycentre of four local boxes:

$$\frac{\mathtt{PR} + \mathtt{PR}'}{2} = \frac{\mathtt{P}_{\mathrm{L}}^{0000} + \mathtt{P}_{\mathrm{L}}^{0101} + \mathtt{P}_{\mathrm{L}}^{1011} + \mathtt{P}_{\mathrm{L}}^{1110}}{4},$$

so this middle point is local by convexity of $\mathcal{L}$. Similarly, the box $\frac{3}{4}$-isoNLB, at the coordinates $\left(\frac{1}{2}, \frac{3}{4}\right)$ is in $\mathcal{L}$ since it could be written as the iso-barycentre of height local extremal points. Note that the segment joining PR and $\overline{\mathtt{PR}}$ and the one joining SR and $\overline{\mathtt{SR}}$ have their middle point in common, which is the box $\mathtt{I} \in \mathcal{L}$, so that we have the relation $\frac{\mathtt{PR}+\overline{\mathtt{PR}}}{2} = \frac{\mathtt{SR}+\overline{\mathtt{SR}}}{2} = \mathtt{I}$. This makes sense as regards Diagram I.(e).

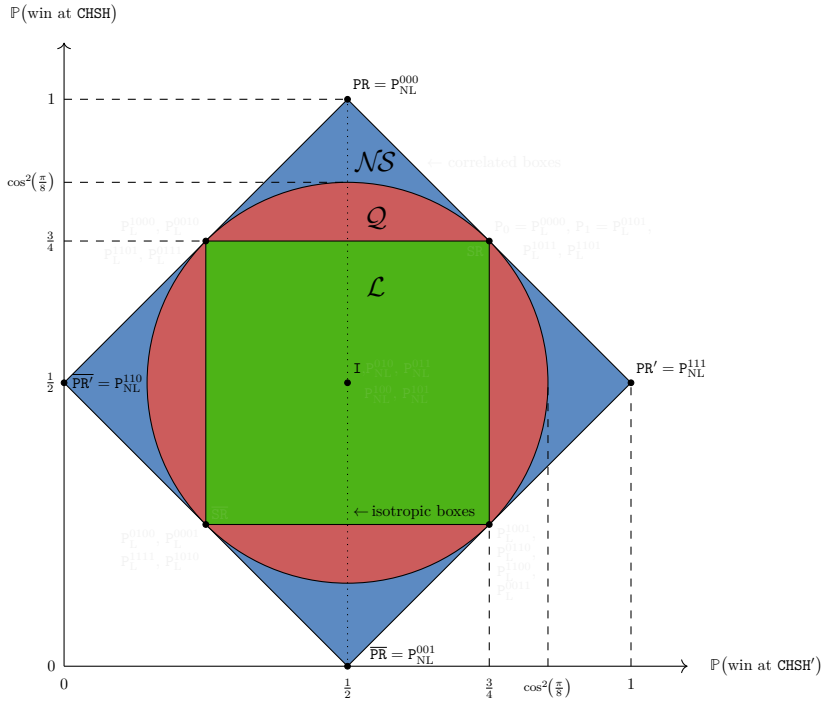


Diagram I.(e) — The 2-dimensional CHSH–CHSH′ slice of the 8-dimensional polytope $\mathcal{NS}$ [Bra11, Figure 1], [BCP+14, Figure 4], [CLB+15, Figure 3]. This slice contains all the points drawn in black. Additionally, in very transparent font are represented the projection of some other boxes into this plane. Recall the definition of extremal points $\mathsf{P_L}$ and $\mathsf{P_{NL}}$ in (7).

I.(3) The Key Tool: Communication Complexity

> « *Most computer scientists would consider a world in which communication complexity is trivial to be as surprising as a modern physicist would find the violation of causality.* » [BBL+06]

Communication complexity could be seen as the difficulty for Alice and Bob to compute the value $f(X,Y)$ for some function f, with the least amount of communication possible, where X is known by Alice and Y by Bob, provided they have access to some shared ressource such as a nonlocal box. It was introduced by the computer scientist Yao in [Yao79], developed in [Tho79, Kus97, CB97] among many, and reviewed in [KN96, RY20].

Why Studying Communication Complexity? Given a non-signalling correlation (a nonlocal box), we want to determine a criterion that tells us whether or not the correlation is quantum. In Physics, there is the idea that limitations observed in Nature often emerge from physical principles. For instance the boundary of the non-signalling set $\mathcal{NS}$ emerges for the principle that no information can be transmitted faster than the speed of light, which is a consequence of Einstein Special Relativity theory [Ein05b]. So now, we want to characterize the set $\mathcal{Q}$ with a new expression, not written in terms of operators in some Hilbert space as it is until this day, so that it becomes a new axiom of Quantum Mechanics. As said earlier, the fact that $\mathcal{NS}$ is strictly bigger than $\mathcal{Q}$ imply that Quantum Mechanics could *not* be deduced solely from the two simple axioms of (1) relativistic causality and of (2) the existence of a nonlocal correlation, something is missing. Numerous directions to finding the remaining axiom are closed because $\mathcal{NS}$ and $\mathcal{Q}$ have manifold properties in common [ABPS09]: *no-cloning* [MAG06, Bar07], *no-broadcasting* [BBLW07], *monogamy of correlations* [MAG06], *information-disturbance trade-offs* [SGB+06], *secure key distribution* [BHK05, AGM06] and *quantumlike dynamical processes* [SBP09]. Many attempts are still in process, and they have been listed and reviewed by Popescu (one of the co-authors of the PR box) in [Pop14]: *nonlocal computation*

[LPSW07], *information causality* [PPK+09], *macroscopic locality* [NW09], *local orthogonality* [FSA+13], *non-locality swapping* [SBP09], *many-box locality* [ZCB+17], and last but not least, *communication complexity* [vD99, Bra05, BBL+06, BS09, BCMdW10, SWH20]. However, none of them has been shown to perfectly single out $\mathcal{Q}$. In this report, we choose to focus on communication complexity because this criterion seems the most promising one due to its precision near the SR box [BS09], see Subsection II.(4).

Communication Complexity Game. We need to introduce the scenario of *communication complexity game* [Yao79]. First, as Alice and Bob are preparing together their strategy, the referee sends them a Boolean function $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$. Then, the game begins and Alice and Bob are geographically separated. Assume that they are allowed to exchange classical bits during the game but consider that this trade-off is costly, so that they want to communicate as few bits as possible. The referee provide Alice with a string $X = (x_1, \dots, x_n) \in \{0,1\}^n$ and Bob with a string $Y = (y_1, \dots, y_m) \in \{0,1\}^m$. As Alice and Bob play, the referee counts the number of bit exchanged between them. At the end of the game, Alice have to answer the referee with a bit $a \in \{0,1\}$, and the referee declares that they won *if, and only if,* $a = f(X,Y)$ (this is the rule of the game). We will say that communication complexity is the minimal number of bits exchanged in order to win, independently of the string X and Y, as follows:

Definition I.8 (Communication complexity of a function)**.** *The* (probabilistic) communication complexity $\boxed{\mathtt{CC}_p(f)}$ *of a Boolean function* $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ *is the minimal number of bits such that, for any strings* $X \in \{0,1\}^n$ *and* $Y \in \{0,1\}^m$ *chosen by the referee, Alice and Bob exchange at most this number of bits and Alice knows the value* $f(X,Y) \in \{0,1\}$ *with probability at least* p*.*

If Alice and Bob use a ressource R in this communication complexity game, for example a nonlocal box, then communication complexity is denoted $\boxed{\mathtt{CC}_p^{\mathtt{R}}(f)}$. For exemple, Cleve and Buhrman introduced the notion of *prior entanglement* [CB97, BCvD01], which is the particular case of when the ressource $\mathtt{R} \in \mathcal{Q}$ is quantum, so we denote $\mathtt{CC}_p^{\mathcal{Q}}(f)$. Prior entanglement often helps to enhance results: some functions can be computed with exponentially less communication than with with ressources $\mathtt{R} \in \mathcal{L}$ [BCW98].

Remark I.9 (Quantum communication complexity). Note that there exists as well a *quantum* version of communication complexity [Yao93, dW02, Bra03, CvDNT13], in which Alice and Bob exchange qubits instead of bits, it is shown that for some problems the amount of communication required in the quantum world is considerably less than the amount of classical communication. This quantum version will be useful in Subsection II.(1).

Example I.10 (Sum). Consider $f(x_1, x_2; y_1, y_2) := x_1 \oplus y_1 \oplus x_2 \oplus y_2 \oplus 1$. First, note that f depends on y_j's, so at least one bit needs to be exchanged. Now, when they prepare their strategy, Alice and Bob could have the brilliant idea to write $f(x_1, x_2; y_1, y_2) = [x_1 \oplus x_2] \oplus [y_1 \oplus y_2 \oplus 1]$. When the game starts, Bob may perform the local sum $y_1 \oplus y_2 \oplus 1$ and then send the result to Alice, so that Alice knows the value $f(x_1, x_2; y_1, y_2)$ by figuring out the sum of $x_1 \oplus x_2$ and the bit she received from Bob. Hence one bit is sufficient in the trade-off, so $\mathtt{CC}_1(f) = 1$.

Example I.11 (Local multiplications). Consider $g(x_1, x_2; y_1, y_2) := [x_1 \wedge x_2] \oplus [y_1 \wedge y_2]$. As in the previous example, on the one hand Alice and Bob need to exchange at least a bit, and on the other hand Bob can perform the product $y_1 \wedge y_2$ and send the result to Alice so that they win the game with only one bit in the trade-off. Hence again $\mathtt{CC}_1(g) = 1$. More generally, any sum of local operations has communication complexity ≤ 1.

Example I.12 (Nonlocal multiplications). Consider $h(x_1, x_2; y_1, y_2) := [x_1 \wedge y_1] \oplus [x_2 \wedge y_2]$. Now the situation is trickier because each multiplication depends on x_i's and y_j's. Note that two bits of trade-off are enough since Bob can send y_1 and y_2 separately to Alice, so that $\mathtt{CC}_p(f) \leq 2$ for any $p \leq 1$. Now, here is the strategy Alice and Bob could establish: if Bob receives $y_1 = y_2 = 0$, then he send 0 to Alice and she knows that $h(x_1, x_2; y_1, y_2)$. Otherwise, Bob send 1 to Alice and Alice answer a uniform random bit r to the referee, so that in this case they win with 50% probability. At the end of the day, with this strategy, they win with probability $\mathbb{P}(\text{win}) = \mathbb{P}(y_1 = y_2 = 0) \times 1 + \mathbb{P}(y_1 \neq 0 \text{ or } y_2 \neq 0) \times \frac{1}{2} = \frac{5}{8}$. Hence $\mathtt{CC}_{5/8}(h) = 1$, but it can be shown that $\mathtt{CC}_1(h) = 2$.

Remark I.13 (Majoration on CC). We naturally always have:

$$\mathtt{CC}_p^{\mathtt{R}}(f) \leq m, \qquad \text{and} \qquad p \leq \tfrac{1}{2} \implies \mathtt{CC}_p^{\mathtt{R}}(f) = 0.$$

Indeed, the first inequality can be deduced from the naive strategy of Bob sending all his bits $y_1, \dots, y_m$ separately to Alice. The second inequality simply yields from the strategy of Alice randomly answering a bit to the referee, independently of the x_i's and y_j's. This strategy wins with 50% probability for any Boolean function f.

Trivial Communication Complexity. We say a ressource $\mathtt{R}$ induces *trivial communication complexity* when:

$$\exists p > \tfrac{1}{2}, \quad \forall n, \forall m, \forall f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}, \qquad \mathtt{CC}_p^{\mathtt{R}}(f) \leq 1. \tag{8}$$

Otherwise, it is said *non-trivial*. The value $\frac{1}{2}$ was chosen in view of Remark I.13.

Remark I.14. It suffices to study the case $n = m$, *i.e.* the case of Boolean functions with same-size entry strings $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, since otherwise we can complete the shortest string with zeroes.

Remark I.15. In our approach, when we say that we use a ressource $\mathtt{R}$, we mean that we can use arbitrarily many copies of this ressource. In [KKLR09], the authors estimate the minimal number of nonlocal boxes needed to compute a function f.

Definition I.16 (Trivial box)**.** *A nonlocal box* $\mathtt{P}$ *is said to be* trivial *(in the sense of communication complexity) when, as a ressource, it induces trivial communication complexity.*

In next section, we will see that all quantum boxes are non-trivial, and we will see as well some examples of post-quantum boxes that are trivial. For instance, the PR box is trivial. Actually, it is conjectured that all post-quantum boxes are trivial; this is the open question that we try to answer in the present report.

II. Historical Overview

In this section, we present what is known about the link between nonlocal boxes and communication complexity. See below a diagram that recaps historical advances. We zoomed in at the top-right corner of the CHSH–CHSH′ slice defined in Diagram I.(e), and we projected the box SR in this plane at coordinates $\left(\frac{3}{4}, \frac{3}{4}\right)$ even if it is not a convex combinaison of PR, PR′ and I. We drawn in red boxes that are known to be **non-trivial**, *i.e.* quantum boxes, and in purple boxes that are know to be **trivial**.

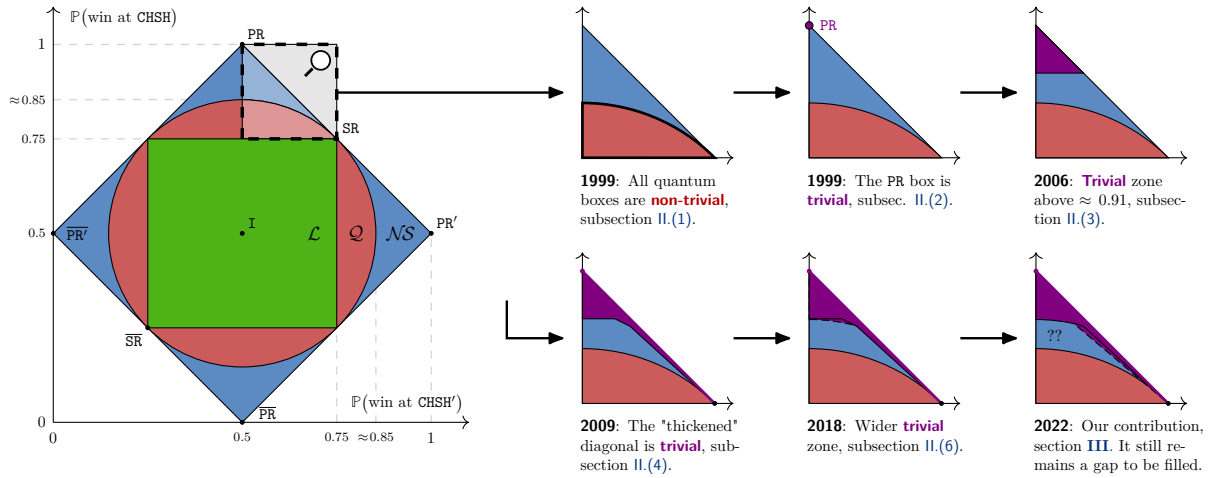


Figure II.(a) — The different historical steps in order to show the conjecture that quantum boxes are *non-trivial* and that post-quantum boxes are *trivial*.

II.(1) 1999: Quantum Boxes are Non-Trivial

In this subsection, we present the idea of the first proof that quantum correlations induce *non-trivial* communication complexity. This result is due to Richard Cleve, Wim van Dam, Michael Nielsen and Alain Tapp [CvDNT99, Section 4]. As the definition of *trivial communication complexity* must hold for any Boolean

function, see equation (8), it suffices to disclose a counter-example if we want to show it is non-trivial. This is what they did, with the *inner product* function:

$$\mathtt{IP}_n\Big(x_1,\dots,x_n;\,y_1,\dots,y_n\Big) := x_1\wedge y_1\oplus\cdots\oplus x_n\wedge y_n, \tag{9}$$

where recall that $\wedge$ denotes the product and $\oplus$ the sum modulo 2. What they show is that communication complexity of $\mathtt{IP}_n$ is of the order $\mathtt{CC}_p^{\mathcal{Q}}(f)=\mathcal{O}(n)$, where the $\mathcal{Q}$ in exponent means that we allow Alice and Bob to have access to prior entanglement [CB97, BCvD01], which therefore tells that communication complexity could not be trivial with quantum ressources! Note that it was already known that $\mathtt{CC}_p^{\mathcal{L}}(\mathtt{IP}_n)=\mathcal{O}(n)$ [CG88, KN96], so the new result of [CvDNT99] subsumes this result because $\mathtt{CC}_p^{\mathcal{L}}(\mathtt{IP}_n)\geq\mathtt{CC}_p^{\mathcal{Q}}(\mathtt{IP}_n)$, or in other words *if you can move mountains you can move molehills.*

Key Ideas. *First, they show the result for* quantum communication complexity*, which generalizes classical communication complexity in the sense that Alice and Bob can communicate not only bits but also* qubits*. Then, they simulate a bit-protocol with a qubit-protocol to obtain the result for classical communication complexity.*

This notion of *quantum communication complextiy* was introduced by Yao [Yao93]. Let us denote $\mathtt{Q}_p^{\mathtt{R}}(f)$ the quantum communication complexity of f, where Alice and Bob can use the ressource $\mathtt{R}$, and where Alice has to successfully know $f(X,Y)$ with at least probability p. It was already known that $\mathtt{IP}_n$ has quantum communication complexity of order $\mathtt{Q}_p(\mathtt{IP}_n)=\mathcal{O}(n)$ for any $p>\frac{1}{2}$ [Kre95], but this result does not hold for allowance to quantum ressources. In particular, the new proof of [CvDNT99] subsumes the latter since $\mathtt{Q}_p(\mathtt{IP}_n)\geq\mathtt{Q}_p^{\mathcal{Q}}(\mathtt{IP}_n)$.

Theorem II.1 (Quantum boxes are non-trivial, [CvDNT99]). *For $\frac{1}{2}<p\leq 1$, we have:*

$$\begin{aligned}\mathtt{Q}_1^{\mathcal{Q}}\big(\mathtt{IP}_n\big)&=\lceil n/2\rceil \quad &&\text{and} \quad &\mathtt{Q}_p^{\mathcal{Q}}\big(\mathtt{IP}_n\big)&\geq \tfrac{1}{2}\left(2p-1\right)^2 n-\tfrac{1}{2},\\ \mathtt{CC}_1^{\mathcal{Q}}\big(\mathtt{IP}_n\big)&=n \quad &&\text{and} \quad &\mathtt{CC}_p^{\mathcal{Q}}\big(\mathtt{IP}_n\big)&\geq \max\Big(\tfrac{1}{2}\left(2p-1\right)^2,\left(2p-1\right)^4\Big) n-\tfrac{1}{2}.\end{aligned}$$

For instance, for the first equality, on the one hand we have the inequality "$\leq$" using a *superdense coding* technique [BW92]: by sending $\lceil n/2\rceil$ qubits in conjunction with $\lceil n/2\rceil$ EPR pairs, Bob can transmit her n classical bits of input to Alice, enabling her to evaluate $\mathtt{IP}_n$ because she knows Bob's string. On the other hand, for the "$\geq$" inequality, they apply a corollary of Holevo's Theorem [Hol73], [CvDNT99, Thm 1].

Then, they prove the results for $\mathtt{CC}$ using the ones for $\mathtt{Q}$. Again by *superdense coding*, the idea is that, given an m-bit protocol for $\mathtt{IP}_n$, one can construct an m-qubit protocol for $\mathtt{IP}_{2n}$. So the first equation of the theorem gives $m\geq\mathtt{Q}_1^{\mathcal{Q}}\big(\mathtt{IP}_{2n}\big)=\lceil 2n/2\rceil=n$. Hence the first equality for $\mathtt{CC}$ because we know as well that it is $\leq n$, see Remark I.13. The inequality with $\mathtt{CC}$ is obtain with the same reasoning, and using additionally the fact that $\mathtt{CC}_p(f)\geq\mathtt{Q}_p(f)$ for any f and p. Hence the result.

II.(2) 1999: The PR Box is Trivial

> « *The solution of all possible distributed functions with a single bit of communication surely does contradict our experiences in computer science.* » [vD99]

In this subsection, we present the original proof of Wim van Dam, one of the co-authors of the previous subsection result, that the PR box is trivial from his Ph.D. thesis [vD99, Chapter 9]. Note that [BBL+06] mentions that this result was as well independently shown by Cleve, another co-author from previous subsection. Van Dam's result may be expressed in terms of our notations, see equation (8), with probability $p=1$ and ressource $\mathtt{R}=\mathtt{PR}$ and Remark I.14:

Theorem II.2 (The PR box is trivial). *A single bit of communication is enough for Alice to compute any Boolean function:*

$$\forall n, \quad \forall f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}, \qquad \boxed{\mathtt{CC}_1^{\mathtt{PR}}(f) \leq 1}.$$

Key Ideas. *Given a Boolean function f and arbitrarily many copies of the* PR *box, (1) Alice and Bob first write $f(X,Y)$ as a sum of nonlocal multiplications, then (2) they turn each nonlocal multiplication into a sum using a* PR *box, and finally (3) Bob locally computes the sum of his bits and sends his result to Alice so that she knows the value $f(X,Y)$ with* only one bit of communication. *The three steps are developed below.*

(0) Distributed Bits. A preliminary clever remark is to try to write the value $f(X,Y)$ as a *distributed bit*. A bit $c \in \{0,1\}$ is said to be *distributed* between Alice and Bob if it could be written as the sum:

$$c = a \oplus b,$$

where Alice knows $a \in \{0,1\}$ and Bob $b \in \{0,1\}$. If a bit c is distributed, then it suffices for Bob to send b to Alice and Alice knows the bit c. Hence, if Alice and Bob are able to write values of f as a distributed bit $f(X,Y) = a_X \oplus b_Y$, then f could be computed by Alice with *only one bit exchanged*. When such a decomposition of f exists for any strings X and Y, we say that f is *distributively computed*. In particular, this is the idea that was behind examples I.10 and I.11 of previous section.

(1) Algebraic Normal Form. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ a Boolean function, and consider strings $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ in $\{0,1\}^n$. Key idea number (1) comes back to writing f as an inner product function as defined in equation (9). To do so, using a similar technique as for *lagrange interpolation polynomial*, first see that f is exactly a polynomial over $\mathbb{Z}/2\mathbb{Z}$:

$$f(X,Y) = \bigoplus_{X',Y' \in \{0,1\}^n} \underbrace{f\big(x'_1, \ldots, x'_n, y'_1, \ldots, y'_n\big)}_{\text{scalar}} \underbrace{\big[x_1 - x'_1 + 1\big] \cdots \big[x_n - x'_n + 1\big] \big[y_1 - y'_1 + 1\big] \cdots \big[y_n - y'_n + 1\big]}_{=1 \text{ if and only if } X' = X \text{ and } Y' = Y},$$

where $X' = (x'_1, \ldots, x'_n)$ and $Y' = (y'_1, \ldots, y'_n)$ are strings of $\{0,1\}^n$, and we recall that $\oplus$ is the mod-2 sum. After developing and re-ordering terms, we obtain the *algebraic normal form* of f:

$$\boxed{f(X,Y) = \bigoplus_{i=1}^{2^n} P_i(X)\, Q_i(Y)},$$

where $P_i \in \mathbb{Z}/2\mathbb{Z}[x_1, \ldots, x_n]$ is some polynomial, and Q_i is a polynomial of the form $Q_i(Y) = \prod_{j \in S_i} y_j$ for some subset $S_i \subseteq \{1, \ldots, n\}$. Note that the above sum index i goes until 2^n as it is the number of subsets of $\{1, \ldots, n\}$. Hence we showed that f could be written in terms of the inner production function $\mathtt{IP}_{2^n}$.

(2) Use some PR boxes. Alice and Bob have access to as many copies of the PR box as they want. Here we will use 2^n PR boxes, where n is fixed as the entry strings size of the given function f. Let $1 \leq i \leq 2^n$. Knowing all the bits of the string X, Alice may locally compute the value $P_i(X)$ and she inputs it her share of the PR box. Similarly, Bob inputs the value $Q_i(Y)$ in his share. The nonlocal box PR then provide Alice and Bob with respective bits α_i and β_i such that $P_i(X)\, Q_i(Y) = \alpha_i \oplus \beta_i$ with probability 100%. It turns out that $f(X,Y)$ is now of the form of a distributed bit:

$$f(X,Y) = \bigoplus_{i=1}^{2^n} (\alpha_i \oplus \beta_i) = \underbrace{\Big(\bigoplus_{i=1}^{2^n} \alpha_i\Big)}_{\text{Alice's side}} \oplus \underbrace{\Big(\bigoplus_{i=1}^{2^n} \beta_i\Big)}_{\text{Bob's side}}.$$

(3) Alice computes the value. As the bit $f(X,Y)$ is distributed, we conclude as in point (0) that Alice can compute $f(X,Y)$ onces she receives the bit $b = \bigoplus_i \beta_i$ from Bob. Hence the result that any Boolean function f is computed by Alice with at most one bit exchanged.

II.(3) 2006: Boxes above ≈ 0.91 are Trivial

> « *A proof that nontrivial communication complexity forbids nonlocal boxes to be approximated with probability greater than* [85.4%] *would be very interesting, as it would render Tsirelson's bound inevitable, making it a candidate for a new information-theoretic axiom for quantum mechanics.* » [BBL+06]

In this section, now that we know that the PR box is trivial, we present an article showing that noisy PR boxes are as well trivial until the error rate threshold $\frac{3+\sqrt{6}}{6} \approx 0.91$ [BBL+06]. It gives the triangle-shape trivial zone of Figure II.(a). This work is due to Gilles Brassard, Harry Buhrman Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger.

Remark II.3 (Isotropic boxes). In particular, isotropic boxes, which are defined as convex combinaison of PR and its opposite $\overline{\texttt{PR}}$, give an interesting type of noise: p-isotropic box with $p \geq 0.5$ are *non-trivial* for $p \leq \cos^2\left(\frac{\pi}{8}\right) \approx 0.85$ by Tsirelson's bound, whereas they are *trivial* for $p > \frac{3+\sqrt{6}}{6} \approx 0.91$. Those isotropic boxes are important, because it was shown that if a p-isotropic box is trivial, then any box $\texttt{P} \in \mathcal{NS}$ wining at CHSH game with probability p is also trivial [MAG06, Appendix A]. This process is called *depolarization*. However, in the gap between ≈ 0.85 and ≈ 0.91, communication complexity behavior is still unknown to this day...

Key Ideas. *Authors' idea is first (1) to distributively compute* any *given Boolean function with a protocol that do* not *involve communication between Alice and Bob, up to some error probability. Then (2) they use the* majority function *to boost the probability of having a good result at step (1). The steps are detailed below.*

Theorem II.4 (Boxes above ≈ 0.91 are trivial)**.** *If a non-signalling box* $\texttt{P} \in \mathcal{NS}$ *wins at* CHSH *game with probability* $p > \frac{3+\sqrt{6}}{6} \approx 91\%$*, then the box* P *is trivial.*

(1) Distributed Computation. As it was the case in van Dam's protocol to show that the PR box is trivial in previous subsection, the authors use here the notion of distributed computation. Find the definition of *distributively computed* function f at page 14. Their idea is to show that *any Boolean function* $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ *can be distributively computed with probability* $> 1/2$*, without communication between Alice and Bob.* Indeed, here is such a protocol. Assume Alice and Bob share a uniformly random string $z \in \{0,1\}^m$ of same size as Bob's strings. Alice strategy is simple: upon receiving her string x, she answers the bit $a = f(x,z)$. As for Bob, it depends on his question string y: in the lucky event that $y = z$ which happens with probability $\frac{1}{2^m}$, he answers $b = 0$; otherwise he answers a uniformly random bit $y = r \in \{0,1\}$. At the end of the day, we have the claimed result:

$$\mathbb{P}\Big(f(x,y) = a \oplus b\Big) \;=\; \tfrac{1}{2^m} \times 1 + \big(1 - \tfrac{1}{2^m}\big) \times \tfrac{1}{2} \;=\; \boxed{\tfrac{1}{2} + \tfrac{1}{2^{m+1}}} \;>\; \tfrac{1}{2}.$$

(2) Majority Function. The *majority function* $\texttt{Maj} : \{0,1\} \times \{0,1\} \times \{0,1\} \to \{0,1\}$ is the Boolean function that outputs the most appearing bit among its three entry bits. For instance $\texttt{Maj}(1,1,1) = 1$ and $\texttt{Maj}(0,1,0) = 0$. The idea is to use this function to correct, to some extent, errors generated by the noise. We want to boost the probability of distributively computing f. We saw that Alice and Bob have a protocol to successfully write $f(x,y) = a \oplus b$ with probability $p_0 = \frac{1}{2} + \frac{1}{2^{m+1}}$, without communication. Image they apply this protocol three times independently. They obtain some pairs $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ such that $f(x,y) = a_i \oplus b_i$ with probability p_0 for each i. To boost the success probability p_0, Alice and Bob may try to distributively compute the majority function of the $a_i \oplus b_i$, *i.e.* they may seek bits a and b such that:

$$a \oplus b = \texttt{Maj}\Big(a_1 \oplus b_1,\, a_2 \oplus b_2,\, a_3 \oplus b_3\Big).$$

This problem is called *nonlocal majority problem.*

Lemma II.5 ([BBL+06, Lemmata 2 and 3])**.** *If Alice and Bob know a protocol to solve the nonlocal majority problem with probability* $q > \frac{5}{6}$*, then communication complexity is trivial.*

Lemma II.6 ([BBL+06, Lemmata 4 and 5]). *Nonlocal majority problem can solved with probability* $p^2+(1-p)^2$*, provided Alice and Bob have access to two copies of a box* $\mathtt{P} \in \mathcal{NS}$ *that wins at* CHSH *game with proba.* p*.*

Proof. (Theorem II.4). Combining the two previous lemmata, we see that communication complexity is trivial whenever p satisfies $p^2+(1-p)^2 > \frac{5}{6}$, which is equivalent to $p > \frac{3+\sqrt{6}}{6}$ or $p < 1-\frac{3+\sqrt{6}}{6}$, thus the result. □

Remark II.7 (Optimality). In this proof, the authors used the majority function with 3 input bits. There exists a more general notion of majority function with n input bits, and we may wonder if it could help to boost better the result. However [Mor16, Theorem 25] shows that the threshold $\frac{3+\sqrt{6}}{6} \approx 91\%$ is not enhanced, for any $n \geq 3$. Actually, the author even shows that no Boolean function in the boosting process, among a large class of functions, leads to a better result than this threshold!! Similarly [SWH20] shows this optimality of $\approx 91\%$ for another large class of functions. Find more details in Subsection II.(5).

II.(4) 2009: Correlated Boxes are Trivial

> « *This result provides a partial answer to the question of why quantum nonlocality is also bounded below Tsirelson's bound, in regions of the polytope close to the local set of correlations.* » [BS09]

In this subsection, we present the result that correlated boxes are all trivial, except the extremal point SR [BS09]. Recall that correlated boxes are convex combinaisons between PR and SR, and they are projected in the diagonal of the triangle in the CHSH–CHSH′ plane, see Figure II.(a). The result is even stronger than that: the authors numerically draw a positive-width trivial area nearby correlated boxes. This work is due to Nicolas Brunner and Paul Skrzypczyk, and it is based on the result of previous subsection [BBL+06]. We denote $\mathtt{triv}_{\mathrm{BBLMTU}}$ the trivial "triangle-shaped" area that was disclosed in [BBL+06]. We will not go into too much details here because our contribution in Section III. is a generalization of this result, the same ideas will be explained in a more general framework.

Remark II.8. This result is outstanding since the authors find for the first time trivial post-quantum boxes arbitrarily close to the quantum set $\mathcal{Q}$ near SR. This means that, at close near SR, communication complexity seems to be a good criterion to single out quantum correlations!

Key Ideas. *The authors introduce (1) a* distillation protocol *that allow to combine two nonlocal boxes into one new box in a way that, in some favorable cases,* CHSH *wining probability is increased. (2) They use this protocol to show that correlated can be distilled until the trivial area* $\mathtt{triv}_{\mathrm{BBLMTU}}$*, and therefore they are trivial as well. Find more details below.*

Theorem II.9 (Correlated boxes are trivial). *Boxes of the form* $p\,\mathtt{PR}+(1-p)\,\mathtt{SR}$ *are trivial for any* $0 < p \leq 1$*.*

Remark II.10. It is not surprising that SR is not trivial, since $\mathtt{SR} \in \mathcal{L} \subseteq \mathcal{Q}$, see Remark I.5, and we saw in Subsection II.(1) that all quantum boxes are non-trivial.

(1) Distillation Protocol. Given two copies of a box P, they "wire" them in the following way, called *distillation protocol*:

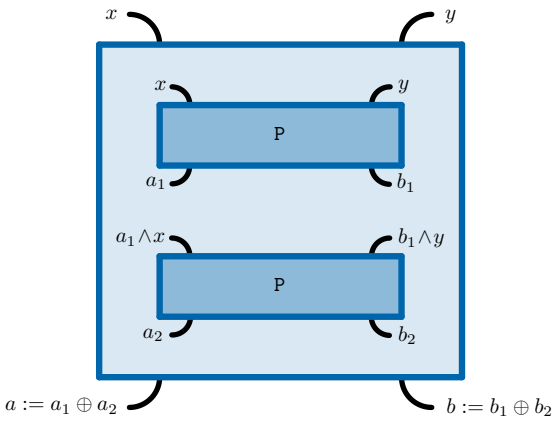


Diagram II.(b) — Distillation protocol of some box $\mathtt{P} \in \mathcal{NS}$. It defines a "bigger" box, called *distilled box* when its CHSH wining probability is greater than the one of P.

Note that the first distillation protocol was defined a bit before the this one, in [FWW09]. Other results about distillation can be found in [DW08, Sho09, ABL+09, EWC22].

(2) Correlated Boxes are Trivial. The idea is to choose a starting correlated box p-corNLB and to repeat this protocol many times. The authors show that the new boxes obtained by this protocol are again correlated boxes and that they eventually reach $\mathtt{triv}_{\mathrm{BBLMTU}}$. As this distillation protocol do *not* increase communication complexity, they deduce that the starting box is trivial, *i.e.* given this box as a ressource, there exists a finite protocol (although potentially very long) such that any Boolean function has trivial communication complexity. Find graphics and more details in our generalized proof in Section **III**.

Remark II.11 (Limitations of this method). It was recently shown in [EWC22] that protocols involving more than two copies of P disclose strictly better results. Although we can marvel the power of distillation protocol, it is shown in [Sho09, BG15] that isotropic boxes *cannot* be distilled into another isotropic box (find more details in **??**Subsection]M-subsection: limiting results), which is a pain since we saw in Remark II.3 that those boxes are really noteworthy. Recall that isotropic are the "vertical" boxes, *i.e.* the convex combinaison between PR and $\overline{\mathtt{PR}}$. However, Proulx found later another method, without using distillation, to show again that correlated boxes induce trivial communication complexity [Pro18].

II.(5) 2015-2020: Limiting Results

> « *The absurdity of a world in which any function could be evaluated by two players with a constant amount of communication in turn provides a tantalizing way to distinguish quantum mechanics from incorrect theories of physics.* » [SWH20]

In this subsection, we present three results showing limitations of some techniques on proving that post-quantum boxes are trivial. It might be good to be aware of limitations in order to have a better intuition.

(1) 2015: Isotropic Boxes cannot be Distilled. We mentioned in Remark II.3 the great interest of considering *isotropic boxes*. Recall that isotropic are the "vertical" boxes, *i.e.* the convex combinaison between PR and $\overline{\mathtt{PR}}$. But Salman Beigi and Amin Gohari showed in [BG15, Theorem 10] that post-quantum isotropic boxes cannot be distilled *in another isotropic box* (this result does not tell about distillation of isotropic boxes into non-isotropic boxes though). Recall that *distillation protocol* was part of the proof of [BS09], see Subsection II.(4), but Marc-Olivier Proulx found later another method to prove the same result, without using distillation [Pro18], see Subsection II.(6). In [BG15], after generalizing the *maximal correlation measure* to post-quantum boxes, the authors show that this measure is monotonically decreasing under wiring. They note that a set of correlations, in order to be consistent in Nature, must be *closed under wirings* [ABL+09, LVN14, NGHA15], so a good idea is to seek sets between $\mathcal{Q}$ and $\mathcal{NS}$ that are closed under wirings. However, given a set of correlations, it is difficult to determine whether or not it closed. This is why they introduce the first general method to construct closed sets of correlations.

(2) 2016: The Threshold ≈ 0.91 is Optimal. In Subsection II.(3), we saw that the authors of [BBL+06] used a 3-input majority function $\mathtt{Maj}_3$ in order to boost the success probability of having a correct distributed computation of f. Instead, they could have used many other functions and they would have probably obtained even better results than their threshold $\frac{3+\sqrt{6}}{6} \approx 91\%$. But actually, later, Ryuhei Mori showed in [Mor16, Theorem 25] that this threshold is not enhanced if we take any other Boolean function in the boosting process, among a large class of functions! Find a similar limitation result in [SWH20], cf point (3). To understand better the class of functions the author considered, we first need to define *XOR functions*: they are Boolean functions g that could be written $g(A, B) = h(A \oplus B)$ for some Boolean function h, where A and B are same-size strings and where $A \oplus B$ is the bit sum component-wise. Additionally, they use the notion of *adaptative protocol*, meaning that box inputs has not to depend on other boxes outputs, and the notion of PR-*adaptative protocol*, which is a protocol for which $f(x, y)$ is computed *without error* when provided PR

boxes. So their large class of function is the class of XOR functions computed by an adaptative PR-correct protocol, and this class contains in particular n-input majority functions $\texttt{Maj}_n$ for $n \geq 3$. The restriction to XOR functions seems to be natural since the strings A and B have meaning especially when their XOR $\oplus$ is taken. Even more astonishing, they show that $\texttt{Maj}_3$ is the unique function, among their class of functions, reaching the threshold $\approx 91\%$, up to adding zeroes on the other coordinates if we consider a function with more than three input bits. Their proof is based on discrete Fourier analysis techniques.

(3) 2020: Tight Limits on NonLocality. In [SWH20], Noah Shutty, Mary Wootters, and Patrick Hayden investigate the extent to which the axiom "communication complexity is nontrivial" can explain the quantum value of nonlocal games. As in point (2), they show that the threshold $\frac{3+\sqrt{6}}{6} \approx 91\%$ from [BBL$^+$06] cannot be improved using a large class of functions. Their class of function C_ϵ is a circuit model on a gate set $\mathcal{G}$ which contains one noisy gate g_ϵ. They apply this idea to formulas of noise-free XOR gates and noisy AND gates. However, this limitation does not rule out all approaches; in particular, it could be that there is a way to use post-quantum correlations in way other than to create noisy AND gates. It is always interesting to rule out any approach, or to find an approach that works. Additionally, note that they exhibit a nonlocal game such that communication complexity collapses in any physical theory whose maximal winning probability exceeds the quantum value!

II.(6) 2018: Boxes are Trivial above a Parabola

In this section, we present the work done by Marc-Olivier Proulx in his Master's thesis [Pro18]. He found new trivial post-quantum boxes, and a new way of proving the result from [BS09], see Subsection II.(4), but without using distillation. His proof is a generalization fo the one from [BBL$^+$06], see Subsection II.(3). His result holds in two slices of the non-signalling polytope $\mathcal{NS}$: the one containing $\texttt{PR}, \texttt{PR}', \texttt{I}$, and the one containing $\texttt{PR}, \texttt{SR}, \texttt{I}$. The latter slice is the same as the one studies in [BS09].

Theorem II.12 (Trivial boxes above a parabola, [Pro18, Thm 1]). *Provided that:*

$$6\,c_1^2 + 3\,(2c_1 - 1)\,c_2 + 2\,c_2^2 - 6\,c_1 + \tfrac{3}{2} > 1,$$

it yields that the box $c_1\,\texttt{PR} + c_2\,\texttt{PR}' + (1 - c_1 - c_2)\,\overline{\texttt{PR}} \in \mathcal{NS}$ *is trivial.*

Theorem II.13 (Trivial boxes above a parabola, [Pro18, Thm 2]). *Provided that:*

$$6\,d_1^2 + \tfrac{9}{2}(2\,d_1 - 1)\,d_2 + \tfrac{15}{4}\,d_2^2 - 6\,d_1 + \tfrac{3}{2} > 1,$$

it yields that the box $d_1\,\texttt{PR} + d_2\,\texttt{SR} + (1 - d_1 - d_2)\,\overline{\texttt{PR}} \in \mathcal{NS}$ *is trivial.*

Those two theorems have share similarities with the proof of [BBL$^+$06]. In particular, note that for isotropic boxes (the "vertical" boxes), the author recovers the same threshold as in [BBL$^+$06], the famous $\frac{3+\sqrt{6}}{6} \approx 91\%$!

Theorem II.14 (Correlated boxes are trivial, [Pro18, Section 4.4]). *Correlated boxes are trivial (except* SR*), without using distillation.*

The proof of this theorem is based on a protocol from [PPK$^+$09]. Given a Boolean function f, the idea is again to distributively compute $f(X, Y)$, where $X, Y \in \{0,1\}^n$. The trick consists in defining a string $F(X)$, for which the k-th element is $F(X)_k = f(X, k)$ for any $1 \leq k \leq 2^n$ (with the convention that an integer $1 \leq k \leq 2^n$ is uniquely associated to a string whose elements are the mod-2 digits of k). Defining the *address function*:

$$\texttt{Addr}_n : \left\{ \begin{array}{ccc} \{0,1\}^{2^n} \times \{0,1\}^n & \longrightarrow & \{0,1\}, \\ \left(x_0, \ldots, x_{2^n-1};\, y_0, \ldots, y_{n-1}\right) & \longmapsto & x_\alpha, \end{array} \right.$$

with $\alpha = \sum_{i=0}^{n-1} y_i 2^i \leq 2^n - 1$, he then obtains the relation:

$$f(X, Y) = \texttt{Addr}_n \left(F(X)_0, \ldots, F(X)_{2^n-1},\, y_0, \ldots, y_{n-1} \right).$$

So it suffices to distributively compute the right handsight, which is done using the PPKSWZ protocol [PPK+09].

II.(7) 2022: Better Distillation Protocols

In this subsection, we mention a very recent work from Giorgos Eftaxias, Mirjam Weilenmann, and Roger Colbeck [EWC22]. We saw in Diagram II.(b) that a distillation protocol with two copies of a box are very powerful, they allow in particular to show that all correlated boxes are trivial [BS09]. But here, in this article, the authors show that mutli-copy distillation protocols can enhance results: they exhibit a particular slice and a particular 3-copy distillation protocol with which they find a new trivial area that is strictly larger than anything achievable with any 2-copy distillation protocol [EWC22, Figure 6]. To this effect, they employ an optimization technique over all 2-copy wiring protocols.

III. Our Contribution: Algebra of Boxes

In this section, we generalize the results obtained in [BS09] in order to find new trivial boxes. The main idea is to introduce an *algebra of boxes* with a new operation: the multiplication, denoted "$\boxtimes$". Using this multiplication, we will then define the notions of *orbit* and of *k-th root* of a box, to eventually find a new trivial area.

III.(1) New Operation: $\boxtimes$

We will define here the *algebra of nonlocal boxes* over the field of real numbers. In a first time, in order to introduce this algebra properly, we will consider not only non-signalling boxes, but also all other possible functions $\{0,1\}^4 \to \mathbb{R}$, so that they form a 16-dimensional vector space $\mathcal{B} = \mathcal{F}\big(\{0,1\}^4, \mathbb{R}\big)$. Later, we will only work in the subset of conditional probability measures, more precisely the one of non-signalling correlations. We endow this vector space $\mathcal{B}$ with the usual addition and scalar multiplication:

$$\begin{aligned} \forall \mathtt{P}, \mathtt{Q} \in \mathcal{B}, \qquad \Big[\mathtt{P} + \mathtt{Q}\Big]\big(a, b \,|\, x, y\big) &:= \mathtt{P}\big(a, b \,|\, x, y\big) + \mathtt{Q}\big(a, b \,|\, x, y\big), \\ \forall \mathtt{P} \in \mathcal{B}, \forall \lambda \in \mathbb{R}, \qquad \Big[\lambda \cdot \mathtt{P}\Big]\big(a, b \,|\, x, y\big) &:= \lambda \cdot \mathtt{P}\big(a, b \,|\, x, y\big). \end{aligned}$$

Multiplication of Boxes. We now need to define a multiplication. Given two boxes $\mathtt{P}$ and $\mathtt{Q}$, we wire them as in the *distiallation protocol* [BS09], so that we obtain a bigger box that we call $\mathtt{P} \boxtimes \mathtt{Q}$:

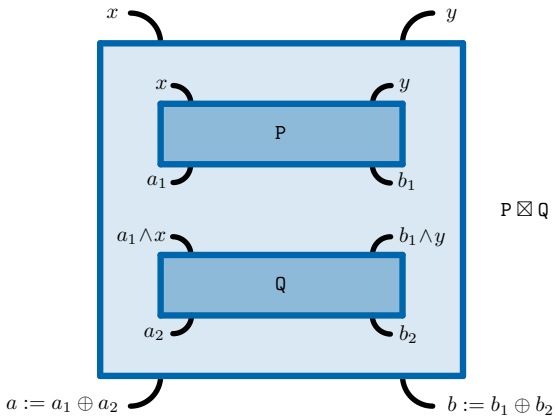


Diagram III.(a) — Distillation protocol of some boxes $\mathtt{P}$ and $\mathtt{Q}$, in this order, which gives rise to a new box, called $\mathtt{P} \boxtimes \mathtt{Q}$.

This product $\boxtimes$ could be more formally written as follows:

$$\mathtt{P} \boxtimes \mathtt{Q}\Big(a, b \,\Big|\, x, y\Big) = \sum_{a_1, b_1, a_2, b_2 \in \{0,1\}} \mathtt{P}\Big(a_1, b_1 \,\Big|\, x, y\Big) \times \mathtt{Q}\Big(a_2, b_2 \,\Big|\, a_1 x, b_1 y\Big) \mathbb{1}_{a = a_1 \oplus a_2} \mathbb{1}_{b = b_1 \oplus b_2} \tag{10}$$

$$= \boxed{\sum_{a_1, b_1 \in \{0,1\}} \mathtt{P}\Big(a_1, b_1 \,\Big|\, x, y\Big) \times \mathtt{Q}\Big(a \oplus a_1, b \oplus b_1 \,\Big|\, a_1 x, b_1 y\Big)}, \tag{11}$$

where a, b, x, y are bits in $\{0,1\}$. From this formula, we clearly see that $\boxtimes$ is *bilinear*, and in particular it is distributive for $+$. Besides the fact that $\boxtimes$ is unquestionably *intern* in $\mathcal{B}$, it is as well intern in the set of conditional probability measures:

$$\begin{aligned}\sum_{a,b\in\{0,1\}} \mathtt{P}\boxtimes\mathtt{Q}\Big(a,\,b\,\Big|\,x,\,y\Big) &= \sum_{a_1,b_1\in\{0,1\}} \mathtt{P}\Big(a_1,\,b_1\,\Big|\,x,\,y\Big)\times\left[\sum_{a,b\in\{0,1\}}\mathtt{Q}\Big(a\oplus a_1,\,b\oplus b_1\,\Big|\,a_1x,\,b_1y\Big)\right]\\ &= \sum_{a_1,b_1\in\{0,1\}} \mathtt{P}\Big(a_1,\,b_1\,\Big|\,x,\,y\Big)\times 1\\ &= 1,\end{aligned}$$

for any $x, y \in \{0,1\}$. As well, note that the local set $\mathcal{L}$, the quantum set $\mathcal{Q}$ and the non-signalling set $\mathcal{NS}$ are all stable under this operation, see [ABL+09]. Altogether, this shows in particular that $\big(\mathcal{B},+,\cdot,\boxtimes\big)$ is a well defined algebra of boxes.

Multiplication Table for $\boxtimes$. Using formula (11), direct computations lead to the following multiplication table:

P \ Q	PR	SR	$\overline{\mathtt{PR}}$	$\overline{\mathtt{SR}}$
PR	PR	PR	$\overline{\mathtt{PR}}$	$\overline{\mathtt{PR}}$
SR	$\frac{1}{2}\big(\mathtt{PR}+\mathtt{SR}\big)$	SR	$\frac{1}{2}\big(\overline{\mathtt{PR}}+\overline{\mathtt{SR}}\big)$	$\overline{\mathtt{SR}}$
$\overline{\mathtt{PR}}$	$\frac{1}{2}\big(\overline{\mathtt{PR}}+\overline{\mathtt{SR}}\big)$	$\overline{\mathtt{PR}}$	$\frac{1}{2}\big(\mathtt{PR}+\mathtt{SR}\big)$	PR
$\overline{\mathtt{SR}}$	$\overline{\mathtt{SR}}$	$\overline{\mathtt{SR}}$	SR	SR

Table III.(b) — Multiplication table given by $\mathtt{P}\boxtimes\mathtt{Q}$.

where we recall that $\overline{\mathtt{SR}} := \mathtt{PR} - \mathtt{SR} + \overline{\mathtt{PR}}$. For instance, let us compute $\mathtt{PR}\boxtimes\mathtt{SR}$. Using formula (11):

$$\begin{aligned}\mathtt{PR}\boxtimes\mathtt{SR}\Big(a,\,b\,\Big|\,x,\,y\Big) &= \sum_{a_1,b_1\in\{0,1\}} \mathtt{PR}\Big(a_1,\,b_1\,\Big|\,x,\,y\Big)\times\mathtt{SR}\Big(a\oplus a_1,\,b\oplus b_1\,\Big|\,a_1x,\,b_1y\Big)\\ &= \sum_{a_1,b_1\in\{0,1\}} \tfrac{1}{2}\mathbb{1}_{a_1\oplus b_1=xy}\times\tfrac{1}{2}\mathbb{1}_{a\oplus a_1=b\oplus b_1},\end{aligned}$$

where $a\oplus a_1 = b\oplus b_1 \Leftrightarrow a_1\oplus b_1 = a\oplus b$, so that the condition $\big(a_1\oplus b_1 = xy\big)\wedge\big(a\oplus a_1 = b\oplus b_1\big)$ is equivalent to saying $a_1\oplus b_1 = xy = a\oplus b$. This last condition is satisfied by exactly two couples (a_1,b_1) of $\{0,1\}^2$, hence after summing it remains:

$$= \tfrac{1}{2}\,\mathbb{1}_{a\oplus b=xy},$$

and we recognize the expression of the PR box. Hence $\boxed{\mathtt{PR}\boxtimes\mathtt{SR}=\mathtt{PR}}$. Alternatively, we may as well rely on Diagram III.(a) to make faster computation: by definition, the first box (PR) gives $a_1\oplus b_1 = xy$ while the second one (SR) gives $a_2\oplus b_2 = 0$. Therefore, the outputs a and b of $\mathtt{PR}\boxtimes\mathtt{SR}$ satisfy $a\oplus b = \big(a_1\oplus b_1\big)\oplus\big(a_2\oplus b_2\big) = xy$, which characterizes the PR box.

Right Identity. The box $\boxed{\mathtt{P}_0\big(a,\,b\,\big|\,x,\,y\big) := \mathbb{1}_{a=b=0}}$ is a right identity for $\boxtimes$:

$$\mathtt{P}\boxtimes\mathtt{P}_0\Big(a,\,b\,\Big|\,x,\,y\Big) \overset{(11)}{=} \sum_{a_1,b_1\in\{0,1\}} \mathtt{P}\Big(a_1,\,b_1\,\Big|\,x,\,y\Big)\times\mathbb{1}_{a_1=a,b_1=b} \;=\; \mathtt{P}\Big(a,\,b\,\Big|\,x,\,y\Big),$$

for any arbitrary box $\mathtt{P}\in\mathcal{B}$. We may compute its coordinates in the CHSH–CHSH′ plane:

$$\mathbb{P}\left(\begin{smallmatrix}\mathtt{P}_0\text{ wins}\\ \text{at }\mathtt{CHSH}\end{smallmatrix}\right) = \sum_{x,y\in\{0,1\}}\tfrac{1}{4}\sum_{a,b\in\{0,1\}}\mathtt{P}_0\Big(a,\,b\,\Big|\,x,\,y\Big)\,\mathbb{1}_{a\oplus b=xy} = \sum_{x,y\in\{0,1\}}\tfrac{1}{4}\,\mathbb{1}_{0=xy} = \tfrac{3}{4},$$

and likewise $\mathbb{P}\big(\mathtt{P}_0\text{ wins at }\mathtt{CHSH}'\big) = \frac{3}{4}$ since the box $\mathtt{P}_0$ does not depend on the entries x and y and because CHSH′ is flipped-entries version of CHSH. Hence $\mathtt{P}_0$ is projected at the same position as SR in the CHSH–CHSH′ plane, at the coordinates $(\frac{3}{4},\frac{3}{4})$, although they are actually different boxes in $\mathcal{B}$.

What about SR?. (1) In view of the second column of the above multiplication table, we may wonder if $\mathtt{SR}$ is a right identity for the operation $\boxtimes$. We see here that it is not the case in $\mathcal{B}$, notwithstanding that we will later obtain that $\mathtt{SR}$ is a right identity in some affine plane $\mathcal{P} \subseteq \mathcal{B}$. For any box $\mathtt{P}$, we have by equation (11):

$$\mathtt{P} \boxtimes \mathtt{SR}\Big(a,\, b \,\Big|\, x,\, y\Big) = \sum_{a_1, b_1 \in \{0,1\}} \mathtt{P}\Big(a_1,\, b_1 \,\Big|\, x,\, y\Big) \times \tfrac{1}{2}\, \mathbb{1}_{a \oplus a_1 = b \oplus b_1},$$

but the condition $a \oplus a_1 = b \oplus b_1$ is equivalent to the case disjunction $(a_1 = a \wedge b_1 = b) \vee (a_1 = a \oplus 1 \wedge b_1 = b \oplus 1)$, so:

$$= \frac{1}{2}\, \mathtt{P}\Big(a,\, b \,\Big|\, x,\, y\Big) + \frac{1}{2}\, \mathtt{P}\Big(a \oplus 1,\, b \oplus 1 \,\Big|\, x,\, y\Big).$$

This relation gives in one go a proof for the second column of the multiplication table, and as well a proof that $\mathtt{SR}$ is not a right identity since for instance $\mathtt{P}_0 \boxtimes \mathtt{SR} \neq \mathtt{P}_0$.

(2) In order to understand better the second line of the table, on the one hand we have that left multiplication by $\mathtt{SR}$ gives:

$$\mathtt{SR} \boxtimes \mathtt{P}\Big(a,\, b \,\Big|\, x,\, y\Big) = \sum_{a_1, b_1 \in \{0,1\}} \tfrac{1}{2}\, \mathbb{1}_{a_1 = b_1} \times \mathtt{P}\Big(a \oplus a_1,\, b \oplus b_1 \,\Big|\, a_1 x,\, b_1 y\Big),$$

where condition $a_1 = b_1$ is equivalent to the case disjunction $(a_1 = b_1 = 0) \vee (a_1 = b_1 = 1)$, so that:

$$= \frac{1}{2}\, \mathtt{P}\Big(a,\, b \,\Big|\, 0,\, 0\Big) + \frac{1}{2}\, \mathtt{P}\Big(a \oplus 1,\, b \oplus 1 \,\Big|\, x,\, y\Big).$$

for any arbitrary box $\mathtt{P} \in \mathcal{B}$. On the other hand, notice that $\mathtt{PR}\big(a,\, b \,\big|\, 0,\, 0\big) = \frac{1}{2}\, \mathbb{1}_{a=b} = \mathtt{SR}\big(a,\, b \,\big|\, x,\, y\big)$, and similarly $\overline{\mathtt{PR}}\big(a,\, b \,\big|\, 0,\, 0\big) = \frac{1}{2}\, \mathbb{1}_{a \neq b} = \mathtt{SR}\big(a,\, b \,\big|\, x,\, y\big)$. As a consequence, this gives a proof for the second line in the multiplication table.

Proposition III.1 (Algebra of Boxes). *The structure $\big(\mathcal{B}, +, \cdot, \boxtimes\big)$ is a non-commutative and non-associative algebra. Moreover, the box $\mathtt{P}_0 := \mathbb{1}_{a=b=0}$ is a right identity for the operation $\boxtimes$.*

Remark III.2. Non-associativity and non-commutativity are both primordial in what follows: it will allow us to enrich results given in [BS09], see Subsection III.(3).

Remark III.3 (Further Properties). Denote $\boxed{\mathtt{P}^{\boxtimes k}}$ the k-th right power $\mathtt{P}^{\boxtimes k} := \Big(\big((\mathtt{P} \boxtimes \mathtt{P}) \boxtimes \mathtt{P}\big) \cdots\Big) \boxtimes \mathtt{P}$. The algebra of boxes $(\mathcal{B}, +, \cdot, \boxtimes)$ satisfies the following properties:

- No Jacobi Identity: $\mathtt{P} \boxtimes (\mathtt{Q} \boxtimes \mathtt{R}) + \mathtt{Q} \boxtimes (\mathtt{R} \boxtimes \mathtt{P}) + \mathtt{R} \boxtimes (\mathtt{P} \boxtimes \mathtt{Q}) \neq 0$ for $\mathtt{P} = \mathtt{Q} = \mathtt{R} = \mathtt{PR}$.
- No Jordan Identity: $(\mathtt{P}^{\boxtimes 2} \boxtimes \mathtt{Q}) \boxtimes \mathtt{P} \neq \mathtt{P}^{\boxtimes 2} \boxtimes (\mathtt{Q} \boxtimes \mathtt{P})$ for $\mathtt{P} = \mathtt{PR}$ and $\mathtt{Q} = \overline{\mathtt{PR}}$.
- No anticommutativity: $\mathtt{P} \boxtimes \mathtt{Q} \neq -\mathtt{Q} \boxtimes \mathtt{P}$ for $\mathtt{P} = \mathtt{Q} = \mathtt{PR}$.
- No alternativity: $(\mathtt{P} \boxtimes \mathtt{P}) \boxtimes \mathtt{Q} \neq \mathtt{P} \boxtimes (\mathtt{P} \boxtimes \mathtt{Q})$ for $\mathtt{P} = \mathtt{SR}$ and $\mathtt{Q} = \mathtt{PR}$.
- No flexibility: $\mathtt{P} \boxtimes (\mathtt{Q} \boxtimes \mathtt{P}) \neq (\mathtt{P} \boxtimes \mathtt{Q}) \boxtimes \mathtt{P}$ for $\mathtt{P} = \mathtt{PR}$ and $\mathtt{Q} = \overline{\mathtt{PR}}$.
- No power associativity: $\big(\mathtt{P}^{\boxtimes 2}\big)^{\boxtimes 2} = (\mathtt{P} \boxtimes \mathtt{P}) \boxtimes (\mathtt{P} \boxtimes \mathtt{P}) \neq \big((\mathtt{P} \boxtimes \mathtt{P}) \boxtimes \mathtt{P}\big) \boxtimes \mathtt{P} = \mathtt{P}^{\boxtimes 4}$ for $\mathtt{P} = \overline{\mathtt{PR}}$.
- No power commutativity: $\mathtt{P}^{\boxtimes 3} \boxtimes \mathtt{P}^{\boxtimes 2} \neq \mathtt{P}^{\boxtimes 2} \boxtimes \mathtt{P}^{\boxtimes 3}$ for $\mathtt{P} = \overline{\mathtt{PR}}$.

So it can difficulty be assimilated to a well-known algebra.

Proof. From what proceeds, we already know that $\big(\mathcal{B}, +, \cdot, \boxtimes\big)$ is a well-defined algebra and that the box $\mathtt{P}_0$ is a right identity for the operation $\boxtimes$. Now, using Table III.(b), we observe that the multiplication $\boxtimes$ is non-commutative: $\mathtt{PR} \boxtimes \overline{\mathtt{SR}} = \overline{\mathtt{PR}} \neq \overline{\mathtt{SR}} = \overline{\mathtt{SR}} \boxtimes \mathtt{PR}$. In addition, we remark that $\boxtimes$ is non-associative since:

$$\begin{aligned} \mathtt{PR} \boxtimes \Big(\overline{\mathtt{PR}} \boxtimes \mathtt{PR}\Big) &= \mathtt{PR} \boxtimes \tfrac{1}{2}\Big(\overline{\mathtt{PR}} + \overline{\mathtt{SR}}\Big) = \tfrac{1}{2}\Big(\overline{\mathtt{PR}} + \overline{\mathtt{PR}}\Big) = \overline{\mathtt{PR}}, \\ \Big(\mathtt{PR} \boxtimes \overline{\mathtt{PR}}\Big) \boxtimes \mathtt{PR} &= \overline{\mathtt{PR}} \boxtimes \mathtt{PR} = \tfrac{1}{2}\Big(\overline{\mathtt{PR}} + \overline{\mathtt{SR}}\Big). \end{aligned}$$

Hence the result. □

The Affine Plane $\mathcal{P} = \langle \mathtt{PR}, \mathtt{SR}, \overline{\mathtt{PR}} \rangle$. Now, in the 16-dimensional vector space $\mathcal{B}$, let us consider the affine plane $\mathcal{P} = \langle \mathtt{PR}, \mathtt{SR}, \overline{\mathtt{PR}} \rangle$, parametrized by barycentric coordinates in terms of $\mathtt{PR}$, $\mathtt{SR}$ and $\overline{\mathtt{PR}}$ (which are non-aligned boxes of $\mathcal{B}$):

$$\mathtt{P}_{\xi,\gamma} \;:=\; \xi\,\mathtt{PR} + \gamma\,\mathtt{SR} + (1-\xi-\gamma)\,\overline{\mathtt{PR}},$$

for $\gamma, \xi \in \mathbb{R}$. This affine plane $\mathcal{P}$ is particularly interesting since it contains both isotropic boxes (convex combinaisons of $\mathtt{PR}$ and $\overline{\mathtt{PR}}$) and correlated boxes (convex combinaisons of $\mathtt{PR}$ and $\mathtt{SR}$). Moreover, we will see in the next lemma that this plane is stable under $\boxtimes$, which makes $\mathcal{P}$ being particularly outstanding. In addition, there is a natural map from $\mathcal{P}$ into the plane $\mathtt{CHSH}$–$\mathtt{CHSH}'$, which for a given box $\mathtt{P}$ outputs its probability of winning at $\mathtt{CHSH}'$ and $\mathtt{CHSH}$ in respectively abscissa and ordinate. This map is a bijection since since it is affine by (12) and the image of the affine basis $\{\mathtt{PR}, \mathtt{SR}, \overline{\mathtt{PR}}\}$ of $\mathcal{P}$ is also an affine basis (a set of three non-aligned points) of $\mathtt{CHSH}$–$\mathtt{CHSH}'$. Due to this bijection, we will note make a difference between a box $\mathtt{P}$ in $\mathcal{P}$ and its image in the plane $\mathtt{CHSH}$–$\mathtt{CHSH}'$.

Recall that, given a box $\mathtt{P}$, we can compute its $\mathtt{CHSH}$ wining probability with formula (3). We denote (x, y) the cartesian coordinates of $\mathtt{P}_{\xi,\gamma}$ in the linear plane $\mathtt{CHSH}$–$\mathtt{CHSH}'$. We have $y = \mathbb{P}\big(\mathtt{P}_{\xi,\gamma} \text{ wins at } \mathtt{CHSH}\big) = \xi\,\mathbb{P}\big(\mathtt{PR} \text{ wins at } \mathtt{CHSH}\big) + \gamma\,\mathbb{P}\big(\mathtt{SR} \text{ wins at } \mathtt{CHSH}\big) + (1-\xi-\gamma)\mathbb{P}\big(\overline{\mathtt{PR}} \text{ wins at } \mathtt{CHSH}\big) = \xi + \frac{3}{4}\,\gamma$, and likewise $x = \mathbb{P}\big(\mathtt{P}_{\xi,\gamma} \text{ wins at } \mathtt{CHSH}'\big) = \frac{1}{2}\,\xi + \frac{3}{4}\,\gamma + \frac{1-\xi-\gamma}{2} = \frac{1}{2} + \frac{1}{4}\,\gamma$. It results the following change of coordinates between $\mathcal{P}$ and $\mathtt{CHSH}$–$\mathtt{CHSH}'$:

$$\left\{\begin{array}{rcl} x &=& \frac{1}{2} + \frac{1}{4}\,\gamma, \\ y &=& \xi + \frac{3}{4}\,\gamma, \end{array}\right. \qquad \Longleftrightarrow \qquad \left\{\begin{array}{l} \xi = \frac{3}{2} - 3x + y, \\ \gamma = 4x - 2. \end{array}\right. \tag{12}$$

We denote the corresponding coordinate change functions as $\mathtt{xyCoord}(\xi, \gamma) = (x, y)$ and $\mathtt{xigammaCoord}(x, y) = (\xi, \gamma)$. In the next lemma, we will also consider $\mathtt{P}_{\alpha,\beta}$ with coefficients $\alpha, \beta \in \mathbb{R}$. Using these notations, we show the astonishing fact that the product $\boxtimes$ of two elements of $\mathcal{P}$ is again in $\mathcal{P}$:

Lemma III.4 ($\mathcal{P}$ is stable under $\boxtimes$)**.** *We have* $\boxed{\mathtt{P}_{\xi,\gamma} \boxtimes \mathtt{P}_{\alpha,\beta} = \mathtt{P}_{\tilde{\xi},\tilde{\gamma}} \in \mathcal{P}}$*, with* $\tilde{\xi}, \tilde{\gamma}$ *such that:*

$$\left\{\begin{array}{l} \tilde{\xi} = \frac{1}{2} - \frac{\xi}{2} - \frac{\beta}{2} + \xi\alpha + \frac{3}{2}\xi\beta, \\ \tilde{\gamma} = \frac{1}{2} - \frac{\xi}{2} - \gamma - \alpha - \frac{\beta}{2} + \xi\alpha + \;\frac{\xi\beta}{2} + 2\gamma\alpha + 2\gamma\beta. \end{array}\right. \tag{13}$$

Proof. By bilinearity of $\boxtimes$, we have:

$$\begin{aligned} \mathtt{P}_{\xi,\gamma} \boxtimes \mathtt{P}_{\alpha,\beta} \;=\; & \xi\alpha\,\mathtt{PR} \boxtimes \mathtt{PR} \;+\; \gamma\alpha\,\mathtt{SR} \boxtimes \mathtt{PR} \;+\; (1-\xi-\gamma)\alpha\,\overline{\mathtt{PR}} \boxtimes \mathtt{PR} \\ & +\; \xi\beta\,\mathtt{PR} \boxtimes \mathtt{SR} \;+\; \gamma\beta\,\mathtt{SR} \boxtimes \mathtt{SR} \;+\; (1-\xi-\gamma)\beta\,\overline{\mathtt{PR}} \boxtimes \mathtt{SR} \\ & +\; \xi\,(1-\alpha-\beta)\,\mathtt{PR} \boxtimes \overline{\mathtt{PR}} \;+\; \gamma\,(1-\alpha-\beta)\,\mathtt{SR} \boxtimes \overline{\mathtt{PR}} \;+\; (1-\xi-\gamma)(1-\alpha-\beta)\overline{\mathtt{PR}} \boxtimes \overline{\mathtt{PR}}, \end{aligned}$$

and using Table III.(b), we have:

$$\begin{aligned} = \; & \xi\alpha\,\mathtt{PR} + \tfrac{\gamma\alpha}{2}\Big[\mathtt{PR} + \mathtt{SR}\Big] + \tfrac{\alpha-\xi\alpha-\gamma\alpha}{2}\Big[\overline{\mathtt{PR}} + \overline{\mathtt{SR}}\Big] \\ & +\; \xi\beta\,\mathtt{PR} \;+\; \gamma\beta\,\mathtt{SR} \;+\; (\beta-\xi\beta-\gamma\beta)\overline{\mathtt{PR}} \\ & +\; (\xi-\xi\alpha-\xi\beta)\overline{\mathtt{PR}} \;+\; \tfrac{\gamma-\gamma\alpha-\gamma\beta}{2}\Big[\overline{\mathtt{PR}} \;+\; \overline{\mathtt{SR}}\Big] + \tfrac{1-\alpha-\beta-\xi+\xi\alpha+\xi\beta-\gamma+\gamma\alpha+\gamma\beta}{2}\Big[\mathtt{PR} + \mathtt{SR}\Big], \end{aligned}$$

and then using the relation $\overline{\mathtt{SR}} := \mathtt{PR} - \mathtt{SR} + \overline{\mathtt{PR}}$ and simplifying coefficients, we obtain:

$$\begin{aligned} = \; & \Big[\tfrac{1}{2} - \tfrac{\xi}{2} - \tfrac{\beta}{2} + \xi\alpha + \tfrac{3}{2}\xi\beta\Big]\mathtt{PR} \;+\; \Big[\tfrac{1}{2} - \tfrac{\xi}{2} - \gamma - \alpha - \tfrac{\beta}{2} + \xi\alpha + \;\tfrac{\xi\beta}{2} + 2\gamma\alpha + 2\gamma\beta\Big]\mathtt{SR} \\ & +\; \Big[\xi + \gamma + \alpha + \beta - 2\xi\alpha - 2\xi\beta - 2\gamma\alpha - 2\gamma\beta\Big]\overline{\mathtt{PR}}. \end{aligned}$$

We see that coefficients sum to 1, so we well obtain that $\mathtt{P}_{\xi,\gamma} \boxtimes \mathtt{P}_{\alpha,\beta}$ produces a box of the form $\mathtt{P}_{\tilde{\xi},\tilde{\gamma}}$ with $\tilde{\xi}$ and $\tilde{\gamma}$ satisfying equations (13). □

Multiplication $\boxtimes$ on $\mathcal{P}$. This lemma induces a magma $\big(\mathcal{P}, \boxtimes\big)$, meaning that the set $\mathcal{P} = \langle \mathtt{PR}, \mathtt{SR}, \overline{\mathtt{PR}} \rangle$ is endowed with an inner multiplication $\boxtimes$:

$$\begin{pmatrix} \xi \\ \gamma \end{pmatrix} \boxtimes \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \;:=\; \begin{pmatrix} \frac{1}{2} - \frac{\xi}{2} - \frac{\beta}{2} + \xi\alpha + \frac{3}{2}\xi\beta, \\ \frac{1}{2} - \frac{\xi}{2} - \gamma - \alpha - \frac{\beta}{2} + \xi\alpha + \;\frac{\xi\beta}{2} + 2\gamma\alpha + 2\gamma\beta \end{pmatrix}, \tag{14}$$

where we represented the box $\mathtt{P}_{\xi,\gamma} = \xi\,\mathtt{PR} + \gamma\,\mathtt{SR} + (1-\xi-\gamma)\overline{\mathtt{PR}}$ in the vector-like style $\begin{pmatrix}\xi\\ \gamma\end{pmatrix}$ for the sake of clarity. In this magma, contrary to the case of the algebra $(\mathcal{B}, +, \cdot, \boxtimes)$, $\boxed{\mathtt{SR}\text{ is a right identity}}$: taking $\alpha = 0$ and $\beta = 1$, we have $\begin{pmatrix}\xi\\ \gamma\end{pmatrix} \boxtimes \mathtt{SR} = \begin{pmatrix}\xi\\ \gamma\end{pmatrix}$. In addition, using the same examples as in the proof of Proposition III.1 , we can see that this magma is *non-commutative* and *non-associative*. Furthermore, if we have two points A and B in the plane CHSH–CHSH′, we may define $\mathtt{A} \boxtimes_{\mathtt{CHSH}} \mathtt{B} := \mathtt{xyCoord}(\mathtt{xigammaCoord}(\mathtt{A}) \boxtimes \mathtt{xigammaCoord}(\mathtt{B}))$. When the situation is not ambiguous, we will omit the indice of $\boxtimes_{\mathtt{CHSH}}$ to simply write $\boxtimes$ instead.

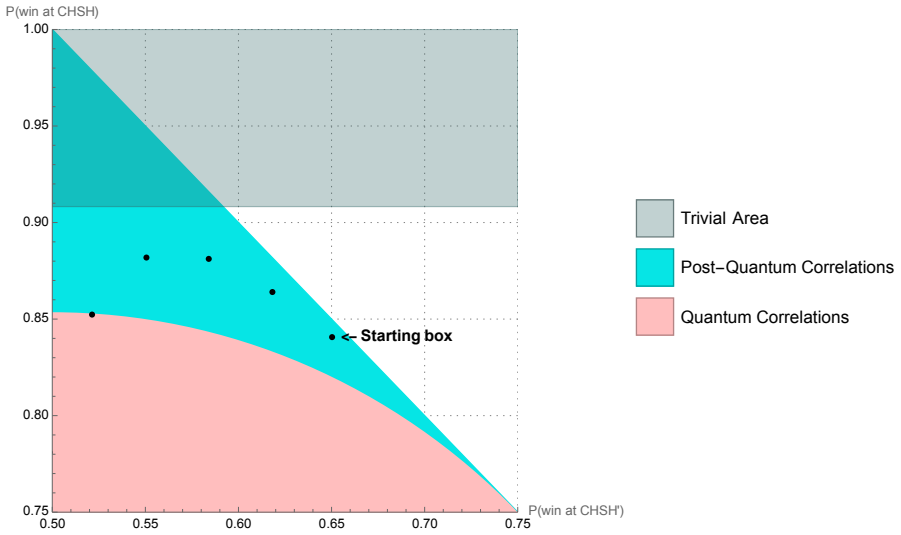
III.(2) Link with Previous Results

Let us restate results from [BS09] in terms of the algebra we have just defined.

Orbit of a Box. Starting from a non-signalling box P, we define a sequence of boxes $(\mathtt{P}_k)_k$ such that $\mathtt{P}_1 := \mathtt{P}$ and $\mathtt{P}_k := \mathtt{P}_{k-1} \boxtimes \mathtt{P}_{k-1}$ for all $k \geq 2$. We then introduce the *orbit* of P as the following set:

$$\mathtt{OrbitBS09}(\mathtt{P}) := \left\{\mathtt{P}_k\right\}_{k\geq 1}.$$

Given an arbitrary large number of copies of the box P, there exists a process for building the box $\mathtt{P}_k$ by setting classical wirings between these copies of P. Notice that this process does *not* increase communication complexity because Alice and Bod do not exchange bits, they just wire some boxes in a certain smart way. This is the reason why it is enough to show that $\mathtt{OrbitBS09}(\mathtt{P})$ intersects the trivial area found by [BBL+06] in order to obtain that P is a trivial box (see the graphic below). This is the idea of Brunner and Skrzypczyk behind their article [BS09]. Such a protocol is called *distillation protocol*. An orbit could be drawn as follows:



Graphic III.(c) — The black dots represent the first 5 elements of $\mathtt{OrbitBS09}(\mathtt{P})$, where $\mathtt{P}_0$ is the point on the right and the following $\mathtt{P}_k$'s are going toward the left side as k grows. The red part represent the set of quantum correlations, the blue one represent the set of post-quantum correlations, and the shaded gray part is the area on which we know that communication complexity is trivial [BBL+06]. Here we took P such that $x = 0.65$ and $y = 0.841$ in the CHSH–CHSH′ plane.

Correlated Boxes are Trivial. In particular, using this process, they managed to show that precisely all correlated boxes are trivial boxes (except for the end point SR): computing p-corNLB $\boxtimes$ p-corNLB, they obtained a $\tilde{p}$-corNLB box such that $\tilde{p} > p$. This way, they distill any correlated box until reached the trivial ara from [BBL+06], which shows that those correlated boxes are trivial boxes. Besides, using a similar technique, they managed to numerically draw a wider region on which communication complexity is trivial as well:

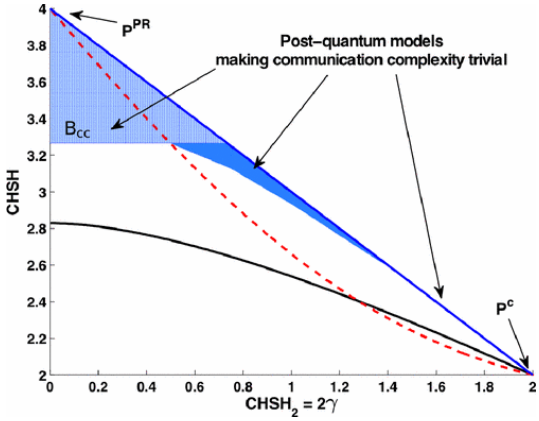


Figure III.(d) — The dark blue area is the contribution of [BS09, Figure 4] (this is the original graphic). It is a region of exclusively trivial boxes, and it was numerically drawn. This is the most recent trivial zone that was found.

III.(3) Richer Notion of Orbit

Using the same type of reasoning as in [BS09], let us widen their trivial area.

Orbit of order k. Our idea is to enrich the notion of *orbit* that we have just introduced hereinabove. To do so, given a non-signalling box $\mathtt{P}$, we first define its *orbit of order k* as the following set:

$$\mathtt{Orbit}_k(\mathtt{P}) := \Big\{\text{products of } k \text{ times } \mathtt{P} \text{ for any parenthesization}\Big\}.$$

For instance, the orbit of respective order three and four are:

$$\begin{aligned}
\mathtt{Orbit}_3(\mathtt{P}) &= \Big\{\mathtt{P}\boxtimes(\mathtt{P}\boxtimes\mathtt{P}), (\mathtt{P}\boxtimes\mathtt{P})\boxtimes\mathtt{P}\Big\},\\
\mathtt{Orbit}_4(\mathtt{P}) &= \Big\{\mathtt{P}\boxtimes\Big(\mathtt{P}\boxtimes(\mathtt{P}\boxtimes\mathtt{P})\Big), \mathtt{P}\boxtimes\Big((\mathtt{P}\boxtimes\mathtt{P})\boxtimes\mathtt{P}\Big),\\
&\qquad \Big(\mathtt{P}\boxtimes(\mathtt{P}\boxtimes\mathtt{P})\Big)\boxtimes\mathtt{P}, \Big((\mathtt{P}\boxtimes\mathtt{P})\boxtimes\mathtt{P}\Big)\boxtimes\mathtt{P},\\
&\qquad \Big(\mathtt{P}\boxtimes\mathtt{P}\Big)\boxtimes\Big(\mathtt{P}\boxtimes\mathtt{P}\Big)\Big\}\\
&= \mathtt{P}\boxtimes\mathtt{Orbit}_3(\mathtt{P}) \bigcup \mathtt{Orbit}_3(\mathtt{P})\boxtimes\mathtt{P} \bigcup \Big\{(\mathtt{P}\boxtimes\mathtt{P})\boxtimes(\mathtt{P}\boxtimes\mathtt{P})\Big\}.
\end{aligned}$$

Remark III.5 (Catalan Number). Note that the size of the set $\mathtt{Orbit}_k(\mathtt{P})$ corresponds to the number of parenthesizations of k terms. This number is called *Catalan number*, it is denoted C_k and it grows exponentially fast:

$$C_k \;=\; \frac{1}{k+1}\binom{2k}{k} \;=\; \frac{(2k)!}{(k+1)!\,k!} \;=\; \prod_{i=2}^{k}\frac{k+i}{i}.$$

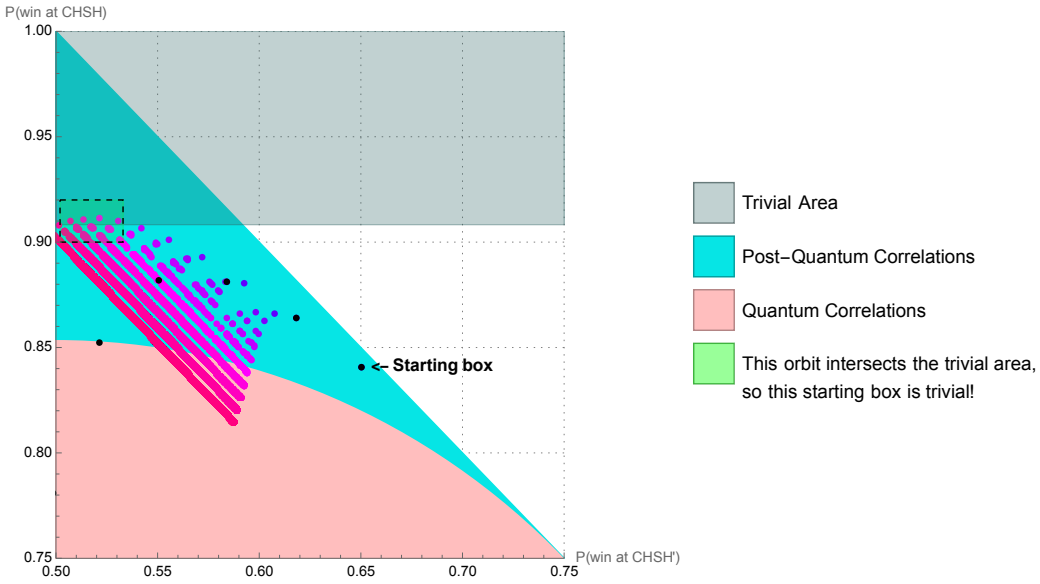
Enriched Orbit. Then, we define a new notion of *orbit*, by taking the union of the orbits of order k:

$$\mathtt{Orbit}(\mathtt{P}) := \bigcup_{k\geq 1}\mathtt{Orbit}_k(\mathtt{P}).$$

As compared to the previous notion of orbit, this one is way richer in the sense that:

$$\mathtt{OrbitBS09}(\mathtt{P}) \subsetneq \bigcup_{k\geq 0}\mathtt{Orbit}_{2^k}(\mathtt{P}) \subsetneq \mathtt{Orbit}(\mathtt{P}).$$

To this point, we may think that this generalized orbit could help to enlarge the trivial area found in Figure III.(d), and we will see in Theorem III.9 that it is well the case. Here is what an orbit looks like:



Graphic III.(e) — We took Graphic III.(c) and we added our new orbit $\texttt{Orbit}(\texttt{P})$. Here we drawn $\texttt{Orbit}_k(\texttt{P})$ for $k = 1, ..., 12$, and the colour goes from blue to red as k increases. We observe that $\texttt{OrbitBS09}(\texttt{P})$ (drawn in black) is well included in $\texttt{Orbit}(\texttt{P})$, but that the latter is much richer, as explained above. Again, here we took $\texttt{P}$ such that $x = 0.65$ and $y = 0.841$ in the $\texttt{CHSH}$–$\texttt{CHSH}'$ plane.

Conjectures. In view of such a graphic, we might conceive that the following conjectures hold:

(I) The new notion $\texttt{Orbit}(\texttt{P})$ allows to find new trivial boxes.

(II) Let $k \geq 3$ be an integer. Then the points of $\texttt{Orbit}_k(\texttt{P})$ are aligned on a line $\mathcal{L}_k$.

(III) Assuming the previous conjecture, lines $\mathcal{L}_k$ and $\mathcal{L}_\ell$ are parallel for any $k, \ell \geq 3$. More precisely, each line $\mathcal{L}_k$ is parallel to the diagonal $\mathcal{L}_D$ of the blue triangle.

(IV) For fixed k, we denote $\texttt{P}_{\max,\,k}$ the highest point of $\texttt{Orbit}_k(\texttt{P})$. Then the union of the $\texttt{P}_{\max,\,k}$'s form a discretized parabola.

In what follows, we will put to the test the veracity of those statements. Be careful: one might think that the first one is obvious as a consequence of the last graphic, but we will see in next subsection that there is a subtlety to check.

III.(4) Testing the Conjectures

As before, let $\texttt{P} \in \mathcal{B}$ be a non-signalling box. We will show our results in an easy case, for we will see later that it is enough to restrict our study in this way. We consider the *lightened orbit of order k* defined recursively as:

$$\widetilde{\texttt{Orbit}}_k(\texttt{P}) := \texttt{P} \boxtimes \widetilde{\texttt{Orbit}}_{k-1}(\texttt{P}) \bigcup \widetilde{\texttt{Orbit}}_{k-1}(\texttt{P}) \boxtimes \texttt{P},$$

for $k \geq 2$, where the initialization is $\widetilde{\texttt{Orbit}}_1(\texttt{P}) := \{\texttt{P}\}$. We have that $\widetilde{\texttt{Orbit}}_k(\texttt{P}) \subseteq \texttt{Orbit}_k(\texttt{P})$, but this is (generally) a strict inclusion for $k \geq 4$. For example, the box $(\texttt{P} \boxtimes \texttt{P}) \boxtimes (\texttt{P} \boxtimes \texttt{P})$ belongs to $\texttt{Orbit}_4(\texttt{P})$ whereas it does not belong to $\widetilde{\texttt{Orbit}}_4(\texttt{P})$.

Conjecture 1 holds. We name $\texttt{triv}_{\text{BBLMTU}}$ the trivial area found in [BBL+06], drawn in gray in previous diagrams, which is the half-plane above the horizontal line of equation $y = \frac{3+\sqrt{6}}{6} \approx 0.91$. Similarly, we name $\texttt{triv}_{\text{BS09}}$ the trivial area found in [BS09], represented in dark blue in their diagram Figure III.(d). As $\texttt{triv}_{\text{BS09}}$ was numerically determined, we do not have an analytic expression of this trivial area and we need to be careful when comparing this region and our new trivial region.

A first step that the authors Brunner and Skrzypczyk can do to determine $\texttt{triv}_{\text{BS09}}$ is to figure out all the starting boxes $\texttt{P}$ such that $\texttt{OrbitBS09}(\texttt{P})$ intersects $\texttt{triv}_{\text{BBLMTU}}$. Recall that if a box $\texttt{Q}$ of the orbit of $\texttt{P}$ is trivial, then $\texttt{P}$ is as well trivial because using the operation $\boxtimes$ many times on copies of $\texttt{P}$ does not increase communication complexity. Hence, those boxes $\texttt{P}$ form a trivial area $\mathcal{T}$. But then, it is possible that $\texttt{triv}_{\text{BS09}}$ is much larger than $\mathcal{T}$. Indeed, the author can apply the same reasoning to $\mathcal{T}$ instead of $\texttt{triv}_{\text{BBLMTU}}$: all boxes $\texttt{P}$ such that $\texttt{OrbitBS09}(\texttt{P})$ intersects $\mathcal{T}$ are trivial. This gives another trivial area $\mathcal{T}'$, and it provides a trivial area $\mathcal{T} \cup \mathcal{T}'$ that may be strictly larger than $\mathcal{T}$. But actually, we show that it is not the case, and that $\texttt{triv}_{\text{BS09}}$ is in fact $\mathcal{T}$:

Proposition III.6 (Expression of $\texttt{triv}_{\text{BS09}}$). *We have:*

$$\texttt{triv}_{\text{BS09}} \;=\; \Big\{\texttt{P} \in \mathcal{NS} : \texttt{OrbitBS09}(\texttt{P}) \cap \texttt{triv}_{\text{BBLMTU}} \neq \emptyset\Big\}. \tag{15}$$

Proof. The particularity of $\texttt{OrbitBS09}$ is that $\texttt{OrbitBS09}(\texttt{P}) = \{\texttt{P}\} \cup \texttt{OrbitBS09}(\texttt{P} \boxtimes \texttt{P})$, so it yields by induction:

$$\forall \texttt{Q} \in \texttt{OrbitBS09}(\texttt{P}), \qquad \texttt{OrbitBS09}(\texttt{P}) \supseteq \texttt{OrbitBS09}(\texttt{Q}).$$

Now, if we start with a non-signalling box $\texttt{P}$ such that $\texttt{OrbitBS09}(\texttt{P})$ does *not* intersect $\texttt{triv}_{\text{BBLMTU}}$, then due to the above inclusion we have that $\texttt{OrbitBS09}(\texttt{Q})$ does not intersect $\texttt{triv}_{\text{BBLMTU}}$ neither for any $\texttt{Q} \in \texttt{OrbitBS09}(\texttt{P})$. As a consequence, none of the points outside of $\mathcal{T}$ can have an orbit intersecting $\mathcal{T}$. Therefore $\mathcal{T}' \subseteq \mathcal{T}$ and $\mathcal{T} = \texttt{triv}_{\text{BS09}}$, which rewrites in (15). □

Lemma III.7 (Local Correlations). *Consider a box $\texttt{P}$ in the affine place $\mathcal{P} \subseteq \mathcal{B}$, and recall that the notation $\mathcal{L} \subseteq \mathcal{B}$ designates the subset of local correlations. We denote $\texttt{xyCoord}(\texttt{P})$ and $\texttt{xyCoord}(\mathcal{L})$ their respective projection into the CHSH–CHSH′ plane. If $\texttt{xyCoord}(\texttt{P}) \in \texttt{xyCoord}(\mathcal{L})$, then $\texttt{P} \in \mathcal{L}$.*

Remark III.8. This lemma is not obvious. For instance, we know that the extremal point $\texttt{P}_{\text{NL}}^{0,1,0}$ of the polytope $\mathcal{NS}$ is projected to the point $\left(\frac{1}{2}, \frac{1}{2}\right)$, which is the center of the square of local correlations in the CHSH-CHSH′ plane, although it is highly non-local since this box is not even a quantum correlation...

Proof. We know that $\mathcal{L}$ is convex polytope of $\mathcal{B}$, so its intersection $\mathcal{L} \cap \mathcal{P}$ with the affine plane $\mathcal{P}$ is a convex polygon, which can be written as the convex hull of some $\texttt{Q}_1, \dots, \texttt{Q}_n \in \mathcal{L} \cap \mathcal{P}$. Write $\texttt{A}_1, \dots, \texttt{A}_n$ their respective projections onto the CHSH-CHSH′ plane. As $\texttt{xyCoord}$ is a affine bijection (see page 22), it preserves barycenters, so $\texttt{xyCoord}(\mathcal{L} \cap \mathcal{P})$ is precisely the convex hull of $\{\texttt{A}_1, \dots, \texttt{A}_n\}$, and we have:

$$\begin{aligned} &\texttt{P} \in \mathcal{L} \cap \mathcal{P} = \text{ConvHull}\Big\{\texttt{Q}_1, \dots, \texttt{Q}_n\Big\} \\ &\quad\iff \qquad \texttt{xyCoord}(\texttt{P}) \in \text{ConvHull}\Big\{\texttt{A}_1, \dots, \texttt{A}_n\Big\} = \texttt{xyCoord}(\mathcal{L} \cap \mathcal{P}) \overset{\text{by bij.}}{=} \texttt{xyCoord}(\mathcal{L}) \cap \texttt{xyCoord}(\mathcal{P}). \end{aligned}$$

But $\texttt{P} \in \mathcal{P}$ by assumption, so $\texttt{xyCoord}(\texttt{P}) \in \texttt{xyCoord}(\mathcal{P})$ and the wanted implication yields (with its converse). □

Theorem III.9 (Conjecture 1 holds). $\widetilde{\texttt{Orbit}}$ *gives rise to new trivial boxes.*

Proof. The intuition behind this proof is based on Graphic III.(e). As in the graphic, we consider the strating box $\texttt{P} \in \mathcal{P}$ with coordinates $(0.65, 0.841)$ in the CHSH–CHSH′ plane. Recall the notation $\texttt{P}^{\boxtimes k} := \big(\big((\texttt{P} \boxtimes \texttt{P}) \boxtimes \texttt{P}\big) \cdots\big) \boxtimes \texttt{P}$. On the one hand, we see that for instance the element $\texttt{P}^{\boxtimes 8}$ of $\widetilde{\texttt{Orbit}}(\texttt{P}) \subseteq \texttt{Orbit}(\texttt{P})$ is in $\texttt{triv}_{\text{BBLMTU}}$, since $\texttt{P}^{\boxtimes 8}$ has ordinate $\approx 0.911 > 0.908 \approx \frac{3+\sqrt{6}}{6}$.
On the other hand, it remains to verify that $\texttt{P} \notin \texttt{triv}_{\text{BS09}}$. By Proposition III.6, it suffices to show that $\texttt{OrbitBS09}(\texttt{P})$ does not intersect $\texttt{triv}_{\text{BBLMTU}}$. We take again notations from page 23. None of the points $\texttt{P}_1, \dots, \texttt{P}_9$ are in the trivial region $\texttt{triv}_{\text{BBLMTU}}$. Moreover, the point $\texttt{P}_{10}$ has (x, y)-coordinates $\approx (0.50, 0.50)$, so it lies in the convex hull of $\texttt{SR}$ and $\frac{1}{4}$-isoNLB and $\overline{\texttt{SR}}$ and $\frac{3}{4}$-isoNLB when projected in the CHSH-CHSH′ plane. But those four boxes are local correlations, so $\texttt{xyCoord}(\texttt{P}_{10}) \in \texttt{xyCoord}(\mathcal{L})$ and by the previous lemma we obtain that $\texttt{P}_{10}$ is local. Now, since the set $\mathcal{L}$ is closed under wirings [ABL+09], we have that all $\texttt{P}_k$ must as well belong $\mathcal{L}$ for $k \geq 10$, and therefore they will never reach the trivial area $\texttt{triv}_{\text{BBLMTU}}$. This shows that

the starting box $\mathtt{P}$ could not be proved to be trivial using uniquely the protocols from [BS09] and [BBL+06]. Hence $\mathtt{P}$ is a new trivial box. □

Conjectures 2 and 3 hold. Conjectures 2 and 3 were about alignement and parallelism of the $\mathtt{Orbit}_k(\mathtt{P})$'s. Let us show the result in the easier case of $\widetilde{\mathtt{Orbit}}_k(\mathtt{P})$:

Proposition III.10 (Conjectures 2 and 3 hold). *For all $k \geq 3$, points of $\widetilde{\mathtt{Orbit}}_k(\mathtt{P})$ are aligned on a line $\mathcal{L}_k$ that is parallel to the diagonal $\mathcal{L}_D$ of the blue triangle.*

Remark III.11. Similarly, we will denote $\mathcal{L}_1$ (resp. $\mathcal{L}_2$) the line passing through the only element of $\widetilde{\mathtt{Orbit}}_1(\mathtt{P})$ (resp. $\widetilde{\mathtt{Orbit}}_2(\mathtt{P})$) and that is parallel to the diagonal $\mathcal{L}_D$.

Remark III.12. By abusing the notation, we will not make a different between a box $\mathtt{P}$ in the affine plane $\mathcal{P}$ and its projection into the CHSH–CHSH′ plane. Indeed, we can assimilate them because we saw that the change of coordinate maps are affine bijections, see (12), and we know that affine transformations preserve alignement and parallelism.

Lemma III.13 (Parallelism). *Consider four points $\mathtt{A},\mathtt{B},\mathtt{C},\mathtt{D}$ such that $\langle \mathtt{A},\mathtt{B}\rangle \parallel \langle \mathtt{C},\mathtt{D}\rangle$, where $\langle \mathtt{A},\mathtt{B}\rangle$ denotes the line passing through $\mathtt{A}$ and $\mathtt{B}$ and "$\parallel$" means "is parallel to". Then $\langle \mathtt{A}\boxtimes\mathtt{P}, \mathtt{B}\boxtimes\mathtt{P}\rangle \parallel \langle \mathtt{C}\boxtimes\mathtt{P}, \mathtt{D}\boxtimes\mathtt{P}\rangle$ and $\langle \mathtt{P}\boxtimes\mathtt{A}, \mathtt{P}\boxtimes\mathtt{B}\rangle \parallel \langle \mathtt{P}\boxtimes\mathtt{C}, \mathtt{P}\boxtimes\mathtt{D}\rangle$.*

Proof. It suffices to notice that the maps $\mathtt{X}\mapsto \mathtt{X}\boxtimes\mathtt{P}$ and $\mathtt{X}\mapsto \mathtt{P}\boxtimes\mathtt{X}$ are affine, so that they preserve parallelism. Denoting $\mathtt{P} = \binom{p_1}{p_2}$ and $\mathtt{X} = \binom{x}{y}$ in the barycentric coordinate system $\binom{\xi}{\gamma}$ of $\mathcal{P}$, we have:

$$\begin{aligned}
\mathtt{X}\boxtimes\mathtt{P} &= \begin{pmatrix} \frac{1}{2} - \frac{p_2}{2} \\ \frac{1}{2} - p_1 - \frac{p_2}{2} \end{pmatrix} + \begin{pmatrix} \frac{1}{2} + p_1 + \frac{3}{2}p_2 & 0 \\ -\frac{1}{2} + p_1 + \frac{p_2}{2} & -1 + 2p_1 + 2p_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \\
\mathtt{P}\boxtimes\mathtt{X} &= \begin{pmatrix} \frac{1}{2} - \frac{p_1}{2} \\ \frac{1}{2} - \frac{p_1}{2} - p1 \end{pmatrix} + \begin{pmatrix} p_1 & -\frac{1}{2} + \frac{3}{2}p_1 \\ -1 + p_1 + 2\,p_2 & -\frac{1}{2} + \frac{p_1}{2} + 2\,p_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},
\end{aligned}$$

which are both affine as a sum of a translation and a linear map. □

Remark III.14. Hence, the map $\mathtt{X}\mapsto\mathtt{X}\boxtimes\mathtt{P}$ is injective (and therefore bijective) *if, and only if,* the determinant of the matrix is not null, *if, and only if,* $\frac{1}{2} + p_1 + \frac{3}{2}p_2 \neq 0$ and $-1 + 2p_1 + 2p_2 \neq 0$.

Lemma III.15 (Alignement). *Consider three points $\mathtt{A},\mathtt{B},\mathtt{C}$ that are aligned. Then, (1) after right multiplication by $\mathtt{P}$, the points $\mathtt{A}\boxtimes\mathtt{P}, \mathtt{B}\boxtimes\mathtt{P}, \mathtt{C}\boxtimes\mathtt{P}$ are aligned on a line $\mathcal{L}$. (2) Similarly after left multiplication: $\mathtt{P}\boxtimes\mathtt{A}, \mathtt{P}\boxtimes\mathtt{B}, \mathtt{P}\boxtimes\mathtt{C}$ are aligned on a line $\mathcal{L}'$. (3) If in addition the line $\langle \mathtt{A},\mathtt{B}\rangle$ is parallel to the diagonal $\mathcal{L}_D$, then $\mathcal{L} = \mathcal{L}'$, meaning that the previous six points are all aligned on a same line $\mathcal{L}$. Moreover, the line $\mathcal{L}$ is parallel to the line $\mathcal{L}_D$.*

Proof. Assertions (1) and (2) follow directly from the fact that the maps $\mathtt{X}\mapsto\mathtt{X}\boxtimes\mathtt{P}$ and $\mathtt{X}\mapsto\mathtt{P}\boxtimes\mathtt{X}$ are affine, see previous proof. Let us prove (3). Supposing that $\mathtt{A}$ and $\mathtt{B}$ are distinct points of the linear plane CHSH–CHSH′, the assumption $\langle \mathtt{A},\mathtt{B}\rangle \parallel \mathcal{L}_D$ means that the slopes of those two lines are the same. So if we write $\mathtt{A} = (a_1, a_2)$ and $\mathtt{B} = (b_1, b_2)$ in the cartesian coordinate system (x, y) of CHSH–CHSH′, we must have $\frac{a_2 - b_2}{a_1 - b_1} = -1$, that is $b_2 = a_1 + a_2 - b_1$. Recall that the operation $\boxtimes$ was defined in $\mathcal{P}$, see (14), and that we applied the coordinate change maps (12) to define its equivalent operation $\boxtimes_{\mathtt{CHSH}}$ in CHSH–CHSH′. Now, writing $\mathtt{A} = (a_1, a_2)$ and $\mathtt{B} = (b_1, a_1 + a_2 - b_1)$ and $\mathtt{P} = (p_1, p_2)$ in the (x, y)-coordinates, we interpolate the points $\mathtt{A}\boxtimes_{\mathtt{CHSH}}\mathtt{P}$ and $\mathtt{B}\boxtimes_{\mathtt{CHSH}}\mathtt{P}$ in order to figure out the equation of the line $\mathcal{L}$ passing through them, and we obtain:

$$\mathcal{L}: \quad x + y \;=\; 1 + 2(a_1 + a_2 - 1)(-1 + p_1 + p_2). \tag{16}$$

Note that this equation implies that the slope of $\mathcal{L}$ is -1, the same as $\mathcal{L}_D$'s one, which tells us right away that $\mathcal{L}$ is parallel to $\mathcal{L}_D$. Finally, in order to show that $\mathcal{L} = \mathcal{L}'$, it suffices to check that both point $\mathtt{P}\boxtimes_{\mathtt{CHSH}}\mathtt{A}$ and $\mathtt{P}\boxtimes_{\mathtt{CHSH}}\mathtt{B}$ satisfies the above equation. It is well the case for $\mathtt{P}\boxtimes_{\mathtt{CHSH}}\mathtt{A}$ (and therefore for $\mathtt{P}\boxtimes_{\mathtt{CHSH}}\mathtt{B}$ by symmetry of the problem) because:

$$\mathtt{P}\boxtimes_{\mathtt{CHSH}}\mathtt{A} \;=\; \frac{1}{8}\begin{pmatrix} 12 - 16p_1 + a_1(-9 + 22p_1 - 2p_2) + a_2(-7 + 10p_1 + 2p_2) \\ 12 - 16p_2 + a_1(-7 - 6p_1 + 18p_2) + a_2(-9 + 6p_1 + 14p_2) \end{pmatrix}.$$

Hence $\mathcal{L} = \mathcal{L}'$, which concludes the proof. □

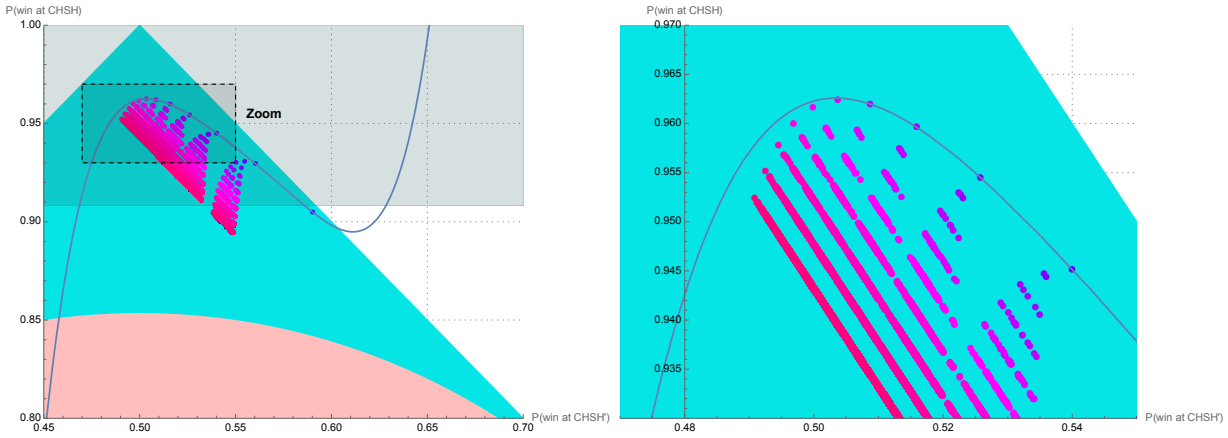
Proof. (Proposition III.10). We proceed by induction on the order k of the orbit $\widetilde{\texttt{Orbit}}_k(\texttt{P})$. We have that $\widetilde{\texttt{Orbit}}_3(\texttt{P})$ contains at most two elements, namely $\texttt{A} = \texttt{P} \boxtimes (\texttt{P} \boxtimes \texttt{P})$ and $\texttt{B} = (\texttt{P} \boxtimes \texttt{P}) \boxtimes \texttt{P}$. If this orbit contains only one element, by convention we take $\mathcal{L}_3$ to be the line passing through this point and that is parallel to the diagonal $\mathcal{L}_D$. Otherwise, we obviously have that $\texttt{A}$ and $\texttt{B}$ are aligned on a line $\mathcal{L}_3$, and it remains to show that $\mathcal{L}_3 \parallel \mathcal{L}_D$. As in previous proof, it suffices to show that the slope is -1, *i.e.* that $a_1 + a_2 = b_1 + b_2$, and it is the case since:

$$\texttt{A} = \frac{1}{4}\begin{pmatrix} 1 + 10p_1^3 + 3p_2 - 4p_2^2 + p_1^2(-13 + 21p_2) + 2p_1(3 - 8p_2 + 6p_2^2) \\ -1 + 6p_1^3 + 9p_2 - 20p_2^2 + 16p_2^3 + p_1^2(-11 + 27p_2) + p_1(6 - 32p_2 + 36p_2^2) \end{pmatrix},$$

$$\texttt{B} = \frac{1}{4}\begin{pmatrix} 1 + 4p_1^3 + 2p_2 - 3p_2^2 + 4p_1^2(-1 + 3p_2) + p_1(3 - 8p_2 + 9p_2^2) \\ -1 + 12p_1^3 + 10p_2 - 21p_2^2 + 16p_2^3 + 4p_1^2(-5 + 9p_2) + p_1(9 - 40p_2 + 39p_2^2) \end{pmatrix},$$

where $\texttt{P} = (p_1, p_2)$, in the (x, y)-coordinates. Hence initialization is done.
Now, suppose the result holds until some $k \geq 3$. Again, if $\widetilde{\texttt{Orbit}}_{k+1}(\texttt{P})$ contains only one element, we make a similar convention for $\mathcal{L}_{k+1}$ as before. Otherwise, by the Alignement Lemma applied to $\texttt{A}, \texttt{B}, \texttt{C}$ any elements of $\widetilde{\texttt{Orbit}}_k(\texttt{P})$, we well have that the points of $\widetilde{\texttt{Orbit}}_{k+1}(\texttt{P})$ are aligned on some line $\mathcal{L}_{k+1}$ that is parallel to $\mathcal{L}_D$. In addition, applying the Parallelism Lemma to the two lines $\mathcal{L}_{k-1} \parallel \mathcal{L}_k$ (they are parallel by transitivity because each of them is parallel to $\mathcal{L}_D$), we have $\mathcal{L}_{k-1} \boxtimes \texttt{P} \parallel \mathcal{L}_k \boxtimes \texttt{P}$, which means $\mathcal{L}_k \parallel \mathcal{L}_{k+1}$. Therefore, again by transitivity we have that $\mathcal{L}_{k+1}$ is parallel to the diagonal $\mathcal{L}_D$, which ends the proof. □

Conjecture 4 does not hold. Counterintuitively, the $\texttt{P}_{\max,k}$'s do not form a parabola, and more generally they do not even belong to a polynomial curve of degree ≤ 5. Indeed, here is a graphin obtained by interpolating the $\texttt{P}_{\max,k}$'s for $k = 1, ..., 6$:



Graphic III.(f) — Polynomial interpolation of the $\texttt{P}_{\max,k}$ fails. The graph on the right is a zoom of the one on the left.

As well, we tried an approach using sin and cos functions but it failed to fit the curve.

III.(5) Expression of $\texttt{P}_{\max,k}$

We define $\texttt{P}_{\max,k}$ as the highest point of $\widetilde{\texttt{Orbit}}_k(\texttt{P})$, "highest" in the sense of having the largest ordinate in the (x, y)-coordinates. Numerically, we can observe that the $\texttt{P}_{\max,k}$'s seem as well to be the highest points of the much larger $\texttt{Orbit}_k(\texttt{P})$, but the proof is more challenging. This is the reason why it is not a big deal to restrict our study to $\widetilde{\texttt{Orbit}}_k(\texttt{P})$. Those highest points are particularly interesting since one of the orbit points that reaches the trivial area (when it occurs) is of the form $\texttt{P}_{\max,k}$. By symmetry of the diagram, we will restrict our study to the up-right part of the graph, defined in the (x, y)-coordinates by:

$$\mathcal{A} := \left(\left[\tfrac{1}{2}, \tfrac{3}{4}\right] \times \left[\tfrac{3}{4}, 1\right] \right) \cap \mathcal{NS} \subseteq \texttt{CHSH–CHSH}' \text{ plane.}$$

Theorem III.16 (Expression of $\mathtt{P}_{\max,k}$). *For any $k \geq 1$ and any box $\mathtt{P} \in \mathcal{A}$, the point $\mathtt{P}_{\max,k}$ is the k-times product on the right of $\mathtt{P}$:*

$$\mathtt{P}_{\max,k} \;=\; \Big(\big((\mathtt{P} \boxtimes \mathtt{P}) \boxtimes \mathtt{P}\big) \cdots \Big) \boxtimes \mathtt{P} \;=:\; \mathtt{P}^{\boxtimes k}.$$

Lemma III.17 (Multiplication by P preserves the height order). *Let $\mathtt{P} \in \mathcal{A}$, and let $\mathtt{Q}, \mathtt{R} \in \mathcal{B}$ such that the line $\langle \mathtt{Q}, \mathtt{R} \rangle$ is parallel to the diagonal $\mathcal{L}_D$. If* Ordinate($\mathtt{Q}$) $\leq$ Ordinate($\mathtt{R}$)*, then:*

$$\text{Ordinate}(\mathtt{Q} \boxtimes \mathtt{P}) \leq \text{Ordinate}(\mathtt{R} \boxtimes \mathtt{P}) \quad \textit{and} \quad \text{Ordinate}(\mathtt{P} \boxtimes \mathtt{Q}) \leq \text{Ordinate}(\mathtt{P} \boxtimes \mathtt{R}).$$

Proof. Write $\mathtt{P} = \binom{p_1}{p_2}$ and $\mathtt{Q} = \binom{q_1}{q_2}$ and $\mathtt{R} = \binom{r_1}{r_2}$ in the (x,y)-coordinates. By the parallelism assumption, the slope of the line $\langle \mathtt{Q}, \mathtt{R} \rangle$ must be -1, so $q_1 + q_2 = r_1 + r_2$ and therefore we may write $\mathtt{R} = (r_1,\, q_1 + q_2 - r_1)$. After simplification, we have:

$$\begin{aligned}
\text{Ordinate}(\mathtt{R} \boxtimes \mathtt{P}) - \text{Ordinate}(\mathtt{Q} \boxtimes \mathtt{P}) \;&=\; \Big(-2 + 3\,p_1 + p_2\Big)\Big(q_1 - r_1\Big).\\
\text{Ordinate}(\mathtt{P} \boxtimes \mathtt{R}) - \text{Ordinate}(\mathtt{P} \boxtimes \mathtt{Q}) \;&=\; \tfrac{1}{4}\Big(-1 + 6\,p_1 - 2\,p_2\Big)\Big(q_1 - r_1\Big).
\end{aligned}$$

Let us check that the first product is ≥ 0, and it is similar for the second one. On the one hand, as $\mathtt{P} \in \mathcal{A}$, we have $p_1 \geq \frac{1}{2}$ and $p_2 \geq \frac{3}{4}$, so the first factor is $\geq \frac{1}{4} \geq 0$. On the other hand, by the parallelism assumption, the second factor is actually $r_2 - q_2$, which is ≥ 0 if Ordinate($\mathtt{Q}$) $\leq$ Ordinate($\mathtt{R}$). □

Lemma III.18 (Lines move to the left). *The distance between the line $\mathcal{L}_k$ and the diagonal $\mathcal{L}_D$ increases as k increases, and it is bounded:*

$$k \leq \ell \quad \Longrightarrow \quad d\Big(\mathcal{L}_1, \mathcal{L}_D\Big) \leq d\Big(\mathcal{L}_k, \mathcal{L}_D\Big) \leq d\Big(\mathcal{L}_\ell, \mathcal{L}_D\Big) < d\Big(\mathcal{L}_\infty, \mathcal{L}_D\Big),$$

where $\mathcal{L}_\infty :\; x + y = 1$ is the line passing through $(\frac{1}{2}, \frac{1}{2})$ and that is parallel to $\mathcal{L}_D$.

Remark III.19. By construction in Proposition III.10, recall that the line $\mathcal{L}_k$ must intersect the set $\mathcal{NS}$ of non-signalling correlations. Hence, the fact that $d\big(\mathcal{L}_k, \mathcal{L}_D\big)$ increases as k increases is equivalent to saying "$\mathcal{L}_k$ goes to the left" and not "to the right" as k increases.

Proof. Let $\mathtt{P} \in \mathcal{A}$ and write $\mathtt{P} = (p_1, p_2)$ in the (x,y)-coordinates. *First, we prove the last inequality by induction on $\ell \geq 1$.* As $\mathcal{L}_1 \parallel \mathcal{L}_\infty$, it suffices to show that the y-intercept of $\mathcal{L}_1$ is greater than the one of $\mathcal{L}_\infty$, *i.e.* that $p_1 + p_2 > 1$. But $\mathtt{P} \in \mathcal{A}$ gives $p_1 \geq \frac{1}{2}$ and $p_2 \geq \frac{3}{4}$ so that $p_1 + p_2 \geq \frac{5}{4} > 1$. Now, suppose that the inequality holds for some $\ell \geq 1$. Let $\mathtt{A} = (a_1, a_2) \in \mathcal{L}_\ell$, which satisfies by assumption $a_1 + a_2 > 1$. In equation (16) from Lemma III.15, we saw that the equation of the line passing through $\mathtt{A} \boxtimes \mathtt{P}$ and that is parallel to $\mathcal{L}_D$ is:

$$\mathcal{L}_{\ell+1} :\quad x + y \;=\; 1 + 2\underbrace{(a_1 + a_2 - 1)}_{>0}\underbrace{(-1 + p_1 + p_2)}_{>0} > 1. \tag{17}$$

Hence $d\big(\mathcal{L}_\ell, \mathcal{L}_D\big) < d\big(\mathcal{L}_\infty, \mathcal{L}_D\big)$ for all $\ell \geq 1$ by induction. *Now, let us show the first and second inequalities.* Without loss of generality, we may assuma that $\ell = k + 1$. Consider $\mathtt{A} = (a_1, a_2) \in \mathcal{L}_k$ and $\mathtt{B} := \mathtt{A} \boxtimes \mathtt{P} = (b_1, b_2) \in \mathcal{L}_{k+1}$, both expressed in the (x,y)-coordinates. We want to show that $a_1 + a_2 \geq b_1 + b_2$. But the expression of $\mathcal{L}_{k+1}$ is given in equation (17), so $b_1 + b_2 = 1 + 2(a_1 + a_2 - 1)(-1 + p_1 + p_2)$, and it yields:

$$(a_1 + a_2) - (b_1 + b_2) \;=\; \Big(a_1 + a_2 - 1\Big)\Big(-1 + 2\,p_1 + 2\,p_2\Big).$$

The first factor is > 0 because we have just shown that $d\big(\mathcal{L}_{k+1}, \mathcal{L}_D\big) < d\big(\mathcal{L}_\infty, \mathcal{L}_D\big)$, and the second factor is ≥ 0 because $\mathtt{P} \in \mathcal{A}$. Hence the wanted result. □

Lemma III.20 (Multiplication to the right is higher). *For any $\mathtt{P} \in \mathcal{A}$ and $\mathtt{Q} \in \widetilde{\mathtt{Orbit}}(\mathtt{P})$ such that* Abscissa($\mathtt{Q}$) $\leq$ Abscissa($\mathtt{P}$)*, we have:*

$$\text{Ordinate}\Big(\mathtt{Q} \boxtimes \mathtt{P}\Big) \;\geq\; \text{Ordinate}\Big(\mathtt{P} \boxtimes \mathtt{Q}\Big).$$

Proof. Fix $\mathtt{P} = \binom{p_1}{p_2}$ in $\mathcal{A}$ and consider any $\mathtt{Q} = \binom{q_1}{q_2}$ in some $\widetilde{\mathtt{Orbit}}_k(\mathtt{P})$, both expressed in the (x,y)-coordinates. We work out the following difference:

$$\mathrm{Ordinate}\Big(\mathtt{Q}\boxtimes\mathtt{P}\Big) - \mathrm{Ordinate}\Big(\mathtt{P}\boxtimes\mathtt{Q}\Big) \;=\; 7\,p_2 - 7\,p_1 + 7\,q_1 - 7\,q_2 + 12\,q_2p_1 - 12\,q_1p_2 \;=:\; f(q_1,q_2).$$

We want to show that $f(q_1,q_2)\geq 0$ and the wanted result will yield. On the one hand, by the previous lemma, as $\mathtt{P}\in\mathcal{L}_1$ and $\mathtt{Q}\in\mathcal{L}_k$, we must have $q_1+q_2\leq p_1+p_2$, that is $q_1\leq p_1+p_2-q_2$. On the other hand, we have $\frac{\partial}{\partial q_1}f(q_1,q_2) = 7-12\,p_2$. But $\mathtt{P}\in\mathcal{A}$ implies $p_2\geq\frac{3}{4}$, so $\frac{\partial}{\partial q_1}f\leq -2\leq 0$. Therefore, as q_1 rely on the segment $(-\infty,\,p_1+p_2-q_2]$ and as $f(\cdot,q_2)$ is decreasing for any fixed q_2, it suffices to prove that $f(q_1,q_2)\geq 0$ for $q_1=p_1+p_2-q_2$, or equivalently for $q_2=p_1+p_2-q_1$. After simplification, we have:

$$f\big(q_1,p_1+p_2-q_1\big) \;=\; 12\,\Big(p_1-q_1\Big)\Big(p_1+p_2-\tfrac{7}{6}\Big).$$

But the first factor is ≥ 0 when $\mathrm{Abscissa}(\mathtt{Q})\leq\mathrm{Abscissa}(\mathtt{P})$; and for the second one, as $\mathtt{P}\in\mathcal{A}$, we have $p_1\geq\frac{1}{2}$ and $p_2\geq\frac{3}{4}$ so $p_1+p_2-\frac{7}{6}\geq\frac{1}{12}\geq 0$. Hence $f\big(q_1,p_1+p_2-q_1\big)\geq 0$, which concludes the proof. □

Lemma III.21 ($\mathtt{P}^{\boxtimes k}$ is to the left of $\mathtt{P}$). *For any $\mathtt{P}\in\mathcal{A}$ and $k\geq 1$, we have:*

$$\mathrm{Abscissa}\big(\mathtt{P}^{\boxtimes k}\big)\leq\mathrm{Abscissa}\big(\mathtt{P}\big).$$

Proof. Write $\mathtt{P}=(p_1,\,p_2)\in\mathcal{A}$ in the (x,y)-coordinates. We prove the result by induction on $k\geq 1$. For $k=1$, the result is obvious. For later, we need as well to treat the case $k=2$. We work out the following difference:

$$\mathrm{Abscissa}(\mathtt{P}) - \mathrm{Abscissa}(\mathtt{P}\boxtimes\mathtt{P}) \;=\; \tfrac{1}{8}\Big[-12-22\,p_1^2+33\,p_1-8\,p_1p_2+7\,p_2-2\,p_2^2\Big] \;=:\; f(p_1,\,p_2).$$

Let us show that $f(p_1,p_2)\geq 0$. We compute $\frac{\partial}{\partial p_2}f(p_1,p_2)=\frac{1}{8}(-8p_1+7-4p_2)$. But as $\mathtt{P}\in\mathcal{A}$, we have $p_1\geq\frac{1}{2}$ and $p_2\geq\frac{3}{4}$, so $\frac{\partial}{\partial p_2}f(p_1,p_2)\leq 0$. Therefore $f(p_1,\cdot)$ is decreasing. Now, as $\mathtt{P}\in\mathcal{NS}$, we must have $p_2\leq\frac{3}{2}-p_1$. So it suffices to check that $f(p_1,\frac{3}{2}-p_1)\geq 0$ for all $\frac{1}{2}\leq p_1\leq\frac{3}{4}$, which is the case since $f(p_1,\frac{3}{2}-p_1)=-\frac{1}{32}(p_1-\frac{1}{2})(p_1-\frac{3}{4})$. This ends the case $k=2$.
Now, assume the result holds for some $k\geq 1$. Here $\mathtt{P}=(p_1,p_2)$ is fixed. Denote $\mathtt{Q}=(q_1,q_2)=\mathtt{P}^{\boxtimes k}$ in the (x,y)-coordinates, which satisfies $q_1\leq p_1$ by hypothesis. We have:

$$\begin{aligned}\mathrm{Abscissa}(\mathtt{P}) - \mathrm{Abscissa}(\mathtt{P}^{\boxtimes k+1}) \;&=\; \mathrm{Abscissa}(\mathtt{P}) - \mathrm{Abscissa}(\mathtt{Q}\boxtimes\mathtt{P})\\ &=\; \tfrac{1}{8}\Big[-12+16q_1+7p_2-10q_1p_2-2p_2q_2+17p_1-22p_1q_1+2p_1q_2\Big] =: g(q_1,\,q_2).\end{aligned}$$

As before, we want to show that $g(q_1,\,q_2)\geq 0$, and we use a partial derivative approach. We show that $\frac{\partial}{\partial q_1}g\leq 0$, so $g(\cdot,\,q_2)$ is decreasing, and as we know that $q_1\leq p_1$, it suffices to study the constant case $q_1=p_1$. Then, similarly $\frac{\partial}{\partial q_1}g(p_1,q_2)\leq 0$, so $g(p_1,\cdot)$ decreases. But $q_2\leq p_2$ due to Lemma III.18 and because $q_1\leq p_1$. So it suffices to verify the case $q_2=p_2$, and we already treated this case when we had $k=2$ since $g(p_1,p_2)=f(p_1,p_2)\geq 0$. Hence the result. □

Proof. (Theorem III.16). Let $\mathtt{P}\in\mathcal{A}$. We prove the result by induction on $k\geq 1$. It is obviously true for $k=1$ since $\widetilde{\mathtt{Orbit}}_1(\mathtt{P})$ only contains $\mathtt{P}$. Now, assume that $\mathtt{P}_{\max,\,k}=\mathtt{P}^{\boxtimes k}$ for some $k\geq 1$. On the one hand, applying Lemma III.17 to $\mathtt{R}=\mathtt{P}_{\max,\,k}$ and $\mathtt{Q}$ any box of $\widetilde{\mathtt{Orbit}}_k(\mathtt{P})$ (the parallel hypothesis is satisfied thanks to Proposition III.10), we have:

$$\mathrm{Ordinate}(\mathtt{P}^{\boxtimes k+1}) \;=\; \mathrm{Ordinate}(\mathtt{P}_{\max,\,k}\boxtimes\mathtt{P}) \;\geq\; \mathrm{Ordinate}(\mathtt{Q}\boxtimes\mathtt{P}).$$

On the other hand, combining Lemma III.21 and Lemma III.20, and then using again Lemma III.17, we obtain:

$$\mathrm{Ordinate}(\mathtt{P}^{\boxtimes k+1}) \;=\; \mathrm{Ordinate}(\mathtt{P}^{\boxtimes k}\boxtimes\mathtt{P}) \;\geq\; \mathrm{Ordinate}(\mathtt{P}\boxtimes\mathtt{P}^{\boxtimes k}) \;\geq\; \mathrm{Ordinate}(\mathtt{P}\boxtimes\mathtt{Q}),$$

for any $\mathtt{Q}\in\widetilde{\mathtt{Orbit}}_k(\mathtt{P})$. Hence $\mathrm{Ordinate}(\mathtt{P}^{\boxtimes k+1})\geq\mathrm{Ordinate}(\mathtt{Q})$ for any $\mathtt{Q}$ in $\widetilde{\mathtt{Orbit}}_{k+1}(\mathtt{P})$, which concludes the proof. □

III.(6) New Trivial Boxes

In this subsection, we eventually present the results that we obtained.

Numerical Results. All the work presented above was done in the 2-dimensional slice of $\mathcal{NS}$ containing PR and SR and I. This slice is a good framework because it is stable under our operation $\boxtimes$ by Lemma III.4. The first drawing below corresponds to that slice. We can do a similar work in the 3-dimensional slice containing the four non-coplanar boxes PR and $\mathtt{P}_0 := \mathbb{1}_{a=b=0}$ and $\mathtt{P}_1 := \mathbb{1}_{a=b=1}$ and I, since one can show that this slice is also stable under $\boxtimes$ (consider here the general product formula from (11)). It allows to find many more trivial boxes as drawn below in the second and third graphs. More generally, as we know that $\mathcal{NS}$ is stable under wiring (for consistency of the theory) [ABL+09], we can even apply the same reasoning directly to the whole polytope $\mathcal{NS}$. But as $\mathcal{NS}$ is an 8-dimensional polytope, we would need 8 variables to write a box as a convex combinaison of 9 affinely independent boxes, which is not very convenient. It is more suitable to think of a box P as a tensor T, as explained in Remark I.3. After finding the corresponding formula of $\mathtt{T} \boxtimes \mathtt{T}'$ derived from (11), it can be easily implemented in computer programs to find trivial boxes anywhere in $\mathcal{NS}$, as shown in the two last drawing hereinbelow.

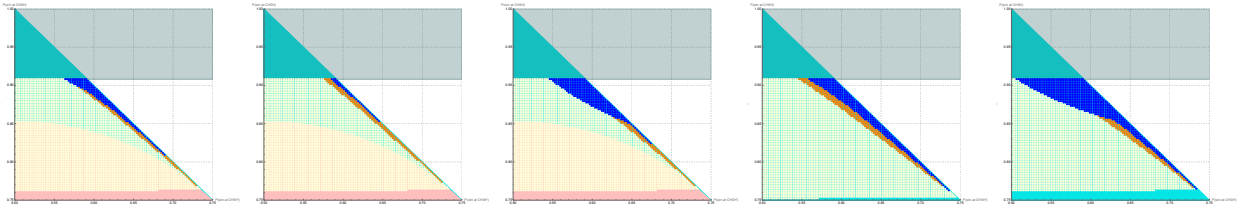


Figure III.(g) — Examples of numerical simulations of some slices of $\mathcal{NS}$. Each time, we consider a slice passing through 3 generating points and we project it in the CHSH–CHSH′ plane. From the left to the right, the 3 generating points are respectively: $\{\mathtt{PR}, \mathtt{SR}, \mathtt{I}\}$, $\{\mathtt{PR}, \mathtt{P}_0, \mathtt{I}\}$, $\{\mathtt{PR}, \mathtt{P}_1, \mathtt{I}\}$, $\{\mathtt{PR}, \mathtt{P}_0, \mathtt{P}_{\mathsf{NL}}^{010}\}$, $\{\mathtt{PR}, \mathtt{P}_1, \overline{\mathtt{PR}'}\}$. Points drawn in **blue** are trivial using recursive pairwise product as in [BS09]; the ones in **orange** are trivial using right multiplication as for $\mathtt{P}_{\max,k}$; and points in **yellow** do not reach the trivial area $\mathtt{triv}_{\mathrm{BBLMTU}}$ drawn in **gray**, so our protocol do not provide information about them. Only the first slice was studied in [BS09].

Explicit Results. It is possible to show that the 2-dimensional slice containing PR and $\mathtt{P}_0 := \mathbb{1}_{a=b=0}$ and $\mathtt{P}_1 := \mathbb{1}_{a=b=1}$ is stable under $\boxtimes$. More precisely, if we write $\mathtt{SR}_\varepsilon := \varepsilon\,\mathtt{P}_0 + (1-\varepsilon)\,\mathtt{P}_1$ and (p,ε)-corNLB $:= p\,\mathtt{PR} + (1-p)\,\mathtt{SR}_\varepsilon$, then we have:

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

$$\text{with} \qquad \widetilde{p} = 2p - p^2 - p\varepsilon + p^2\varepsilon =: f_\varepsilon(p) \qquad \text{and} \qquad \widetilde{\varepsilon} = \frac{2 - 4\varepsilon^2(-1+p) - 2p + \varepsilon(-4+5p)}{2 + 2(-1+\varepsilon)p}.$$

The case $p = 0$ is not interesting since is correspond to some local boxes (indeed, $\mathtt{P}_0$ and $\mathtt{P}_1$ are both local boxes, an by convexity of $\mathcal{L}$, any convex combinaison of $\mathtt{P}_0$ and $\mathtt{P}_1$ is in $\mathcal{L}$ as well), which are therefore non-trivial. Now, for $p > 0$ and $0 \leq \varepsilon < 1$, we have that f_ε has exactly two fixed points: $p = 0$, which is repulsive since $f'_\varepsilon(0) = 2 - \varepsilon > 1$; and $p = 1$, which is attractive since $f'_\varepsilon(1) = \varepsilon < 1$. Hence, applying recursively the operation $\boxtimes$ on (p,ε)-correlated boxes, we obtain a sequence of boxes converging toward the PR box. In particular, there exists a finite step at which the sequence enters in the "triangled-shaped" trivial area $\mathtt{triv}_{\mathrm{BBLMTU}}$, which shows that the starting box (p,ε)-corNLB is trivial when $\varepsilon \neq 1$. Now when $\varepsilon = 1$ we have $\widetilde{p} = p$ and $\widetilde{\varepsilon} = 1 - \frac{p}{2}$. Therefore, as $p \neq 0$, we are reduced to the previous case $0 \leq \widetilde{\varepsilon} < 1$.
This proves the following theorem:

Theorem III.22 (New trivial triangle). *The triangle given by the three boxes* PR *and* $\mathtt{P}_0$ *and* $\mathtt{P}_1$ *is trivial, except boxes in the segment joining* $\mathtt{P}_0$ *to* $\mathtt{P}_1$. □

Remark III.23 (Another algebra of boxes). We also tried another algebra of boxes with the operation $\mathtt{P} \wedge \mathtt{Q}$ defined as feeding P and Q with x and y, taking the AND of the respective outputs. This algebra is commutative and associative, with neutral element $\mathtt{P}_1$. Numerically, it seems that $\mathtt{P}^{\wedge k} \to \mathtt{P}_0$ when $k \to \infty$ for any box P (except $\mathtt{P}_1$). But $\mathtt{P}_0$ is a right identity for $\boxtimes$ and $\boxtimes$ is continuous, so we should have $\mathtt{Q} \boxtimes \mathtt{P}^k \to \mathtt{Q}$ for any boxes P and Q, which might be interesting?...

Conclusions

We have seen an historical overview covering the last two decades, telling the evolution of the link between nonlocal boxes and communication complexity. To this day, we know that all quantum boxes are *non-trivial*, whereas some post-quantum boxes are *trivial*, but the initial question is still open. Our contribution was to define an algebra of boxes in order to enhance the distillation protocol from [BS09] by wiring boxes in a more optimal order: instead of pairwise multiplying boxes, one can multiply only to the right at each iteration, and it gives better results. This technique allowed us not only to numerically enlarge the known trivial area in some slices of the non-signalling polytope $\mathcal{NS}$, but also to find a new explicit trivial area in the boundary of $\mathcal{NS}$: the triangle defined by PR and $\mathtt{P}_0$ and $\mathtt{P}_1$ is trivial, except for boxes in the segment from $\mathtt{P}_0$ to $\mathtt{P}_1$. Note that tensors were a convenient tool to generalize ideas from 2-dimensional slices of $\mathcal{NS}$ to multi-dimensional slices of $\mathcal{NS}$.

A first idea for future researches could be to try to generalize our new trivial triangle to the whole boundary of $\mathcal{NS}$ apart from, of course, boundary points that are local. We can as well study different algebras of boxes by considering other products than $\boxtimes$. A good idea could be to combine many types of products depending on the starting box position, maybe with a machine learning algorithm. Another idea we had was to consider the n-th root of a box (in the sense of right multiplication), so that we may find an explicit expression of the trivial area near the diagonal by taking the n-th root of boxes from $\mathtt{triv}_{\mathrm{BBLMTU}}$. But we are not yet able to conclude with something really convincing using this method. (This method would require to show existence and unicity of such a root. It seems to be the case numerically in a portion of the non-signalling polytope.)

Here are some ideas in order to go further in this work. **(1)** There exist many generalizations of CHSH game: for instance, a version seen as a particular case of magic square game [CMMN20], for which it is know that the same separation $\mathcal{L} \subsetneq \mathcal{Q} \subsetneq \mathcal{NS}$ is displayed; or a more natural way to generalize CHSH by taking inputs and outputs in the finite field $\mathbb{F}_q$ and considering the mod-q sum in the rule [BS15, KST+19], but much less results are known in this context. **(2)** There is a generalization of nonlocal boxes to multi-party nonlocal boxes [BM06, GWAN11]. Note that, for more than two parties, one seems to need more than bipartite principles to capture the quantum set. **(3)** One could consider Generalized Probabilistic Theories (GPTs), which are a class of theories that include classical and quantum theories and that allow for example PR boxes [WC20a, WC20b], . **(4)** There are many variants of the definition of the quantum set $\mathcal{Q}$. We already saw that $\mathcal{Q}_{\mathrm{finite}} = C_q \subsetneq \mathcal{Q} = C_{qa}$ [SLO19, DPP19], but there are also $C_{qa} \subsetneq C_{qc}$ [JNV+21] and $C_{qc} \subsetneq C_{vect}$ [CMR+14]. One could probably use communication complexity to distinguish them in some game? **(5)** It is possible to consider *quantum* communication complexity [Yao93, Kre95, CvDNT99, dW02, Bra03, CvDNT13], in which Alice and Bob communicate *qubits* instead of bits. **(6)** Given a function f, we can count the minimal number of nonlocal boxes required in order for Alice to compute $f(X, Y)$ [KKLR09]. **(7)** Consider another axiom than nontrivial communication complexity to single out $\mathcal{Q}$. See a list of examples at page 10.

I give my acknowledgements to my three advisors, Anne Braodbent, Ion Nechita, Clément Pellegrini, who diligently supported me during my whole master's research programm. As well, I want to highlight the quality of Marc-Olivier Proulx's work in [Pro18], it allowed me to benefit from more hindsight, especially at the beginning of the project. Finally, I express my gratitude to Arthur Mehta, Éric Culf, Faedi Loulidi and Denis Rochette, with whom I had interesting discussions about this work, and more generally to the whole Quasar team from Ottawa and the quantum group from Toulouse. Thank you!

References

[ABL+09] Jonathan Allcock, Nicolas Brunner, Noah Linden, Sandu Popescu, Paul Skrzypczyk, and Tamás Vértesi. Closed sets of nonlocal correlations. *Phys. Rev. A*, 80:062107, Dec 2009. DOI: 10.1103/PhysRevA.80.062107.

[ABPS09] Jonathan Allcock, Nicolas Brunner, Marcin Pawlowski, and Valerio Scarani. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Phys. Rev. A*, 80:040103, Oct 2009. DOI: 10.1103/PhysRevA.80.040103.

[AGM06] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97:120405, Sep 2006. DOI: 10.1103/PhysRevLett.97.120405.

[AGR82] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's

inequalities. *Phys. Rev. Lett.*, 49:91–94, Jul 1982. DOI: 10.1103/PhysRevLett.49.91.

[Bar07] Jonathan Barrett. Information processing in generalized probabilistic theories. *Phys. Rev. A*, 75:032304, Mar 2007. DOI: 10.1103/PhysRevA.75.032304.

[BBL+06] Gilles Brassard, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Phys. Rev. Lett.*, 96:250401, Jun 2006. DOI: 10.1103/PhysRevLett.96.250401.

[BBLW07] Howard Barnum, Jonathan Barrett, Matthew Leifer, and Alexander Wilce. Generalized no-broadcasting theorem. *Phys. Rev. Lett.*, 99:240501, Dec 2007. DOI: 10.1103/PhysRevLett.99.240501.

[BCMdW10] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Rev. Mod. Phys.*, 82:665–698, Mar 2010. DOI: 10.1103/RevModPhys.82.665.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. DOI: 10.1103/RevModPhys.86.419.

[BCvD01] Harry Buhrman, Richard Cleve, and Wim van Dam. Quantum entanglement and communication complexity. *SIAM Journal on Computing*, 30(6):1829–1841, 2001. DOI: 10.1137/S0097539797324886.

[BCW98] Harry Buhrman, Richard Cleve, and Avi Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 63–68, New York, NY, USA, 1998. Association for Computing Machinery. DOI: 10.1145/276698.276713.

[Bel64] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. DOI: 10.1103/PhysicsPhysiqueFizika.1.195.

[Bel90] JS Bell. La nouvelle cuisine, w: Between science and technology, red. a. sarlemijn, p. kroes, 1990.

[BG15] Salman Beigi and Amin Gohari. Monotone measures for non-local correlations. *IEEE Transactions on Information Theory*, 61(9):5185–5208, 2015. Under the supervision of Anne Broadbent and David Poulin. DOI: 10.1109/TIT.2015.2452253.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005. DOI: 10.1103/PhysRevLett.95.010503.

[BLM+05] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71:022101, Feb 2005. DOI: 10.1103/PhysRevA.71.022101.

[BM06] Anne Broadbent and André Allan Méthot. On the power of non-local boxes. *Theoretical Computer Science*, 358(1):3–14, 2006. DOI: 10.1016/j.tcs.2005.08.035.

[Bra03] Gilles Brassard. Quantum communication complexity. *Foundations of Physics*, 33(11):1593–1616, 2003. DOI: 10.1023/A:1026009100467.

[Bra05] Gilles Brassard. Is information the key? *Nature Physics*, 1(1):2–4, 2005. DOI: 10.1038/nphys134.

[Bra11] Cyril Branciard. Detection loophole in bell experiments: How postselection modifies the requirements to observe nonlocality. *Phys. Rev. A*, 83:032123, Mar 2011. DOI: 10.1103/PhysRevA.83.032123.

[Bro16] Anne Broadbent. Popescu-rohrlich correlations imply efficient instantaneous nonlocal quantum computation. *Phys. Rev. A*, 94:022318, Aug 2016. DOI: 10.1103/PhysRevA.94.022318.

[BS09] Nicolas Brunner and Paul Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Physical Review Letters*, 102(16), Apr 2009. DOI: 10.1103/PhysRevLett.102.160403.

[BS15] Mohammad Bavarian and Peter W. Shor. Information causality, szemerédi-trotter and algebraic variants of chsh. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, ITCS '15, page 123–132, New York, NY, USA, 2015. Association for Computing Machinery. DOI: 10.1145/2688073.2688112.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992. DOI: 10.1103/PhysRevLett.69.2881.

[Cab05] Adán Cabello. How much larger quantum correlations are than classical ones. *Phys. Rev. A*, 72:012113, Jul 2005. DOI: 10.1103/PhysRevA.72.012113.

[CB97] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Phys. Rev. A*, 56:1201–1204, Aug 1997. DOI: 10.1103/PhysRevA.56.1201.

[CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988. DOI: 10.1137/0217015.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. DOI: 10.1103/PhysRevLett.23.880.

[Cir80] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980. DOI: 10.1007/BF00417500.

[CLB+15] Bradley G. Christensen, Yeong-Cherng Liang, Nicolas Brunner, Nicolas Gisin, and Paul G. Kwiat. Exploring the limits of quantum nonlocality with entangled photons. *Phys. Rev. X*, 5:041052, Dec 2015. DOI: 10.1103/PhysRevX.5.041052.

[CMMN20] David Cui, Arthur Mehta, Hamoon Mousavi, and Seyed Sajjad Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4:346, October 2020. DOI: 10.22331/q-2020-10-21-346.

[CMR+14] Toby Cubitt, Laura Mancinska, David E. Roberson, Simone Severini, Dan Stahlke, and Andreas Winter. Bounds on entanglement-assisted source-channel coding via the lovász ϑ number and its variants. *IEEE Transactions on Information Theory*, 60(11):7330–7344, 2014. DOI: 10.1109/TIT.2014.2349502.

[CS78] J F Clauser and A Shimony. Bell's theorem. experimental tests and implications. *Reports on Progress in Physics*, 41(12):1881–1927, dec 1978. DOI: 10.1088/0034-4885/41/12/002.

[CvDNT99] Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp. *Quantum Entanglement and the Communication Complexity of the Inner Product Function*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999. Pages 61–74. DOI: 10.1007/3-540-49208-9_4.

[CvDNT13] Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. *Theoretical Computer Science*, 486:11–19, 2013. DOI: 10.1016/j.tcs.2012.12.012.

[Dir39] P. A. M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(3):416–418, 1939. DOI: 10.1017/S0305004100021162.

[DLTW08] Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 199–210, 2008. DOI: 10.1109/CCC.2008.26.

[DPP19] Ken Dykema, Vern I. Paulsen, and Jitendra Prakash. Non-closure of the set of quantum correlations via graphs. *Communications in Mathematical Physics*, 365(3):1125–1142, 2019. DOI: 10.1007/s00220-019-03301-1.

[dW02] Ronald de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337–353, 2002. DOI: 10.1016/S0304-3975(02)00377-8.

[DW08] Dejan D. Dukaric and Stefan Wolf. A limit on nonlocality distillation, 2008. DOI: 10.48550/ARXIV.0808.3317.

[Ein05a] A. Einstein. Über einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt. *Annalen der Physik*, 322(6):132–148, 1905. DOI: 10.1002/andp.19053220607.

[Ein05b] Albert Einstein. On the electrodynamics of moving bodies. *Annalen der physik*, 17(10):891–921, 1905. URL: http://fisica.ufpr.br/mossanek/etc/specialrelativity.pdf.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. DOI: 10.1103/PhysRev.47.777.

[EWC22] Giorgos Eftaxias, Mirjam Weilenmann, and Roger Colbeck. Advantages of multi-copy nonlocality distillation and its application to minimizing communication complexity, 2022. DOI: 10.48550/ARXIV.2206.02817.

[FSA+13] T. Fritz, A. B. Sainz, R. Augusiak, J Bohr Brask, R. Chaves, A. Leverrier, and A. Acín. Local orthogonality as a multipartite principle for quantum correlations. *Nature Communications*, 4(1):2263, 2013. DOI: 10.1038/ncomms3263.

[FWW09] Manuel Forster, Severin Winkler, and Stefan Wolf. Distilling nonlocality. *Phys. Rev. Lett.*, 102:120401, Mar 2009. DOI: 10.1103/PhysRevLett.102.120401.

[GA17] Rodrigo Gallego and Leandro Aolita. Nonlocality free wirings and the distinguishability between bell boxes. *Phys. Rev. A*, 95:032118, Mar 2017. DOI: 10.1103/PhysRevA.95.032118.

[GKW+18] Koon Tong Goh, J ędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018. DOI: 10.1103/PhysRevA.97.022104.

[GNTZ11] S. Goldstein, T. Norsen, D. Victor Tausk, and N. Zanghi. Bell's theorem. *Scholarpedia*, 6(10):8378, 2011. DOI: 10.4249/scholarpedia.8378.

[GWAN11] Rodrigo Gallego, Lars Erik Würflinger, Antonio Acín, and Miguel Navascués. Quantum correlations require multipartite information principles. *Phys. Rev. Lett.*, 107:210403, Nov 2011. DOI: 10.1103/PhysRevLett.107.210403.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015. DOI: 10.1038/nature15759.

[Hol73] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. ZMATH: 0317.94003.

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip* = re. *Commun. ACM*, 64(11):131–138, oct 2021. DOI: 10.1145/3485628.

[Kar21] Martti Karvonen. Neither contextuality nor nonlocality admits catalysts. *Phys. Rev. Lett.*, 127:160402, Oct 2021. DOI: 10.1103/PhysRevLett.127.160402.

[KKLR09] Marc Kaplan, Iordanis Kerenidis, Sophie Laplante, and Jérémie Roland. Non-local box complexity and secure function evaluation. *arXiv*, 2009. DOI: 10.48550/ARXIV.0903.2179.

[KN96] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1996. DOI: 10.1017/CBO9780511574948.

[Kre95] Ilan Kremer. Quantum communication. *The Hebrew University of Jerusalem*, Master's Thesis, 1995.

[KST+19] Jędrzej Kaniewski, Ivan Supić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum*, 3:198, October 2019. DOI: 10.22331/q-2019-10-24-198.

[KT92] Leonid A. Khalfin and Boris S. Tsirelson. Quantum/classical correspondence in the light of bell's inequalities. *Foundations of Physics*, 22(7):879–948, 1992. DOI: 10.1007/BF01889686.

[Kus97] Eyal Kushilevitz. *Communication Complexity*, volume 44, pages 331–360. Elsevier, 1997. DOI: 10.1016/S0065-2458(08)60342-3.

[Lan88] Lawrence J. Landau. Empirical two-point correlation functions. *Foundations of Physics*, 18(4):449–460, 1988. DOI: 10.1007/BF00732549.

[LPSW07] Noah Linden, Sandu Popescu, Anthony J. Short, and Andreas Winter. Quantum nonlocality and beyond: Limits from nonlocal computation. *Phys. Rev. Lett.*, 99:180502, Oct 2007. DOI: 10.1103/PhysRevLett.99.180502.

[LVN14] Ben Lang, Tamás Vértesi, and Miguel Navascués. Closed sets of correlations: answers from the zoo. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424029, oct 2014. DOI: 10.1088/1751-8113/47/42/424029.

[MAG06] Ll. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Phys. Rev. A*, 73:012112, Jan 2006. DOI: 10.1103/PhysRevA.73.012112.

[Mas03] Ll. Masanes. Necessary and sufficient condition for quantum-generated correlations, 2003. DOI: 10.48550/arXiv.quant-ph/0309137.

[Mas06] Lluís Masanes. Asymptotic violation of bell inequalities and distillability. *Phys. Rev. Lett.*, 97:050503, Aug 2006. DOI: 10.1103/PhysRevLett.97.050503.

[Mor16] Ryuhei Mori. Three-input majority function as the unique optimal function for the bias amplification using nonlocal boxes. *Phys. Rev. A*, 94:052130, Nov 2016. DOI: 10.1103/PhysRevA.94.052130.

[NGHA15] Miguel Navascués, Yelena Guryanova, Matty J. Hoban, and Antonio Acín. Almost quantum correlations. *Nature Communications*, 6(1):6288, 2015. DOI: 10.1038/ncomms7288.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007.
DOI: 10.1103/PhysRevLett.98.010401.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, jul 2008.
DOI: 10.1088/1367-2630/10/7/073013.

[NW09] Miguel Navascués and Harald Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 466(2115):881–890, 2009.
DOI: 10.1098/rspa.2009.0453.

[Pai79] A. Pais. Einstein and the quantum theory. *Rev. Mod. Phys.*, 51:863–914, Oct 1979.
DOI: 10.1103/RevModPhys.51.863.

[Pit89] Itamar Pitowsky. *Quantum Probability — Quantum Logic*, volume 321 of *Lecture Notes in Physics*. Springer Berlin, Heidelberg, 1989.
DOI: 10.1007/BFb0021186.

[Pop14] Sandu Popescu. Nonlocality beyond quantum mechanics. *Nature Physics*, 10(4):264–270, 2014.
DOI: 10.1038/nphys2916.

[PPK+09] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. Information causality as a physical principle. *Nature*, 461(7267):1101–1104, 2009.
DOI: 10.1038/nature08400.

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.
DOI: 10.1007/BF02058098.

[Pro18] Marc-Olivier Proulx. A limit on quantum nonlocality from an information processing principle. Master's thesis, Department of Physics, University of Ottawa, Canada, 2018.
DOI: 10.20381/ruor-22258.

[RDBC19] Ashutosh Rai, Cristhiano Duarte, Samuraí Brito, and Rafael Chaves. Geometry of the quantum set on no-signaling faces. *Phys. Rev. A*, 99:032106, Mar 2019.
DOI: 10.1103/PhysRevA.99.032106.

[RKM+01] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409(6822):791–794, 2001.
DOI: 10.1038/35057215.

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications*. Cambridge University Press, 2020.
DOI: 10.1017/9781108671644.

[SBP09] Paul Skrzypczyk, Nicolas Brunner, and Sandu Popescu. Emergence of quantum correlations from nonlocality swapping. *Phys. Rev. Lett.*, 102:110402, Mar 2009.
DOI: 10.1103/PhysRevLett.102.110402.

[Sca19] Valerio Scarani. *Bell nonlocality*. Oxford Graduate Texts, 2019.
DOI: 10.1093/oso/9780198788416.001.0001.

[Sch35] Erwin Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23(48):807–812, 1935.
DOI: 10.1007/BF01491891.

[SGB+06] Valerio Scarani, Nicolas Gisin, Nicolas Brunner, Lluis Masanes, Sergi Pino, and Antonio Acín. Secrecy extraction from no-signaling correlations. *Phys. Rev. A*, 74:042339, Oct 2006.
DOI: 10.1103/PhysRevA.74.042339.

[Sha61] Claude Elwood Shannon. Two-way communication channels. *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability*, 1:611–644, 01 1961.
zbMATH: 0106.11509.

[Sho09] Anthony J. Short. No deterministic purification for two copies of a noisy entangled state. *Phys. Rev. Lett.*, 102:180502, May 2009.
DOI: 10.1103/PhysRevLett.102.180502.

[SLO19] WILLIAM SLOFSTRA. The set of quantum correlations is not closed. *Forum of Mathematics, Pi*, 7:e1, 01 2019.
DOI: 10.1017/fmp.2018.3.

[SMSC+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015.
DOI: 10.1103/PhysRevLett.115.250402.

[SWH20] Noah Shutty, Mary Wootters, and Patrick Hayden. Tight limits on nonlocality from nontrivial communication complexity; a.k.a. reliable computation with asymmetric gate noise. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 206–217, 2020.
DOI: 10.1109/FOCS46700.2020.00028.

[Tho79] C. D. Thompson. Area-time complexity for vlsi. In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 81–88, New York, NY, USA, 1979. Association for Computing Machinery.
DOI: 10.1145/800135.804401.

[Tsi87] B. S. Tsirel'son. Quantum analogues of the bell inequalities. the case of two spatially separated domains. *Journal of Soviet Mathematics*, 36(4):557–570, 1987.
DOI: 10.1007/BF01663472.

[Tsi93] B. S. Tsirelson. Some results and problems on quantum bell-type inequalities. *Hadronic Journal Supplement*, 8(4):329–345, 1993.
URL: https://cir.nii.ac.jp/crid/1570854176056088192.

[vD99] Wim van Dam. *Nonlocality & Communication Complexity*. Ph.d. thesis., University of Oxford, Departement of Physics, 1999.

[WC20a] Mirjam Weilenmann and Roger Colbeck. Self-testing of physical theories, or, is quantum theory optimal with respect to some information-processing task? *Phys. Rev. Lett.*, 125:060406, Aug 2020.
DOI: 10.1103/PhysRevLett.125.060406.

[WC20b] Mirjam Weilenmann and Roger Colbeck. Toward correlation self-testing of quantum theory in the adaptive clauser-horne-shimony-holt game. *Phys. Rev. A*, 102:022203, Aug 2020.
DOI: 10.1103/PhysRevA.102.022203.

[Weh06] Stephanie Wehner. Tsirelson bounds for generalized clauser-horne-shimony-holt inequalities. *Phys. Rev. A*, 73:022110, Feb 2006.
DOI: 10.1103/PhysRevA.73.022110.

[WW01] Reinhard F. Werner and Michael M. Wolf. Bell inequalities and entanglement, 2001.
DOI: 10.48550/arXiv.quant-ph/0107093.

[Yao79] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing(preliminary report). In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79, pages 209–213, New York, NY, USA, 1979. Association for Computing Machinery.
DOI: 10.1145/800135.804414.

[Yao93] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 352–361, 1993.
DOI: 10.1109/SFCS.1993.366852.

[ZCB+17] Yuqian Zhou, Yu Cai, Jean-Daniel Bancal, Fei Gao, and Valerio Scarani. Many-box locality. *Phys. Rev. A*, 96:052108, Nov 2017.
DOI: 10.1103/PhysRevA.96.052108.