A LIMIT ON QUANTUM NONLOCALITY FROM AN INFORMATION PROCESSING PRINCIPLE

Marc-Olivier Proulx

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements for the degree of
Master of Science in Physics

Department of Physics
Faculty of Science
University of Ottawa

Abstract

Quantum entanglement is known to give rise to *nonlocal* correlations that are not possible in a classical theory. Even though quantum correlations are stronger than classical correlations, they are still limited by the mathematical structure of quantum mechanics. Since physical limits usually emerge from physical principles, multiple principles were suggested in order to give a more physical explanation of the quantum limit on nonlocal correlations. None of these principles were able to completely rule out all super-quantum correlations. In this work, we study the principle of non-trivial communication complexity (NTCC), that sets a limit on what can be done in a particular information processing setting. Nonlocal correlations that violate this principle are believed to be impossible in nature. In this work, we expand the set of super-quantum correlations that are known to be ruled out by the NTCC principle, thus providing an explanation for their impossibility in quantum mechanics. We achieve this result by studying the consequences of more general super-quantum correlations in a protocol from Brassard, Buhrman, Linden, Méthot, Tapp and Unger. Additionally, we give a new proof of NTCC violation by a certain type of super-quantum correlations studied by Brunner and Skrzypczyk by describing and analyzing a simple and elegant protocol. Our work provides a framework for further studies of the consequences of super-quantum correlations on the NTCC principle.

Résumé

Il est connu que l'intrication quantique donne lieu à des corrélations *non-locales* qui sont impossibles dans la théorie classique. Bien qu'elles soient plus fortes que les corrélations classiques, les corrélations quantiques sont tout de même limitées par la structure mathématique de la mécanique quantique. Puisque les limites physiques émergent habituellement de principes physiques, plusieurs principes ont été suggérés afin de donner une explication à la limite quantique sur les corrélations non-locales. Aucun de ces principes n'est en mesure d'exclure complètement toutes les corrélations plus fortes que les corrélations quantiques. Dans ce document, nous étudions le principe de *complexité de la communication non-triviale* (CCNT), qui donne une limite sur ce qui peut être accompli dans un câdre informatique particulier. Il est généralement accepté que les corrélations non-locales qui violent ce principe sont fondamentalement impossibles à réaliser. Dans cette thèse, nous agrandissons l'ensemble des corrélations non-locales qui sont exclues par le principe CCNT, ce qui fournit une explication pour leur impossibilité dans la mécanique quantique. Nous obtenons ce résultat en étudiant les conséquences de corrélations plus générales dans un protocol proposé par Brassard, Buhrman, Linden, Méthot, Tapp et Unger. En outre, nous donnons une nouvelle preuve que le principe CCNT exclut un certain type de corrélations étudié par Brunner et Skrzypczyk en décrivant et en analysant un protocol simple et élégant. Notre travail fournit un cadre pour l'étude des conséquences de corrélations plus fortes que les corrélations quantiques sur le principe CCNT.

Summary of contributions

It is known that local measurements on shared quantum systems generate correlations that are not possible within a classical theory. Because these correlations violate Bell's inequalities, which restrict the correlations achievable by local theories, quantum correlations are said to be nonlocal. However, quantum mechanics does not allow for the maximal violation of Bell's inequalities and therefore quantum correlations are not maximally nonlocal. Such physical limitations usually emerge from physical principles. For instance, the *no signaling* principle limits the communication of information to the speed of light. Quantum mechanics, in its current formulation, does not provide a physical principle that limits nonlocal correlations. In the last decades, many candidate principles were suggested to explain what limits nonlocal correlations in nature, but none of them was able to completely single out the set of quantum correlations. Non-trivial communication complexity (NTCC) is one of the principles that were suggested in this search for a physical intuition on the limits on nonlocal correlations [vD13].

The NTCC principle states that nature does not allow correlations that make communication complexity trivial. Communication complexity is an information processing principle that quantifies the amount of communication needed for two distant parties to compute a function on a shared input. We say that a nonlocal correlation makes communication complexity trivial when this correlation can be harnessed to make such a computation possible with only one bit of communication, regardless of the function to be computed. In 1994, Popescu and Rohrlich introduced a theoretical tool called the *nonlocal box* to study super-quantum correlations [PR94]. The PR-box is a nonlocal box that produces the CHSH correlation [CHSH69], maximally violating the CHSH inequality, the most well-known Bell inequality. This tool is used to study the consequences of super-quantum correlations.

It is known that some super-quantum correlations violate the NTCC principle [BBL$^+$06, BS09, vD13]. Indeed, in a 2005 paper, van Dam showed that PR-boxes make communication complexity trivial [vD13]. In 2006, this result was extended

by Brassard, Buhrman, Linden, Méthot, Tapp and Unger in a paper where they prove that nonlocal boxes that produce the CHSH correlation with probability more than $\approx 91\%$ independently of the inputs (isotropic nonlocal boxes) violate NTCC [BBL+06]. Their proof is given in the form of the description and analysis of a protocol that we call the *BBLMTU protocol*. In 2009, Brunner and Skrzypczyk showed using nonlocal box distillation that all stronger-than-quantum nonlocal boxes of a certain type, which they term *correlated* nonlocal boxes (nonlocal boxes that produce either the CHSH correlation or identical bits), violate NTCC [BS09]. In their paper, they also join their result to the one from [BBL+06] by presenting a set of nonlocal boxes that are convex combinations of isotropic and correlated nonlocal boxes that violate NTCC.

In this work, we expand the set of nonlocal correlations that are known to violate NTCC in two subspaces of the non-signaling set of correlations. The first subspace is the subspace containing the PR-box, the PR$'$-box (nonlocal box that produces the CHSH correlation with flipped inputs) defined in [Bra11] and the fully random correlation. The second subspace in which we expand the known set of correlations that violate NTCC is the subspace from [BS09], containing isotropic and correlated nonlocal boxes. Finally, in this work, we give a new proof that stronger-than-quantum correlated nonlocal boxes violate NTCC. Contrarily to the existing proof of [BS09], ours does not rely on nonlocal box distillation. Our proof is based on the analysis of a simple and elegant protocol.

To expand the set of nonlocal correlations that are known to violate NTCC, we study different types of nonlocal boxes in the BBLMTU protocol [BBL+06]. In the BBLMTU protocol, nonlocal boxes are used to distributively compute multiplications. The factors in these multiplications, which become the inputs to the nonlocal boxes, are not independent from each other. Some combinations of nonlocal box inputs happen with higher probabilities. While isotropic nonlocal boxes compute multiplications with a success probability independent of their inputs, this is not the case for non-isotropic nonlocal boxes. Therefore, the success probability of the protocol using non-isotropic nonlocal boxes depends on the probability that the nonlocal boxes correctly compute multiplications for each input pair. To find what nonlocal boxes make communication complexity trivial with the BBLMTU protocol, we use tensors to obtain an expression for the success probability of the BBLMTU protocol with non-isotropic nonlocal boxes. This expression leads us to a new boundary for the set of nonlocal correlations that violate NTCC. Finally, to obtain our proof that all super-quantum correlated nonlocal boxes violate NTCC, we give and analyze a protocol that exploits the anisotropy of correlated nonlocal boxes, i.e. the fact

that such nonlocal boxes produce correlations that respect the CHSH condition with different probabilities depending on their inputs.

In addition to expanding the set of nonlocal correlations that are known to make communication complexity trivial, we provide a framework for the study of other protocols by using a method and notation that can be adapted to other protocols. For more complex protocols, our tensor notation can be harnessed by developing these tensors into tensor networks that could make it possible to find new boundaries for the set of nonlocal correlations that violate NTCC. Furthermore, by describing a new protocol that proves that all super-quantum correlated nonlocal boxes make communication complexity trivial, we offer additional tools for the study of the consequences of stronger-than-quantum correlations on the NTCC principle in the search for intuition on the limits on quantum nonlocality.

Acknowledgments

I would like to thank my supervisor, Prof. Anne Broadbent and co-supervisor Prof. David Poulin for their support throughout my work.

I would like to thank Anne for her precious help during the writing of this thesis, as well as during my research. I am thankful for the opportunities she gave me of attending international conferences and being immersed in the world of scientific research. I also want to thank her for the confidence she had in me and the freedom she gave me throughout my work.

I would like to thank David for the helpful discussions during my visits in Sherbrooke. You always had ideas and tips to give me inspiration for my work when I needed it.

I would like to thank all the passionate members of the Ottawa Quantum Information Group (OQIG) for making my journey more enjoyable with interesting discussions.

Finally, I would like to thank the University of Ottawa, the NSERC and the FRQNT for their financial support.

Contents

List of Figures x

Notations xi

1 Introduction 1

2 Basics and notation 4
- 2.1 Nonlocal correlations . . . 4
  - 2.1.1 The CHSH game . . . 5
  - 2.1.2 Tsirelson's bound . . . 7
  - 2.1.3 The nonlocal box . . . 8
  - 2.1.4 The set of quantum correlations . . . 10
- 2.2 Communication complexity . . . 15
  - 2.2.1 Communication complexity . . . 15
  - 2.2.2 Example: Communication complexity of the inner product . . . 16
  - 2.2.3 Non-trivial communication complexity . . . 17
- 2.3 Other tools and definitions . . . 17
  - 2.3.1 Distributed bit and distributed computation . . . 17
  - 2.3.2 The success bias . . . 18
  - 2.3.3 Tensors . . . 19

3 Prior results on non-trivial communication complexity 20
- 3.1 NTCC violation with PR-boxes . . . 20
  - 3.1.1 Prior concepts . . . 21
  - 3.1.2 PR-boxes in the VD protocol . . . 22
  - 3.1.3 Isotropic nonlocal boxes in the VD protocol . . . 22
- 3.2 Nonlocal box distillation . . . 23
- 3.3 NTCC violation with p-isoNLB if $p > \frac{3+\sqrt{6}}{6}$ . . . 24

3.3.1 The BBLMTU protocol . . . 24
3.3.2 Threshold on isotropic nonlocal boxes that make communication complexity trivial . . . 27
3.4 On the optimality of $\mathscr{P}_{\text{BBLMTU}}$ . . . 30
3.4.1 Distributed computation of the address function . . . 33
3.4.2 The PPKSWZ protocol . . . 34
3.4.3 Conditions on the decoding function . . . 35

4 Expanding the set of nonlocal correlations that are known to violate NTCC **37**
4.1 Success probability of the BBLMTU protocol with general nonlocal boxes . . . 38
4.2 Nonlocal boxes from the CHSH-CHSH′ subspace in the BBLMTU protocol . . . 42
4.2.1 Notable case . . . 47
4.3 Generalized correlated nonlocal boxes in the BBLMTU protocol . . . 47
4.3.1 Notable cases . . . 49
4.4 NTCC violation with p-corNLB if $p > 0$ . . . 51

5 Conclusion **54**
5.1 Summary of contributions . . . 54
5.2 Future work . . . 54

A The CHSH and CHSH′ probabilities for nonlocal boxes in the CHSH-CHSH′ subspace **56**

B Bias of the combination of processes when errors cancel in pairs **59**

List of Figures

2.1 The CHSH game 5
2.2 A nonlocal box 8
2.3 Slice from the set of non-signaling correlations 12
2.4 Upper half of the slice of the set of non-signaling correlations shown in figure 2.3 14

3.1 Usage of the nonlocal boxes in the BBLMTU protocol 27
3.2 Nonlocal boxes from the CHSH-CHSH′ slice for which communication complexity is known to be trivial and non-trivial 31
3.3 Set of nonlocal correlations that are known to violate NTCC 32
3.4 Decomposition of Addr_n function into multiple Addr_1 functions . . . 35

4.1 Nonlocal boxes that violate NTCC with the BBLMTU protocol . . . 46
4.2 Generalized correlated boxes that violate NTCC 50
4.3 The biased PPKSWZ protocol 53

Notations

Abbreviations

BBLMTU	Protocol from Brassard, Buhrman, Linden, Méthot, Tapp and Unger [BBL+06] (section 3.3)
CHSH	Game and inequality from Clauser, Horne, Shimony and Holt [CHSH69] that separates quantum from classical theories (section 2.1.1)
NTCC	Non-trivial communication complexity (section 2.2.3)
PPKSWZ	Protocol from Pawlowski, Paterek, Kaszlikowski, Scarani, Winter and Zukowski [PPK+09] (section 3.4.2)
VD	Protocol from van Dam [vD13] (section 3.1)

Symbols

$\oplus$	Addition modulo 2
$\{0,1\}^n$	The set of all n-bit strings
P_{PR}	Probability distribution of the PR-box (section 2.1.3)
$P_{\overline{\mathrm{PR}}}$	Probability distribution of the $\overline{\mathrm{PR}}$-box (section 2.1.3)
$P_{\mathrm{PR}'}$	Probability distribution of the PR′-box (section 2.1.3)
$P_{\overline{\mathrm{PR}'}}$	Probability distribution of the $\overline{\mathrm{PR}'}$-box (section 2.1.3)
P_{SR}	Probability distribution of the SR-box (section 2.1.3)
p-isoNLB	The isotropic nonlocal box described by $pP_{\mathrm{PR}} + (1-p)P_{\overline{\mathrm{PR}}}$ (section 2.1.3)
p-corNLB	The correlated nonlocal box described by $pP_{\mathrm{PR}} + (1-p)P_{\overline{\mathrm{SR}}}$ (section 2.1.3)
p_{CHSH}	The parameter p_{CHSH} of a nonlocal box is its winning probability at the CHSH game (section 2.1.4)
$p_{\mathrm{CHSH}'}$	The parameter $p_{\mathrm{CHSH}'}$ of a nonlocal box is its winning probability at the CHSH′ game (section 2.1.4)
$\mathscr{P}_C$	Maximal winning probability at the CHSH game for a classical strategy (section 2.1.1)
$\mathscr{P}_Q$	Maximal winning probability at the CHSH game for a quantum strategy (section 2.1.1)
$\mathscr{P}_{\mathrm{BBLMTU}}$	Winning probability at the CHSH game of the threshold nonlocal box for the BBLMTU protocol (section 3.3)
$\mathscr{P}_{\mathrm{PR}}$	Winning probability at the CHSH game of the PR-box (section 2.3.2)
δ_C	Success bias associated with the success probability $\mathscr{P}_C$ (section 2.3.2)
δ_Q	Success bias associated with the success probability $\mathscr{P}_Q$ (section 2.3.2)
δ_{BBLMTU}	Success bias associated with the success probability $\mathscr{P}_{\mathrm{BBLMTU}}$ (section 3.3.2)
δ_{PR}	Success bias associated with the success probability $\mathscr{P}_{\mathrm{PR}}$ (section 2.3.2)

Chapter 1

Introduction

Quantum mechanics is a very well tested physical theory that predicts and explains phenomena that transcend our every day experiences. However, in their most common formulations, the axioms of quantum mechanics refer to the way physical concepts (states, observables, measurement outcomes, time evolution) are described mathematically. These mathematical axioms are useful to make very precise predictions, but they make it difficult to have a good intuition about the phenomena we observe. For example, given the description of a quantum state and the description of a measurement, the axioms tell us how to calculate the probability distribution of the different possible measurement outcomes. However, they do not give us a good intuitive explanation of the measurement process. Indeed, there exist many interpretations of measurements in quantum mechanics and there even exist different interpretations of the whole quantum theory. The existence of these interpretations and the absence of consensus are symptoms of the lack of physical intuition in these mathematical axioms.

Nonlocality is another feature of quantum mechanics that arises from the mathematical axioms but that lacks an intuitive understanding. In this thesis, nonlocality refers to *Bell nonlocality*, which relates to the idea that actions on a given system can have an effect on a separate system without the use of any form of communication. Because no communication is required, this means that spacelike separated events in space-time can affect each other. Nonlocality reveals itself in the correlations that local measurements on entangled states can exhibit that cannot be achieved by variables that are completely described individually, locally. In 1980, Boris Tsirelson (also spelled Cirel'son) proved, using the mathematical axioms of quantum mechanics, that quantum nonlocality is limited by what is now known as Tsirelson's bound [Cir80], meaning that there exist nonlocal correlations

that are stronger than those produced by quantum mechanics. Although stronger-than-quantum (also called *super-quantum*) correlations have not been observed in nature, we only have a marginal understanding of the quantum limit on nonlocality beyond Tsirelson's mathematical proof. Physical limitations usually stem from physical principles. For instance, the *no signaling principle* limits the communication of information to the speed of light. The absence of a physical principle from which the quantum limit on nonlocality emerges triggered a lot of research on this subject in the past decades.

In an effort to gain a more physical understanding of quantum mechanics, Sandu Popescu and Daniel Rohrlich presented a theoretical tool, a hypothetical device now known as the Popescu-Rohrlich box (PR-box) (see section 2.1.3) to study quantum nonlocality. These PR-boxes can be generalized to *nonlocal boxes*, which are used to explore the consequences of stronger-than-quantum nonlocality by studying correlations that are not limited by Tsirelson's bound. Following the introduction of this tool, many physical principles have been suggested to explain the quantum limit on nonlocality. Even if they provide an explanation for the impossibility of producing some correlations with quantum mechanics, these principles only provide a partial explanation of the limits on quantum nonlocality since none of them was able to completely single out the set of quantum correlations. One of the suggested principles is based on the information processing concept of *communication complexity* (see section 2.2) and is called *non-trivial communication complexity* (NTCC). Even though it is known that all quantum correlations respect this principle, it is not yet known if all super-quantum correlations violate it. This work aims to gain information on this question.

Goal of this work. The goal of this work is to improve our understanding of quantum mechanics by studying consequences of stronger-than-quantum correlations on the principle of non-trivial communication complexity.

Overview of our results and technique. In this work, we give an intuitive explanation for the reason why some stronger-than-quantum correlations are impossible in nature by expanding the set of correlations that are known to violate the information processing principle of non-trivial communication complexity, presented in section 2.2.3. To achieve this, we use nonlocal boxes to study a protocol that was suggested in [BBL$^+$06], that we present in section 3.3, in order to find conditions on nonlocal boxes that violate NTCC. Additionally, we suggest and analyze a protocol that provides a new proof of NTCC violation by a certain type of nonlocal correla-

tions. Our work provides a framework for future work since our techniques can be adapted to other protocols and other types of super-quantum nonlocal correlations to further expand the set of correlations that are known to violate the NTCC principle.

Outline of this thesis. In the next chapter, we review some relevant concepts and establish some notation. The concepts are presented with a unified notation that is used throughout our work and that establishes a framework for future research. In chapter 3, we present prior results that are relevant to our research question. While some of these results provide a good starting point to work from, some of them are impossibility proofs that help us eliminate some possible avenues of solutions. The results presented in sections 3.2 and 3.3 are particularly relevant for our work since they provide a set of super-quantum correlations that violate the NTCC principle. Our contribution is presented in chapter 4, where we expand the set of correlations that are known to violate NTCC. Finally, chapter 5 puts our results in perspective and gives avenues for future work.

Chapter 2

Basics and notation

In this chapter, we present important concepts that are related to our work. In this thesis, it is assumed that the reader has some basic knowledge of quantum mechanics and is familiar with the concepts of measurements and entanglement. We first introduce the concept of *nonlocal correlations* in section 2.1 and then, we present the concept of *communication complexity* in section 2.2. Finally, we give additional definitions in section 2.3.

2.1 Nonlocal correlations

Quantum entanglement is a key feature in the quantum theory. It is one of the elements that separates quantum from classical theories. The strange statistics resulting from local measurements on entangled states raised questions on the completeness of quantum mechanics [EPR35], suggesting that there could be some unknown local variables responsible for the observed behaviour. However, in 1964, John S. Bell proved that local hidden variable theories[1] cannot produce the kind of correlations that can be observed by some measurements on entangled states [Bel64]. His proof implies inequalities, called *Bell's inequalities*, that bound some statistical quantities for local hidden variable theories. Bell's inequalities can be experimentally tested and an experimental violation of these inequalities is a proof that nature cannot be described by a local hidden variable theory. Such experiments have been conducted multiple times (see [FC72], [AGG82], [MMM+08] and [SUK+10] for example). Over the years, many possible loopholes were found [BCP+14], rendering the

[1]Here, a local hidden variable theory is simply one where all states are completely described by some local variable, which may be unknown to the observer.

previous experiments less convincing, which led to more experiments trying to close these loopholes. It is in 2015 that the first loophole-free Bell inequality violations were observed [HBD+15, SMSC+15].

The most well-known Bell inequality is called the CHSH inequality [CHSH69], named after Clauser, Horne, Shimony and Holt. This inequality is usually given as a bound on a sum of expectation values, but it can also be described in the form of the optimal success probability achievable by two parties in the CHSH game, described below.

2.1.1 The CHSH game

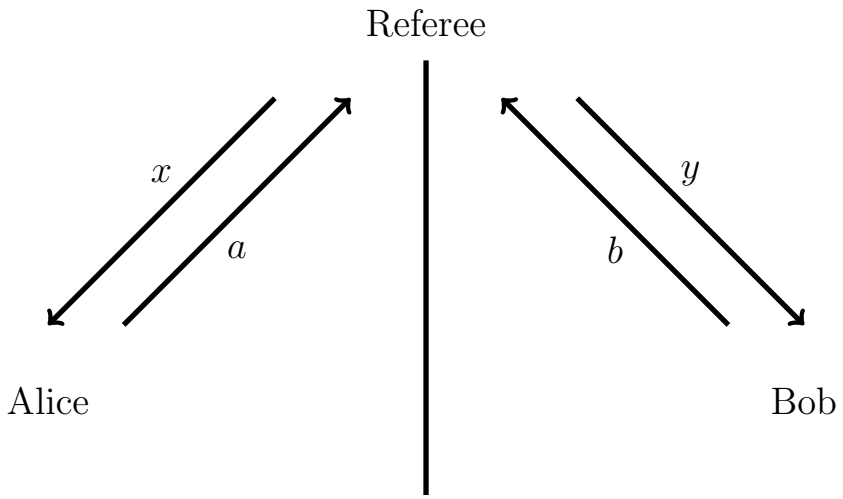


Figure 2.1: In the CHSH game, Alice and Bob each receive a random *question bit* (x and y) and have to output an *answer bit* (a and b). It is physically impossible for them to communicate once the game has started. They win if and only if $a \oplus b = xy$.

The CHSH game is a hypothetical scenario presented in the form of a game played by two parties and is used to show a separation between local and nonlocal theories. The scenario can be described as follows. Two parties, Alice and Bob, are respectively given by a referee a random bit x and y, that we call *question bits*. They each have to answer with a bit, respectively a and b, as shown in figure 2.1. The winning conditions are the following:

- If $x = y = 1$, they win if $a \neq b$

- Otherwise, they win if $a = b$.

These conditions can be written as the following equation where the symbol $\oplus$ represents addition modulo 2:

$$a \oplus b = xy\,. \tag{2.1}$$

To make the game more challenging, before they are given the question bits x and y, Alice and Bob are separated in such a way that it is physically impossible for them to communicate during the game. They can however agree on a strategy beforehand.

A classical strategy. An example of a strategy would be to flip a coin before the game starts to obtain a random bit r, known both by Alice and Bob. When they play the game, Alice answers with $a = xr$. If by chance their shared random bit r is equal to the bit Bob receives, $r = y$ (happens with probability 1/2), Bob answers $b = 0$. This way, $a \oplus b = xr \oplus 0 = xy$, condition 2.1 is fulfilled and they win. However, if $r \neq y$, Bob answers with a new random bit r'. With these answers, $a \oplus b = xr \oplus r'$. Since r' is a uniformly random bit, then $a \oplus b$ is also a uniformly random bit, which means they will win with probability 1/2. Therefore, this strategy has a winning probability of 3/4.

This turns out to be an optimal classical strategy. The CHSH inequality, in its formulation in terms of the winning probability at this game states that there is no better strategy if Alice and Bob are governed by a local hidden variable theory. Defining $\mathscr{P}_C := 3/4$, the success probability of any classical strategy at the CHSH game is at most $\mathscr{P}_C$.

A quantum strategy. By using entanglement, Alice and Bob can do better at the CHSH game. Instead of sharing a random bit r before the game starts, they prepare the entangled pair $\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$ and each take one particle from the pair[2]. Define the states

$$|\phi_0(\theta)\rangle = \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle \tag{2.2}$$

$$|\phi_1(\theta)\rangle = -\sin(\theta)\,|0\rangle + \cos(\theta)\,|1\rangle\,, \tag{2.3}$$

with $\theta \in [-2\pi, 2\pi]$. If she receives the question bit $x = 0$, Alice measures her share of the entangled pair in the $\{|\phi_0(0)\rangle, |\phi_1(0)\rangle\}$ basis. If she receives $x = 1$, she measures in the $\{|\phi_0(\pi/4)\rangle, |\phi_1(\pi/4)\rangle\}$ basis. If Bob receives the question bit $y = 0$,

[2]For example, this state could be made of spins: $\frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\uparrow\rangle + |\downarrow\rangle \otimes |\downarrow\rangle)$.

he measures his share of the entangled pair in the $\{|\phi_0(\pi/8)\rangle, |\phi_1(\pi/8)\rangle\}$ basis. If he receives $y = 1$, he measures in the $\{|\phi_0(-\pi/8)\rangle, |\phi_1(-\pi/8)\rangle\}$ basis. They answer with 0 when their measurement outcome is $|\phi_0(\theta)\rangle$ and 1 when it is $|\phi_1(\theta)\rangle$.

Because of how a measurement on a quantum state affects the state, the two measurement outcomes will be correlated in a way that will lead to a greater winning probability. Indeed, by using these rules to determine their answer bit, Alice and Bob can achieve the optimal success probability for a quantum strategy and satisfy the CHSH condition with probability $\mathscr{P}_Q$ [Cir80]:

$$\mathscr{P}_Q := cos^2\left(\frac{\pi}{8}\right) = \frac{2+\sqrt{2}}{4} \approx 0.85\,. \tag{2.4}$$

This difference between the classical and quantum optimal success probability is what makes it possible for the experiments mentioned in section 2.1 to show that nature is not classical by achieving a winning rate that is higher than the classical optimal. Note that, even though quantum entanglement provides an advantage over classical resources, it cannot be used for faster-than-light communication. In fact, no information can be transmitted using entanglement alone without other communication. We say that quantum correlations are *non-signaling*, meaning that they do not allow for faster-than-light communication.

2.1.2 Tsirelson's bound

As shown by the study of the CHSH game, the greatest probability with which quantum mechanics can produce bits that respect the CHSH condition (equation 2.1) given random question bits is approximately 85%. This well-known limit is called Tsirelson's bound (sometimes spelled Cirel'son) and it is derived from the mathematical structure of quantum mechanics [Cir80].

Even though it does not exist in quantum mechanics, it is possible to imagine a resource that would allow Alice and Bob to win the CHSH game with certainty, without allowing them to communicate faster than the speed of light. Because the correlation of the answer bits generated by such a resource would yield an even greater violation of the CHSH inequality than what is possible with quantum entanglement, we say that the correlation is more nonlocal than quantum correlations. These super-quantum correlations seem otherwise reasonable and therefore are a good starting point to seek physical intuition on the quantum theory. Finding unreasonable consequences for stronger-than-quantum correlations would provide a more intuitive explanation for the quantum limit on nonlocality. However, the set of all correlations permitted by quantum mechanics is complicated and Tsirelson's bound is only

one of the limits on this set (see section 2.1.4). The study of the limit on quantum correlations includes, but is not limited to, the study of Tsirelson's bound. Over the last fifteen years, many principles were suggested to give a physical intuition on the limits on quantum correlations. In all cases, the suggested principle is believed to be one that any reasonable physical theory (like quantum mechanics) should follow. The suggested principles include *information causality* [PPK+09], *macroscopic locality* [NW09], *no advantage for nonlocal computation* [LPSW07] and *non-trivial communication complexity* [vD13, BBL+06] (see [Pop14] for a review of some of these principles.). All these principles rule out some super-quantum correlations, but none of them is known to completely explain the quantum boundary. In particular, it is unknown if the non-trivial communication complexity principle is strong enough to explain Tsirelson's bound, even though it is known to explain another quantum limit on nonlocal correlations [BS09]. The principle of non-trivial communication complexity is described in details in section 2.2.3.

2.1.3 The nonlocal box

Every strategy for the CHSH game can be summarized by the probability distribution $\{P(a, b \mid x, y)\}$, describing the probability that Alice and Bob respectively output the answer bits a and b, given that they received the question bits x and y, for each a, b, x and y. In this work, we define a *correlation* to be such a set of joint probabilities. Even though multi-party nonlocal boxes were suggested and studied (see [BM06, GWAN11], for instance), we restrict ourselves to correlations between two parties, with $a, b, x, y \in \{0, 1\}$. We define a *quantum correlation* to be a correlation achievable by local measurements on quantum states (possibly entangled). To study non-signaling correlations without making assumptions on the underlying theory in which it is generated, we can make abstraction of the way they are obtained by studying them in a black box model. To explore how non-signaling correlations could be used in certain tasks, we study what Alice and Bob could do with a box that produces these correlations. Since these boxes have the possibility of producing correlations that violate Bell's inequalities, we call them *nonlocal boxes*.

Figure 2.2: A nonlocal box. Alice inputs x and Bob inputs y into the box. The box produces the bits a and b. For a PR-box, $a, b, x, y \in \{0, 1\}$, $a \oplus b = xy$ and a and b are locally uniformly random. The behaviour of a general bipartite nonlocal box can be described with a probability distribution $\{P(a, b \mid x, y)\}$.

A nonlocal box is a hypothetical device shared by two parties. The box takes an input from each party and returns an output with some probability distribution (figure 2.2). A *Popescu-Rohrlich box* (PR-box) [PR94] is a nonlocal box that takes one input bit from each party, respectively x and y and returns one output bit to each party a and b such that the CHSH relation 2.1 is respected. The probability distribution for the PR-box is

$$P_{\mathrm{PR}}(a, b \mid x, y) = \begin{cases} 1/2 & \text{if } a \oplus b = xy \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

Note that a and b are locally random. Individually, they are uncorrelated from x and y, meaning that regardless of the inputs x and y, a and b will each be 0 with probability 1/2 and 1 with probability 1/2. Only when considered together do they convey any information. For this reason, a PR-box cannot be used for instantaneous communication. We define three additional variations of the PR-box: The $\overline{\mathrm{PR}}$-box, the PR$'$-box and the $\overline{\mathrm{PR}'}$-box.

We call $\overline{\mathrm{PR}}$-box the nonlocal box that always returns the complement of the CHSH correlation:

$$P_{\overline{\mathrm{PR}}}(a, b \mid x, y) = \begin{cases} 1/2 & \text{if } a \oplus b = xy \oplus 1 \\ 0 & \text{otherwise.} \end{cases} \tag{2.6}$$

The PR$'$-box is the box returning the following correlation:

$$P_{\mathrm{PR}'}(a, b \mid x, y) = \begin{cases} 1/2 & \text{if } a \oplus b = (x \oplus 1)(y \oplus 1) \\ 0 & \text{otherwise.} \end{cases} \tag{2.7}$$

This corresponds to the CHSH correlation with flipped inputs. In this work, we call this the CHSH$'$ correlation. We also associate a game to the CHSH$'$ correlation, the CHSH$'$ game, similar to the CHSH game but where the winning condition is

$$a \oplus b = (x \oplus 1)(y \oplus 1)\,. \tag{2.8}$$

We also define the nonlocal box that returns the complement of the CHSH$'$ correlation, the $\overline{\mathrm{PR}'}$-box:

$$P_{\overline{\mathrm{PR}'}}(a, b \mid x, y) = \begin{cases} 1/2 & \text{if } a \oplus b = (x \oplus 1)(y \oplus 1) \oplus 1 \\ 0 & \text{otherwise.} \end{cases} \tag{2.9}$$

In the context of this work, nonlocal boxes are studied as a resource for computing functions (see sections 2.2 and 3.1 for related discussions). More specifically, we study protocols in which the nonlocal boxes are used to distributively compute multiplications (see section 2.3.1). The PR-box is perfectly suited for this task, since its outputs are bits whose sum is the multiplication of its inputs. Nonlocal boxes other than the PR-box can be seen as imperfect PR-boxes, that compute multiplications with some success probability.

Nonlocal boxes that are convex combinations of the PR-box and the $\overline{\text{PR}}$-box are called *isotropic* nonlocal boxes [BS09]. The isotropic nonlocal box defined as $pP_{PR} + (1-p)P_{\overline{PR}}$ outputs the CHSH correlation with probability p. In this thesis, we denote this box p-isoNLB.

We define the *shared randomness* SR-box, which outputs the same random bit for both parties, regardless of the input:

$$P_{\text{SR}}(a, b \mid x, y) = \begin{cases} 1/2 & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases} \tag{2.10}$$

Nonlocal boxes that are convex combinations of the PR-box and the SR-box are called *correlated* nonlocal boxes [BS09]. The correlated nonlocal box defined as $pP_{PR} + (1-p)P_{SR}$ is denoted p-corNLB and outputs the CHSH correlation with probability $3/4 + p/4$ provided each input pair (x, y) is equally likely.

2.1.4 The set of quantum correlations

Consider all possible bipartite correlations of the form $\{P(a, b \mid x, y)\}$, with $a, b, x, y \in \{0, 1\}$. The following restrictions naturally apply for probabilities:

$$\forall a, b, x, y \quad P(a, b \mid x, y) \geq 0 \tag{2.11}$$

$$\forall x, y \quad \sum_{a,b} P(a, b \mid x, y) = 1 \tag{2.12}$$

Each correlation in the resulting set can be described by 16 real numbers between 0 and 1, corresponding to the conditional probability for the 16 combinations of a, b, x and y. Therefore, each correlation can be represented as a vector in the 16-dimensional space $\mathbb{R}^{16}$. However, we only want to study non-signaling correlations, meaning that Alice cannot use a to learn information about y and Bob cannot use b to learn information about x. Thus, we impose that the a is independent of the value y

and that b is independent of x, the *no signaling* conditions [GKW+18, BLM+05]:

$$\forall b, x, x', y \quad \sum_a P(a, b \mid x, y) = \sum_a P(a, b \mid x', y) \tag{2.13}$$

$$\forall a, x, y, y' \quad \sum_b P(a, b \mid x, y) = \sum_b P(a, b \mid x, y') \,. \tag{2.14}$$

Because of these conditions, the dimension of the space of correlations that we study is effectively cut down to 8 [BCP+14, GKW+18]. Thus the set of non-signaling correlations $\mathcal{NS}$ corresponds to the subspace of dimension 8 of the space of all correlations described by equations 2.11, 2.12, 2.13 and 2.14. The most common representation of the non-signaling set of correlations is depicted in figure 2.3.

The subspace of the set of correlations represented in figure 2.3 is the 2-dimensional subspace that is the slice of the no signaling subspace containing the four variations of the PR-box described in section 2.1.3. In this work, we call this slice the CHSH-CHSH′ slice (or subspace) since it contains the PR-box that produces the CHSH correlation and the PR′-box that produces the CHSH′ correlation (respecting equation 2.8). All the correlations in the CHSH-CHSH′ slice are convex combinations of the four variations of PR-box. Therefore, they can be represented as

$$\begin{aligned} P(a, b \mid x, y) = &\alpha P_{\mathrm{PR}}(a, b \mid x, y) + \beta P_{\overline{\mathrm{PR}}}(a, b \mid x, y) \\ &+ \gamma P_{\mathrm{PR}'}(a, b \mid x, y) + \delta P_{\overline{\mathrm{PR}'}}(a, b \mid x, y) \end{aligned} \tag{2.15}$$

with $\alpha, \beta, \gamma, \delta \in [0, 1]$ and $\alpha + \beta + \gamma + \delta = 1$. Note that this is not a unique representation. Even though a quadruplet $(\alpha, \beta, \gamma, \delta)$ specifies a single nonlocal box, there could exist multiple quadruplets that specify the same nonlocal box. In fact, since this is a two-dimensional subspace, only two parameters are needed to uniquely specify each nonlocal box in the CHSH-CHSH′ slice. Figure 2.3 uses p_{CHSH} and $p_{\mathrm{CHSH}'}$, the winning probability at the CHSH and the CHSH′ games (see appendix A for the relationship between these winning probabilities and the representation of equation 2.15).

The set of local correlations $\mathcal{L}$ is specified by Bell's inequalities. In the CHSH-CHSH′ subspace, $\mathcal{L}$ is delimited by the CHSH inequality and by the CHSH′ inequality, as shown in figure 2.3.

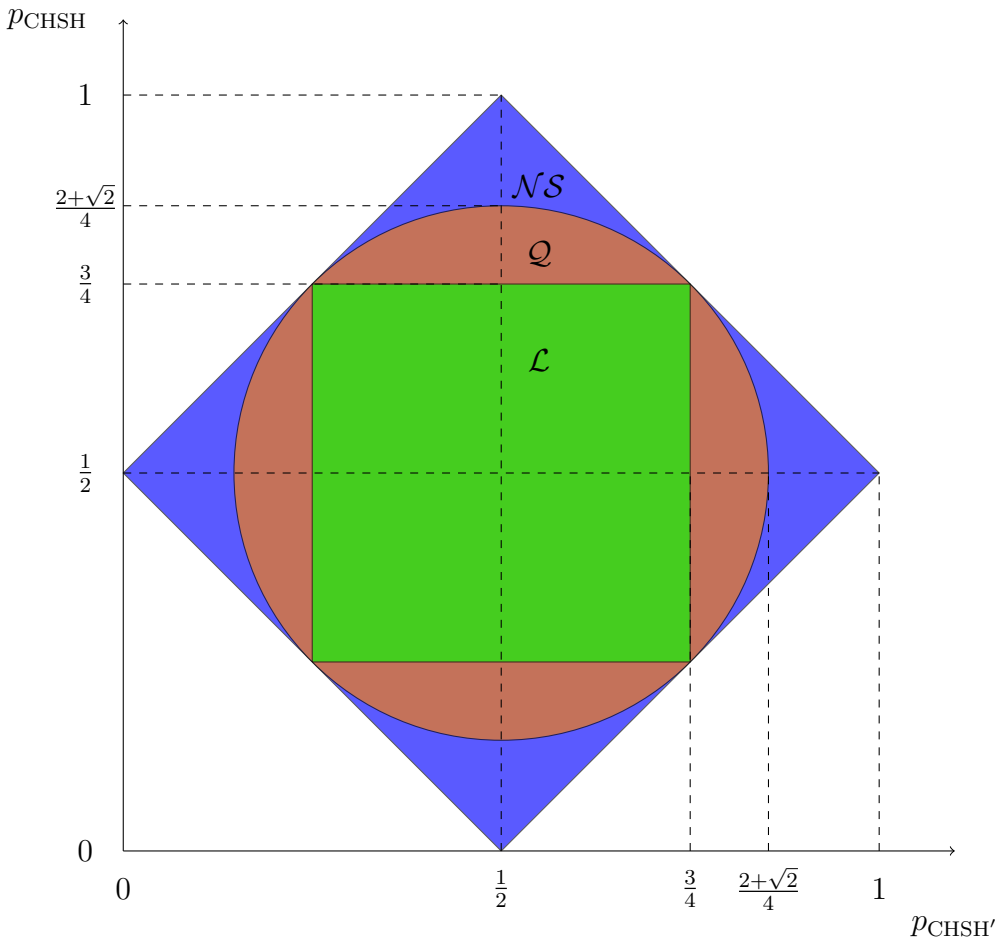


Figure 2.3: Slice from the set of non-signaling correlations (blue) in the plane containing the PR-box, $\overline{\text{PR}}$-box and the PR$'$-box. The winning probability at the CHSH game is represented on the vertical axis. The horizontal axis represents the winning probability at the CHSH$'$ game. The set of quantum correlations (orange) is contained in a circle inscribed in the square of non-signaling correlations. The set of local correlations (green) is contained in a square circumscribed in that circle. This figure is based on figure 2 of [GKW+18] and figure 1 of [Bra11].

Recall that the CHSH inequality implies that for classical correlations,

$$p_{\text{CHSH}} \leq \frac{3}{4}\,. \tag{2.16}$$

Because a box that produces a correlation with $p_{\text{CHSH}} = p$ can be converted into a

box with $p_{\text{CHSH}} = 1 - p$ by flipping one of the outputs, the CHSH inequality also implies

$$p_{\text{CHSH}} \geq \frac{1}{4}. \tag{2.17}$$

A similar reasoning leads to bounds on the parameter $p_{\text{CHSH}'}$ for classical correlations:

$$p_{\text{CHSH}'} \leq \frac{3}{4} \tag{2.18}$$

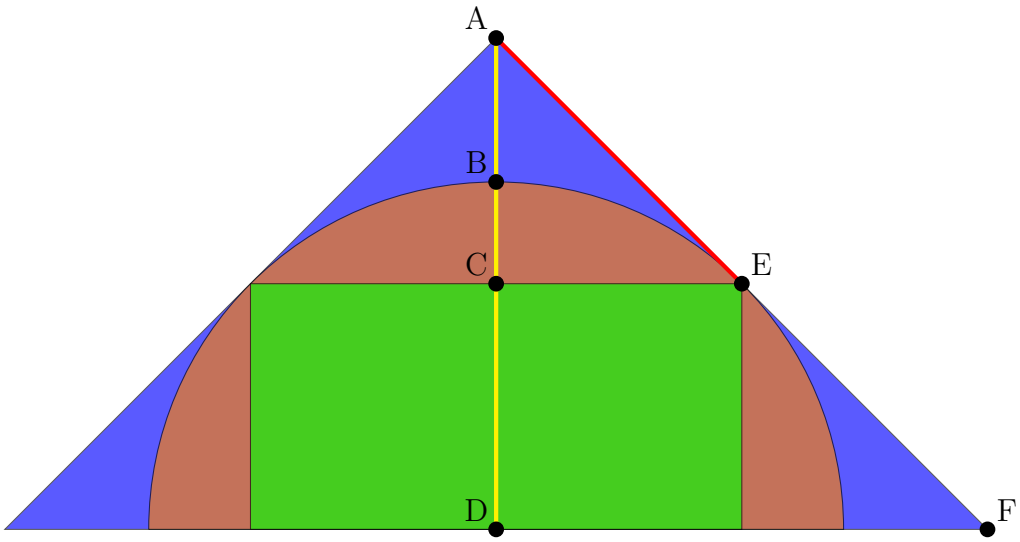
$$p_{\text{CHSH}'} \geq \frac{1}{4}. \tag{2.19}$$

On the other hand, little is known about the set of quantum correlations $\mathcal{Q}$. It is known that it is convex (convex combinations of correlations in $\mathcal{Q}$ are also in $\mathcal{Q}$) and its geometry is well understood in some regions [GKW+18]. The CHSH-CHSH′ subspace is one of these well-understood regions. In the representation of figure 2.3 of the CHSH-CHSH′ slice, the set of quantum correlations is a circle inscribed in the set of non-signaling correlations.

The SR-box presented earlier is not a convex combination of the four variations of the PR-box (see section 2.1.3) and cannot be written in the form of equation 2.15. Therefore, correlated nonlocal boxes (convex combinations of the PR-box and the SR-box) are not in the CHSH-CHSH′ slice of figure 2.3, with the obvious exception of the 1-corNLB, which is the PR-box. Figure 2.4 shows the upper portion of the CHSH-CHSH′ slice on which is projected the correlated nonlocal box subset to show where this type of nonlocal box stands with regards to p_{CHSH} and $p_{\text{CHSH}'}$. The 0-corNLB respects the CHSH and the CHSH′ inequalities as well as all other Bell inequalities, meaning that 0-corNLB$\in \mathcal{L}$ [BS09].

The parameter p_{CHSH} is often used to quantify nonlocality of correlations. It may be a good measure of nonlocality for isotropic nonlocal boxes, but for all other nonlocal boxes, p_{CHSH} does not tell the whole story. A nonlocal box that violates one of the four inequalities 2.16, 2.17, 2.18 and 2.19 can be made into one that violates any other of the four inequalities by local operations [GKW+18] (note that no correlation in $\mathcal{NS}$ violates more than one of the inequalities [LHBR10]). This means that a nonlocal box with $1/4 \leq p_{\text{CHSH}} \leq 3/4$ can still produce a correlation that is nonlocal if it violates another Bell inequality. For correlations in the CHSH-CHSH′ slice, p_{CHSH} and $p_{\text{CHSH}'}$ have to be considered together to determine if a correlation is local, quantum or stronger than quantum.

Since our goal is to find intuition on the quantum bounds on nonlocal correlations, we study well-known regions of the set of non-signaling correlations. In particular,



(a) Isotropic nonlocal boxes lie on the yellow line $\overline{AD}$. The red line $\overline{AE}$ is the projection of correlated nonlocal boxes onto the CHSH-CHSH′ slice.

Point	Description
A	PR-box
B	$\mathscr{P}_Q$-isoNLB
C	$\mathscr{P}_C$-isoNLB
D	1/2-isoNLB (Uncorrelated bits)
E	Projection of 0-corNLB
F	PR′-box

(b) Description of some points in the set of non-signaling correlations.

Figure 2.4: Upper half of the slice of the set of non-signaling correlations shown in figure 2.3 with some notable points. Isotropic and correlated nonlocal boxes are emphasized.

we study correlations in the CHSH-CHSH′ slice and correlations that are convex combinations of the PR-box, the $\overline{\text{PR}}$-box and the SR-box.

2.2 Communication complexity

Nonlocal correlations can be used as a resource in multiple information processing settings (see [BCP+14, BM06, Bro16]). In this work, we study the consequences of stronger-than-quantum nonlocality on an information processing task, described in section 2.2.1, to find an intuitive argument for the quantum limit on nonlocality. We start by defining the theoretical computer science concept of *communication complexity*. Then, we present an example of a case that saturates the upper bound on communication complexity and for which quantum correlations provide no advantage over classical resources. Finally, we define the information processing principle that we use to rule out some stronger-than-quantum correlations from any reasonable physical theory, like quantum mechanics, namely *non-trivial communication complexity*.

2.2.1 Communication complexity

Consider two parties, Alice and Bob. Each are given an n-bit string: x for Alice, y for Bob. They cannot see the string of the other party. Together, they want to compute a Boolean function, $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ on x and y. However, communication is expensive and they get charged for every bit they send, so they want to use as few as they can. The minimum number of bits they need to exchange for Alice to learn $f(x,y)$ is called the *communication complexity* of f, denoted $\mathrm{CC}(f)$, and is a function of the input size n.

Alternatively, communication complexity could be defined as the minimum number of bits of communication needed for Bob, or even both Alice and Bob to learn $f(x,y)$. In all cases, communication complexity differs by at most one bit. Indeed, if Alice can learn $f(x,y)$ after exchanging m bits with Bob, then she can send $f(x,y)$ to Bob, who learns it after exchanging $m+1$ bits with Alice. Since we are generally interested in how $\mathrm{CC}(f)$ varies with the input size n this is not a significant difference and all these definitions will lead to the same conclusions. For simplicity, in this work, we adhere to the definition where Alice needs to learn $f(x,y)$.

We can also give Alice and Bob shared entanglement and see how it affects communication complexity. In this thesis, we denote $\mathrm{CC}^Q(f)$ the smallest number of bits Alice and Bob need to communicate to compute $f(x,y)$ using quantum entanglement as a resource. More generally, we denote $\mathrm{CC}^R(f)$ the communication complexity of f given some resource R. We also consider probabilistic communication complexity, where Alice is only required to learn $f(x,y)$ with probability equal or greater than

a constant ϵ, with $1/2 < \epsilon \leq 1$, denoted $\mathrm{CC}_\epsilon(f)$ and $\mathrm{CC}_\epsilon^{\mathcal{Q}}(f)$ for the entanglement-assisted case.

Note that since the entanglement-assisted case only adds resources to the classical case and the probabilistic one only differs from the others by allowing some constant error, we have $\forall f, \mathrm{CC}(f) \geq \mathrm{CC}^{\mathcal{Q}}(f) \geq \mathrm{CC}_\epsilon^{\mathcal{Q}}(f)$. Also, in all cases, the communication complexity is upper-bounded by the input size n, since it is always possible for Bob to send his whole input to Alice, who can then compute the function locally with certainty. For some functions, there are protocols that can do better, but there are some functions for which this strategy is optimal. The *inner product* function is one such example as described in the following section.

2.2.2 Example: Communication complexity of the inner product

Consider the following Boolean function $\mathrm{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ defined in modulo 2 arithmetic by

$$\mathrm{IP}_n(x, y) = \bigoplus_{i=1}^{n} x_i y_i \,, \tag{2.20}$$

where x_i is the ith bit of the n-bit string x and y_i is the ith bit of the n-bit string y. The communication complexity of this function is n [CvDNT13]. Allowing for entanglement does not help and allowing for error reduces the amount of communication needed by a factor [CvDNT13]:

$$\begin{aligned} \mathrm{CC}(\mathrm{IP}_n) &= n \\ \mathrm{CC}^{\mathcal{Q}}(\mathrm{IP}_n) &= n \\ \mathrm{CC}_\epsilon^{\mathcal{Q}}(\mathrm{IP}_n) &\geq \max\left(\frac{1}{2}\left(2\epsilon - 1\right)^2, \left(2\epsilon - 1\right)^4\right) n - \frac{1}{2} \,. \end{aligned} \tag{2.21}$$

Note that in all cases, the two parties need to exchange a number of bits that grows linearly with n. In the communication complexity setup, the multiplications involving both parties' input are the difficult part of the computation (see section 3.1.3). The inner product function contains many such multiplications, which explains why it saturates the upper bound on communication complexity.

2.2.3 Non-trivial communication complexity

Even with quantum resources, some functions require an amount of communication linear in the size of the inputs to be computed in the communication complexity setting. In a world in which there would exist resources that make it possible to compute every function with a constant amount of communication (independent of the size of inputs), we say that communication complexity *collapses*, as the concept of communication complexity becomes *trivial*.

Definition 1 (Trivial communication complexity)**.** *If there exists a resource R within a physical theory such that there exist constants $\epsilon > 1/2$ and $c \in \mathbb{N}$ such that $\forall f, \forall n, \mathrm{CC}_\epsilon^R(f) \leq c$, then we say communication complexity is trivial within that theory.*

It is strongly believed that in nature, communication complexity is not trivial, that there should be some notion of complexity related to this computing task. This is the *Non-trivial communication complexity* principle:

Definition 2 (Non-trivial communication complexity (NTCC))**.** *Physical principle according to which communication complexity should not be trivial in nature. We say a physical theory respects the NTCC principle when resources (like nonlocal correlations) allowed within that theory do not make communication complexity trivial.*

2.3 Other tools and definitions

In addition to the nonlocal box and the concept of communication complexity, we use a few other tools in this work. In this section, we define these tools and provide a brief explanation of their relevance for our work.

2.3.1 Distributed bit and distributed computation

In this work, the considered computing tasks happen between two parties, Alice and Bob. In the course of a computation, bits are often *distributed* between Alice and Bob.

Definition 3 (Distributed bit)**.** *We say that a bit z is* distributed *when Alice knows a bit $z^{(A)}$ and Bob a bit $z^{(B)}$ such that $z = z^{(A)} \oplus z^{(B)}$.*

In this work, we consider protocols that enable Alice and Bob to *compute* functions *distributively*.

Definition 4 (Distributed computation)**.** *We say that a computation is* distributed *when the outcome of the computation is a distributed bit.*

Note that, in these terms, a PR-box allows Alice and Bob to distributively compute the product of the inputs since it returns bits whose sum is the product of its inputs. It is easy to see that a function f that can be distributively computed with m bits of communication has $CC(f) \leq m + 1$. Therefore, protocols for distributed computations provide upper bounds on communication complexity. Because using nonlocal boxes to compute multiplications introduces distributed bits in a computation, it is natural to focus our attention on protocols for distributed computation when studying communication complexity with nonlocal boxes.

2.3.2 The success bias

In this work, we study the probability that protocols succeed at certain tasks. Often, these protocols compute bits (possibly distributed), which means that they either succeed completely or fail completely. It also means that if the outcome of a protocol was to be replaced with a random bit, the success probability would be $1/2$. Therefore, when studying the success probability of a protocol, its deviation from $1/2$ is a relevant quantity. This is why we define the *success bias* of a protocol.

Definition 5 (Success bias)**.** *If a process has a success probability $P > 1/2$, then it has* success bias $\beta = 2P - 1$ *such that* $P = \frac{1+\beta}{2}$.

A success bias can also be associated to a nonlocal box when it is used to distributively compute a product. In this case, the success bias is related to the CHSH probability of the nonlocal box. The optimal CHSH success probabilities $\mathscr{P}$ presented in section 2.1.1 can be translated to a CHSH success bias δ in the following way:

$$\mathscr{P}_C = 3/4 \longrightarrow \delta_C = \frac{1}{2} \tag{2.22}$$

$$\mathscr{P}_Q = \frac{2+\sqrt{2}}{4} \longrightarrow \delta_Q = \sqrt{\frac{1}{2}} \tag{2.23}$$

$$\mathscr{P}_{\mathrm{PR}} = 1 \longrightarrow \delta_{\mathrm{PR}} = 1\,. \tag{2.24}$$

Note that if a process has success probability $\frac{1+\beta}{2}$ then it has error probability $1 - \frac{1+\beta}{2} = \frac{1-\beta}{2}$.

The main advantage of using success bias over success probability is the way it behaves in processes where errors cancel in pairs. Consider a protocol that produces a bit by summing N bits modulo 2. If these N bits were imperfectly produced, say, each independently with success bias β, then the bit obtained by summing the N imperfect bits will yield the correct result with success bias β^N. Indeed, the success probability P of such a combination is given by

$$P = \sum_{i=0}^{\left\lfloor \frac{N}{2} \right\rfloor} \binom{N}{2i} \left(\frac{1+\beta}{2}\right)^{N-2i} \left(\frac{1-\beta}{2}\right)^{2i} \tag{2.25}$$

which takes into account the probability of all the possible ways to have an even number of errors in the N imperfect bits. Conveniently, it can be shown that this expression can be simplified to (see proof in appendix B)

$$P = \frac{1+\beta^N}{2}\,. \tag{2.26}$$

2.3.3 Tensors

In this work, a rank-m tensor is merely an m-dimensional array of real numbers, where each element of the array is referred to by m indices. For instance, a rank-0 tensor is a scalar, a rank-1 tensor is a vector and a rank-2 tensor is a matrix. In chapter 4, we use rank-5 tensors to represent the probability of occurrence of certain events. In this work, the rank-5 tensors could be replaced by functions like $h : \{0,1\}^5 \to [0,1]$ whose inputs correspond to the 5 indices of the tensor and that return the corresponding tensor element.

The use of tensors is justified by the fact that it provides a framework to study different protocols. Indeed, the tensors we define in chapter 4 can be adapted to other protocols. The reader who is familiar with tensor networks will see that for more complex protocols, the required tensors can be found by decomposing them in tensor networks (see [Orú14] for an introduction to tensor networks).

Chapter 3

Prior results on non-trivial communication complexity

In this chapter, we present prior results on which this work builds. First, in section 3.1, we present a result that shows that PR-boxes make communication complexity trivial. Then, we see in section 3.2 what can and cannot be done with nonlocality distillation, the idea of using multiple nonlocal boxes to simulate one that is closer to a PR-box. Also, we see in section 3.3 that by using error correction methods, it can be shown that p-isoNLBs with $p > \frac{3+\sqrt{6}}{6}$ make communication complexity trivial, thus providing an explanation for why they are not permitted by the quantum theory. Finally, an impossibility result is presented in section 3.4. It shows that the result presented in section 3.3 cannot be improved by simply changing the decoding function in the error correction process.

3.1 NTCC violation with PR-boxes

In this section, we present results from [vD13]. We first present some concepts that help us introduce the protocol described in [vD13], which then leads to the result presented in section 3.1.2.

3.1.1 Prior concepts

It is known that every Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ can be written in its *algebraic normal form*, which in modulo 2 arithmetic can be expressed as

$$f(x,y) = \bigoplus_{i=1}^{2^n} x'_i(x) y'_i(y)\,, \tag{3.1}$$

where the x'_i are functions of x and the y'_i are functions of y. In other words, new 2^n-bit inputs x' and y' can be computed locally as functions of respectively x and y such that $f(x,y)$ can be written as the sum of products of the new inputs. At most 2^n of these new inputs are needed and they can be expressed as polynomials in respectively the x_i's and y_i's [vD13]. Note that the inner product function introduced in section 2.2.2 has an algebraic normal form that has only n terms, since equation 2.20 is already of the correct form. The algebraic normal form essentially expresses functions in the form of an inner product $f(x,y) = \mathrm{IP}_{2^n}(x',y')$.

Consider the computation of a function f by Alice and Bob in the communication complexity setting. We see from equation 3.1 that all functions can be written with only additions and multiplications. If f can be written with only additions (equation 3.2), then $\mathrm{CC}(f) = 1$. Indeed, since the addition is commutative, Bob can perform all the additions that use his inputs (equation 3.3) and send the result to Alice, who can then perform the remaining additions:

$$f(x,y) = \left(\bigoplus_{i=1}^{n} c_i x_i\right) \oplus \left(\bigoplus_{j=1}^{n} d_j y_j\right) \tag{3.2}$$

$$= \bigoplus_{i=1}^{n} c_i x_i \oplus B \tag{3.3}$$

with $c_i, d_j \in \{0,1\}$ coefficients indicating if the inputs x_j and y_j are present in the sum and where B is the bit that Bob needs to send to Alice.

In the protocol described here, the function f can be distributively computed without any communication since Alice and Bob can compute a distributed bit equal to $f(x,y)$ for any x and y: Alice computes a bit $A = \bigoplus_{i=1}^{n} c_i x_i$ and Bob a bit $B = \bigoplus_{j=1}^{n} d_j y_j$ such that $f(x,y) = A \oplus B$.

A similar protocol can be used if the function can be written with additions and local multiplications, i.e. multiplications involving only one party's input at a time since it is still possible for them to locally compute A and B such that $f(x,y) = A \oplus B$. Recall that in this case, we say that $A \oplus B$ is a distributed bit (see section 2.3.1).

Things get more complicated when the function can only be written with multiplications involving both parties' input. Indeed, in this case we cannot re-arrange the terms to get to a form like equation 3.3. In summary, when looking at a function in modulo 2 arithmetic, multiplications between variables involving both parties' inputs are what require the extra communication. This is where nonlocal boxes come into play.

3.1.2 PR-boxes in the VD protocol

Distributively computing a multiplication between a variable known by Alice and one known by Bob is similar to playing the CHSH game. A protocol that wins the CHSH game with probability p can distributively compute such a multiplication without communication with success probability p. The protocol described in [vD13] uses these ideas. We call this the *VD* protocol, after its author, van Dam.

VD protocol Consider a function f written as an inner product in the form of equation 3.1. Alice knows x, Bob knows y and they share an unlimited number of PR-boxes. They can use 2^n PR-boxes to distributively compute the 2^n multiplications $x'_i y'_i$. By doing this, they transform the function into one that contains only additions, that they can easily compute distributively. Bob can send his share of the final distributed bit to Alice, who learns $f(x, y)$ with only one bit of communication.

Since every f can be written in the algebraic normal form, this protocol works for all functions. We conclude that if nature allowed PR-boxes, communication complexity would be trivial. This is not reasonable and therefore it gives an explanation for the impossibility of PR-boxes in nature and gives an intuition for why quantum resources cannot win the CHSH game perfectly ($\mathscr{P}_Q < 1$).

3.1.3 Isotropic nonlocal boxes in the VD protocol

One may ask if by replacing the PR-boxes by p-isoNLBs the VD protocol could still be used to achieve trivial communication complexity. Using this protocol with such nonlocal boxes would mean that each of the 2^n multiplications would be successfully computed with probability p. Since the additions are taken modulo 2, errors in the computation of multiplications cancel in pairs when they are added together. The final success probability is the probability that an even number of errors occur. To calculate this probability, we use the success bias of the protocol, as defined in section 2.3.2.

We see, from equation 2.26 that using the protocol from [vD13] with p-isoNLBs with corresponding success bias δ will result in a success probability of $\frac{1+\delta^{2^n}}{2}$. For $\delta < 1$, this success probability approaches $1/2$ as n increases. There is no constant $\epsilon > 1/2$ such that $\frac{1+\delta^{2^n}}{2} > \epsilon$ for all n. Therefore, the VD protocol does not allow computation of all f with a probabilistic communication complexity of 1 except if $p = 1$ and therefore cannot be used to extend the trivial communication complexity result to nonlocal boxes other than PR-boxes.

3.2 Nonlocal box distillation

In the VD protocol, the source of errors is the computation of multiplications by nonlocal boxes. It is natural to try to find a way to improve these multiplications so that the same protocol also leads to a constant success probability even with nonlocal boxes that are not PR-boxes. That could mean using multiple nonlocal boxes to simulate one with a greater CHSH probability. This idea is called *nonlocal box distillation* and has been the subject of extensive research. We know it is not possible to simulate a p-isoNLB for $p > \mathscr{P}_Q$ from $\mathscr{P}_Q$-isoNLBs since that would imply that quantum resources could violate Tsirelson's bound. However, one could ask if some super-quantum nonlocal boxes could be distilled to obtain a better CHSH probability.

In [BG15], it is shown that distillation of isotropic nonlocal boxes is not possible. However, in [BS09] and [FWW09] it is shown that correlated nonlocal boxes can be distilled.

Note that the p-corNLB defined in section 2.1.3 is a box with the following behaviour on inputs x and y:

- With probability p, output a and b such that $a \oplus b = xy$
- With probability $1 - p$, output a and b such that $a = b$ (regardless of x and y).

Correlated and isotropic nonlocal boxes can be seen as imperfect PR-boxes with different noise models. While a p-isoNLB gives the complement of the CHSH condition with probability $1 - p$, a p-corNLB gives identical bits with probability $1 - p$. This means that a p-corNLB always respects the CHSH condition on all inputs except $x = y = 1$, where the CHSH condition is only respected with probability p.

With quantum resources, correlated nonlocal boxes p-corNLBs cannot be simulated except for $p = 0$ [BS09]. This turns out to also be the classical limit, meaning that quantum resources provide no advantage over classical resources for simulating

correlated nonlocal boxes. All p-corNLBs with $p > 0$ can be distilled to become arbitrarily close to PR-boxes [BS09]. This implies that all super-quantum (and super-classical) correlated nonlocal boxes make communication complexity trivial, which provides an intuitive explanation for this limit.

As shown in [MAG06], a p-corNLB ($p_{\text{CHSH}} = 3/4 + p/4$) can be transformed, by local operations, into an isotropic nonlocal box with the same CHSH probability, $(3/4 + p/4)$-isoNLB ($p_{\text{CHSH}} = 3/4 + p/4$). This process is called depolarization. The possibility to make isotropic nonlocal boxes from correlated nonlocal boxes means that any limit on p_{CHSH} of isotropic boxes also implies a limit on correlated boxes.

The fact that isotropic nonlocal boxes cannot be distilled means that proofs of trivial communication complexity that use distillation cannot be generalized to isotropic nonlocal boxes. A condition on isotropic nonlocal boxes that violate NTCC was found in [BBL+06] (presented in the next section) by considering a protocol that uses error correction to improve the final success probability of the computation without improving the success probability of the individual nonlocal boxes.

3.3 NTCC violation with p-isoNLB if $p > \frac{3+\sqrt{6}}{6}$

As mentioned in the previous section, a constant success probability cannot be achieved with one bit of communication by trying to improve the multiplications individually in the VD protocol. In [BBL+06], the authors make use of basic error correction adapted to the communication complexity setting to reduce the probability of error on an imperfect computation. Doing this, they show that p-isoNLBs make communication complexity trivial when

$$p > \mathscr{P}_{\text{BBLMTU}} = \frac{3+\sqrt{6}}{6} \approx 91\% \,. \tag{3.4}$$

3.3.1 The BBLMTU protocol

To achieve this result, consider the following protocol, that we call the *BBLMTU* protocol after the authors of [BBL+06] (Brassard, Buhrman, Linden, Méthot, Tapp and Unger). In this protocol, Alice and Bob respectively know $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and want Alice to learn $f(x,y)$, where $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, like in the communication complexity setting described earlier. We suppose they have access to an unlimited number of PR-boxes. In section 3.3.2, we show what happens when we replace the PR-boxes by p-isoNLBs and derive a threshold on p

for trivial communication complexity. The BBLMTU protocol can be split into two parts: the initial distributed computation and the error correction phase. The error correction phase uses one of the simplest error correction methods: the *repetition code* and *majority decoding*. The idea of an m-bit repetition code, as its name implies, is to encode one bit into m copies of itself before it undergoes a noisy process. The idea of the majority decoding is to choose the value that is the most likely to be correct among the m copies by selecting the one that is repeated the most often. The m-input majority function returns 1 if more than $m/2$ input bits have value 1 and 0 otherwise[1]. The BBLMTU protocol makes use of the 3-input majority function.

The initial distributed computation Let $z \in \{0,1\}^n$ be a random string known both by Alice and Bob and r be a random bit known by Bob. They perform an initial distributed computation, where Alice computes A and Bob computes B such that:

$$A = f(x, z) \tag{3.5}$$

$$B = \begin{cases} 0 & \text{if } z = y \\ r & \text{otherwise.} \end{cases} \tag{3.6}$$

This can be interpreted like Alice making a guess z for Bob's input y and computing $A = f(x, z)$ with her guess. If the guess is correct, Bob sets his output $B = 0$ such that $A \oplus B = f(x, y)$. If the guess is incorrect, he sets his output to be a random bit r such that $A \oplus B$ is a random bit, which will then be equal to $f(x, y)$ with probability $1/2$. The success probability P_0 of this initial distributed computation is given by

$$\begin{aligned} P_0 &= P\left[z = y\right] + P\left[z \neq y\right] P\left[f(x, z) \oplus r = f(x, y)\right] \\ &= \frac{1}{2^n} + \left(1 - \frac{1}{2^n}\right) \frac{1}{2} \\ &= \frac{1}{2} + \frac{1}{2^{n+1}} \,. \end{aligned} \tag{3.7}$$

The error correction phase The probability P_0 depends on n. Alice and Bob use error correction to make it independent of n in the following way. They repeat the initial distributed computation step three times, with fresh random strings z and

[1]Sometimes the m-input majority function is defined to return 1 if *at least* $m/2$ inputs have value 1 and 0 otherwise. These two definitions only differ for the tie case when m is even.

fresh random bits r each time. They now have three distributed bits $A_i \oplus B_i$, each with independent success probability $1/2+1/2^{n+1}$. They can distributively compute the majority function on these three distributed bits by using two PR-boxes since the 3-input majority function can be written as

$$\mathrm{Maj}_3(\alpha, \beta, \gamma) = \alpha\beta \oplus \alpha\gamma \oplus \beta\gamma \tag{3.8}$$

which, in our case, with three distributed bits $A_i \oplus B_i$ becomes

$$\begin{aligned}
&\mathrm{Maj}_3(A_1 \oplus B_1, A_2 \oplus B_2, A_3 \oplus B_3) \\
&\qquad = (A_1 \oplus B_1)(A_2 \oplus B_2) \oplus (A_1 \oplus B_1)(A_3 \oplus B_3) \oplus (A_2 \oplus B_2)(A_3 \oplus B_3) \\
&\qquad = (A_1 \oplus A_2)(B_2 \oplus B_3) \oplus (A_2 \oplus A_3)(B_1 \oplus B_2) \\
&\qquad \oplus A_1A_2 \oplus A_1A_3 \oplus A_2A_3 \oplus B_1B_2 \oplus B_1B_3 \oplus B_2B_3 \\
&\qquad = (A_1 \oplus A_2)(B_2 \oplus B_3) \oplus (A_2 \oplus A_3)(B_1 \oplus B_2) \\
&\qquad \oplus \mathrm{Maj}_3(A_1, A_2, A_3) \oplus \mathrm{Maj}_3(B_1, B_2, B_3)\,.
\end{aligned} \tag{3.9}$$

Using two PR-boxes with the inputs shown in figure 3.1 to get the outputs a_1, b_1, a_2 and b_2, Alice and Bob hold the distributed bit

$$(a_1 \oplus a_2 \oplus \mathrm{Maj}_3(A_1, A_2, A_3)) \oplus (b_1 \oplus b_2 \oplus \mathrm{Maj}_3(B_1, B_2, B_3))\,, \tag{3.10}$$

which is equal to $\mathrm{Maj}_3(A_1 \oplus B_1, A_2 \oplus B_2, A_3 \oplus B_3)$. In general, the 3-input majority function on three variables that have success probability η leads to a success probability $\eta^3 + 3\eta^2(1-\eta)$ since the result is correct if all three variables are correct (probability η^3) or if two of them are correct (probability $3\eta^2(1-\eta)$). Therefore, the new distributed bit given by expression 3.10 is equal to $f(x, y)$ with probability P_1:

$$P_1 = P_0^3 + 3P_0^2(1 - P_0)\,. \tag{3.11}$$

Note that $P_1 > P_0$ since $P_0 > 1/2$. This idea can be repeated by concatenating the repetition code. Alice and Bob repeat this whole computation three times with fresh random strings z and fresh random bits r and using two PR-boxes each time, to end up with three distributed bits that are equal to $f(x, y)$ independently with probability P_1. They then distributively compute the majority on these three distributed bits using two more PR-boxes. They have a new distributed bit that is equal to $f(x, y)$ with probabilty P_2:

$$P_2 = P_1^3 + 3P_1^2(1 - P_1)\,, \tag{3.12}$$

again with $P_2 > P_1$. After concatenating k times, they reach a success probability of

$$P_k = P_{k-1}^3 + 3P_{k-1}^2(1 - P_{k-1}) > P_{k-1}\,. \tag{3.13}$$

By choosing k big enough, this probability can be made arbitrarily close to 1. This means that there exists an $\epsilon > 1/2$ such that for all n, there exists a k such that $P_k \geq \epsilon$. This implies that given access to PR-boxes, Alice and Bob can compute any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with success probability at least ϵ using only one bit of communication. This statement means that PR-boxes make communication complexity trivial, which we already know from section 3.1. In the next section we show that the BBLMTU protocol also works with some isotropic nonlocal boxes.

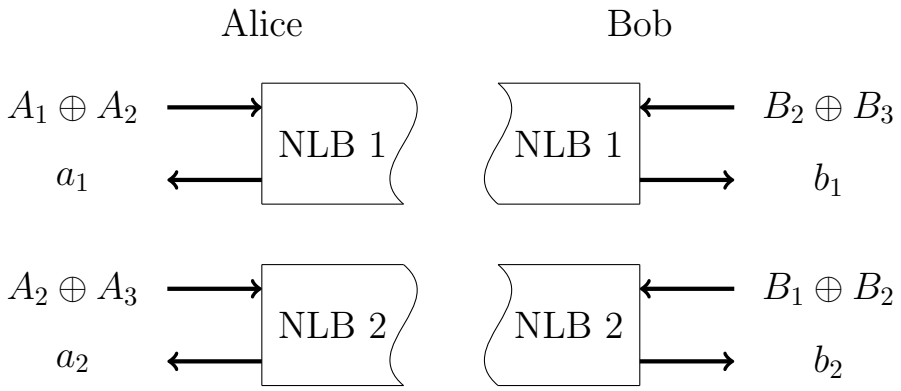


Figure 3.1: Inputs and outputs to the nonlocal boxes in the BBLMTU protocol for the distributed computation of $\mathrm{Maj}_3(A_1 \oplus B_1, A_2 \oplus B_2, A_3 \oplus B_3)$.

3.3.2 Threshold on isotropic nonlocal boxes that make communication complexity trivial

Here, we present a result from [BBL+06], but use a terminology that will make it easier to present our results in section 4.

If instead of PR-boxes, Alice and Bob were given $\frac{1+\delta}{2}$-isoNLBs, their distributed computation of the majority function would be imperfect. Therefore, the computation of equation 3.9 with two nonlocal boxes (figure 3.1) would give them the distributed bit given by expression 3.10, which would be equal to $\mathrm{Maj}_3(A_1 \oplus B_1, A_2 \oplus B_2, A_3 \oplus B_3)$ if and only if both or none of the nonlocal boxes

have correctly computed the multiplications. This happens with probability $\frac{1+\delta^2}{2}$. Conversely, the computation of the majority function is erroneous if and only if exactly one out of the two nonlocal boxes fails to compute a multiplication, which happens with probability $1 - \frac{1+\delta^2}{2} = \frac{1-\delta^2}{2}$. In that case, the distributed bit given by expression 3.10 is equal to $f(x, y)$ if at least two of the distributed inputs to the majority function are equal to $f(x, y) \oplus 1$, since in that case, the error in the computation of the majority function cancels with the error in the inputs.

Therefore, the probability P_k that their distributed bit is equal to $f(x, y)$ after k layers of concatenation becomes

$$P_k = \frac{1+\delta^2}{2}\left(P_{k-1}^3 + 3P_{k-1}^2\left(1 - P_{k-1}\right)\right) + \frac{1-\delta^2}{2}\left(\left(1 - P_{k-1}\right)^3 + 3P_{k-1}\left(1 - P_{k-1}\right)^2\right) . \tag{3.14}$$

To find the values δ for which this recursion relation converges to a probability greater than $1/2$, we re-write equation 3.14 in terms of success biases by defining $\mu_k := 2P_k - 1$, the success bias associated to the success probability P_k. With this change of variable and by re-arranging the terms, equation 3.14 becomes

$$\mu_k = \frac{\delta^2}{2}\left(3\mu_{k-1} - \mu_{k-1}^3\right) . \tag{3.15}$$

This recursion relation is a one-dimensional map. To study the behaviour of this map in the range $\mu_{k-1} \in [0, 1]$, we look at its fixed points, the values for which the success bias remains unchanged after taking the majority. The fixed points are the solutions of

$$\mu = \frac{\delta^2}{2}\left(3\mu - \mu^3\right) . \tag{3.16}$$

From this equation, we see that in the range $\mu \in [0, 1]$, the fixed points are:

$$\mu^* = 0 \tag{3.17}$$

$$\mu^{**} = \sqrt{3 - \frac{2}{\delta^2}} . \tag{3.18}$$

We say a fixed point is stable when any success bias in its vicinity is mapped to a point closer to that fixed point with each iteration of the map. A fixed point is unstable if all the surrounding success biases move away from that fixed point with

each iteration. A fixed point is stable if the derivative of the map at this point is smaller than 1 (see [Str18]):

$$\left.\frac{\mathrm{d}\mu_k}{\mathrm{d}\mu_{k-1}}\right|_{\mu_{k-1}=\mu^*} < 1 \tag{3.19}$$

and is unstable if the derivative is greater than 1. In the case where the derivative is equal to 1, further information is needed to determine the stability of the fixed point. We see that the fixed point $\mu^* = 0$ is unstable when $\delta > \sqrt{2/3}$:

$$\left.\frac{\mathrm{d}\mu_k}{\mathrm{d}\mu_{k-1}}\right|_{\mu_{k-1}=\mu^*} = \frac{3\delta^2}{2} \begin{cases} > 1 & \text{if } |\delta| > \sqrt{2/3} \\ < 1 & \text{if } |\delta| < \sqrt{2/3}\,. \end{cases} \tag{3.20}$$

A similar analysis reveals that the fixed point μ^{**} is stable and distinct from μ^* when $\delta > \sqrt{2/3}$ or $\delta < -\sqrt{2/3}$. This means that in this regime, any success bias greater than 0 will approach μ^{**} with each iteration of the map. Therefore, $\frac{1+\delta}{2}$-isoNLBs with $\delta > \sqrt{2/3}$ or $\delta < -\sqrt{2/3}$, can be used to distributively compute any function in the communication complexity scetting without communication, with probability arbitrarily close to $\sqrt{3 - \frac{2}{\delta^2}}$.

The threshold on p such that p-isoNLBs make communication complexity trivial with the BBLMTU protocol is

$$\mathscr{P}_{\mathrm{BBLMTU}} := \frac{3+\sqrt{6}}{6} \tag{3.21}$$

which is the success probability corresponding to the threshold on δ

$$\delta_{\mathrm{BBLMTU}} := \sqrt{\frac{2}{3}}\,. \tag{3.22}$$

This result means that any reasonable physical theory should not allow isotropic nonlocal correlations that respect the CHSH condition with probability more than $\mathscr{P}_{\mathrm{BBLMTU}}$ since these stronger correlations lead to trivial communication complexity. Figure 3.2 displays a visual representation of the nonlocal boxes in the CHSH-CHSH′ slice for which we know communication complexity to be trivial from the BBLMTU protocol [BBL+06]. Because correlated nonlocal boxes can be depolarized to isotropic nonlocal boxes with the same p_{CHSH} (see section 3.2), all nonlocal boxes that are a convex combination of the PR-box, the $\overline{\mathrm{PR}}$-box and the SR-box with $p_{\mathrm{CHSH}} > \mathscr{P}_{\mathrm{BBLMTU}}$ can be transformed into isotropic nonlocal boxes

with $p_{\text{CHSH}} > \mathscr{P}_{\text{BBLMTU}}$ and therefore violate NTCC [BS09]. Figure 3.3 combines these results by showing a projection on the CHSH-CHSH′ slice of the nonlocal boxes that are convex combinations of the PR-box, the $\overline{\text{PR}}$-box and the SR-box that are known to make communication complexity trivial.

3.4 On the optimality of $\mathscr{P}_{\text{BBLMTU}}$

In the error correction phase of the BBLMTU protocol, the 3-input majority function is used to improve the success probability of the initial distributed computation. One could ask if we could get a better threshold on nonlocal boxes that make complexity trivial by using a different decoding function while still using the repetition code. This is the approach considered by Mori in [Mor16], on which this section is based. For example, we could consider the 5-input majority function, or more generally, the m-input majority function. Even more generally, we could consider any function g of m inputs to decode the m-bit repetition code in the BBLMTU protocol.

A decoding function g will increase the success probability of the computation only if it is itself correctly computed with high enough probability. In this work, we call the *threshold on the decoding function* the smallest value q_t for which this function increases the success probability of the computation when it is itself computed with any probability $q > q_t$.

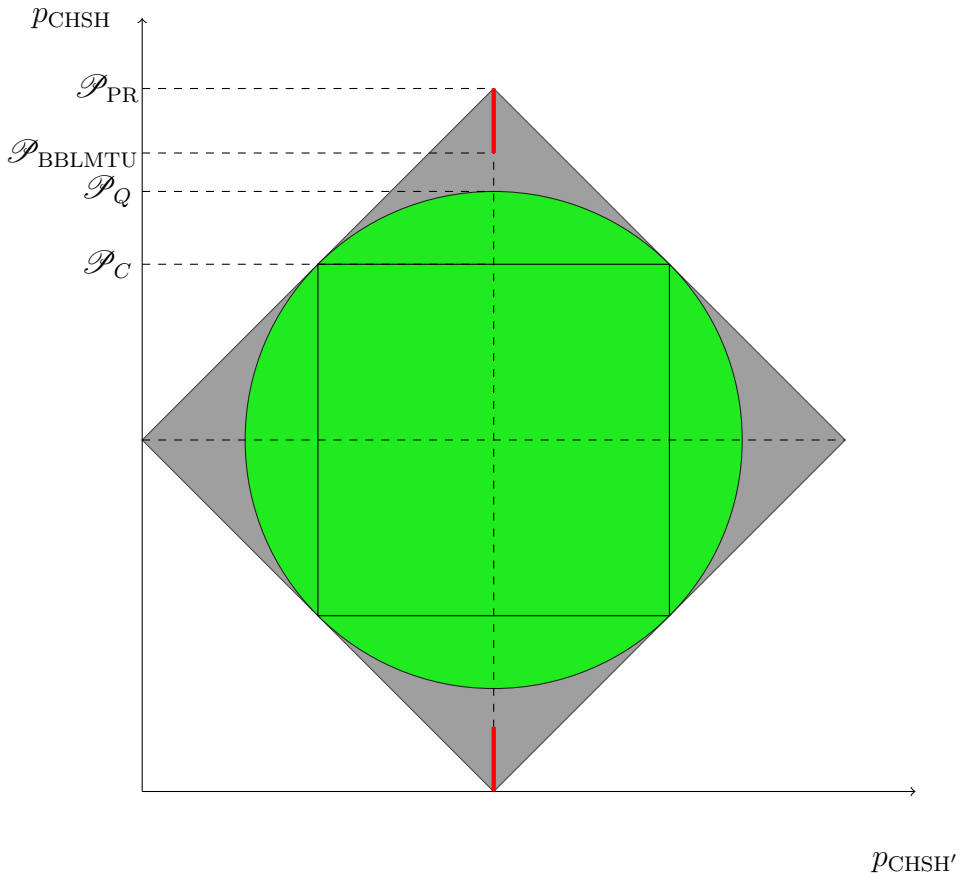
Each possible decoding function will lead to a threshold on nonlocal boxes p_t, the smallest value for which for all $p > p_t$, the decoding function can be distributively computed with probability greater than q_t with p-isoNLBs. In other words, the threshold on the decoding function q_t dictates how well the function has to be computed to increase the success probability of the computation, and the threshold on nonlocal boxes p_t dictates what p-isoNLBs can achieve q_t.

The choice of the decoding function g affects the threshold on nonlocal boxes in two ways:

1. The value q_t has to be low to tolerate errors in the computation of g itself.

2. The way g is computed with the nonlocal boxes will affect how q_t translates to p_t.

For example, in the case of 3-input majority, this function needs to be correctly computed with probability q greater than 5/6 [vN56] in order to increase the success probability of its inputs, meaning that for the 3-input majority, $q_t = 5/6$. Also,



(a) The nonlocal boxes in the green region of the CHSH-CHSH′ slice are known to respect NTCC. The ones on the red lines are known to violate NTCC from [BBL+06]. In the gray area, it is unknown if NTCC holds.

Point	Value	CHSH probability of
$\mathscr{P}_{\text{PR}}$	1	PR-box
$\mathscr{P}_{\text{BBLMTU}}$	$\frac{3+\sqrt{6}}{6} \approx 91\%$	Threshold nonlocal box from [BBL+06]
$\mathscr{P}_Q$	$\frac{2+\sqrt{2}}{4} \approx 85\%$	Best quantum approximation of a PR-box
$\mathscr{P}_C$	3/4	Best classical approximation of a PR-box

(b) Summary of relevant p_{CHSH} values.

Figure 3.2: Nonlocal boxes from the CHSH-CHSH′ slice for which communication complexity is known to be trivial and non-trivial from [BBL+06].

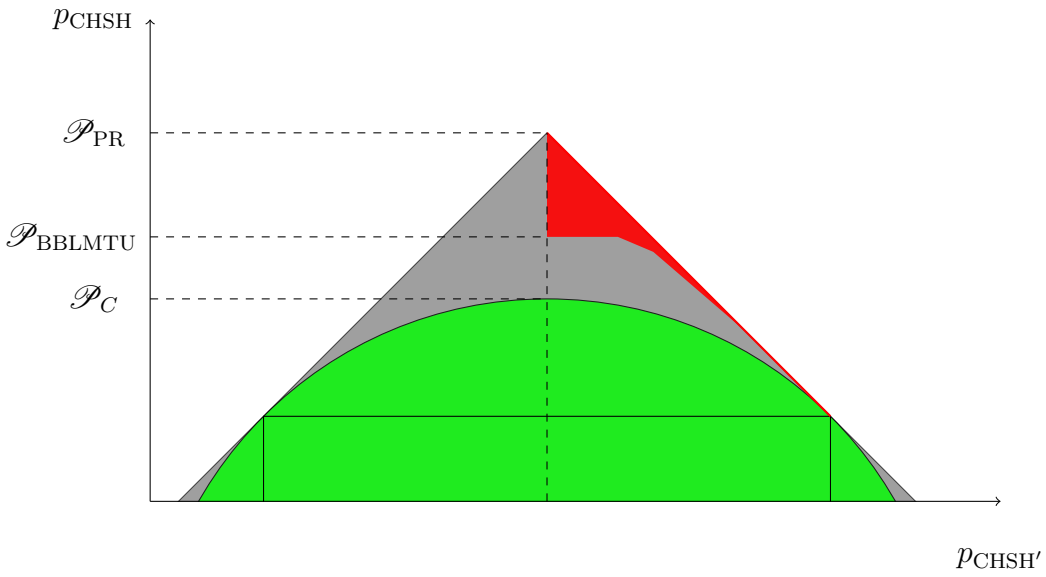


Figure 3.3: CHSH-CHSH′ slice on which is projected the nonlocal boxes that are convex combinations of the PR-box, the $\overline{\text{PR}}$-box and the SR-box that are known to make communication complexity trivial (in red). This figure is an approximation of the real region shown in figure 4 of [BS09].

since the distributed computation of 3-input majority takes two nonlocal boxes, given p-isoNLBs, we know that the 3-input majority function can be computed with probability $q = p^2 + (1-p)^2$ [BBL+06]. This expression that links the CHSH probability p of the nonlocal boxes to the probability q of successfully computing the decoding function dictates how q_t translates to p_t and can differ for other functions. Therefore, when looking for a decoding function with a better threshold on nonlocal boxes for trivial communication complexity, we need to make assumptions on the protocol that is used to distributively compute the function to get a value p_t from the threshold q_t.

In [Mor16], the author shows that the threshold on nonlocal boxes that make communication complexity trivial cannot be improved by replacing the 3-input majority function in the BBLMTU protocol by a different decoding function g. To show this, the author makes the assumption that the decoding function is distributively computed using a protocol we call *PPKSWZ*[2] after the authors of [PPK+09]

[2]In [Mor16], the PPKSWZ protocol is called *Pawłowski et al's protocol*.

(Pawłowski, Paterek, Kaszlikowski, Scarani, Winter and Żukowski). We present this protocol in section 3.4.2. Before we introduce the PPKSWZ protocol, we define the *address function*, which is at the heart of the PPKSWZ protocol.

3.4.1 Distributed computation of the address function

The address function is defined as follows:

$$\mathrm{Addr}_n(x_0, ...x_{2^n-1}, y_0, ..., y_{n-1}) := x_y \tag{3.23}$$

where the x_i are bits (in our case, known by Alice) and the y_i are bits describing the index $y = \sum_{i=0}^{n-1} y_i 2^i$ (in our case, known by Bob). Using only one $\frac{1+\delta}{2}$-isoNLBs, it is possible to distributively compute Addr_1 correctly with probability $\frac{1+\delta}{2}$ [Mor16]:

$$\mathrm{Addr}_1(x_0, x_1, y_0) = x_0 \oplus y_0(x_0 \oplus x_1) \tag{3.24}$$

$$= x_y\,. \tag{3.25}$$

The nonlocal box is used with inputs $x_0 \oplus x_1$ and y_0 and outputs a and b. Alice holds $A = x_0 \oplus a$ and Bob $B = b$ such that

$$A \oplus B = \mathrm{Addr}_1(x_0, x_1, y_0) \tag{3.26}$$

with probability $\frac{1+\delta}{2}$. Note that when the multiplication is not correctly computed by the nonlocal box, the resulting distributed bit is equal to $x_y \oplus 1$. The computation of the address function allows Bob to select which of Alice's bits they hold distributively.

For $k > 1$, the function Addr_k can be reduced to the computation of two Addr_{k-1} and one Addr_1 functions [Mor16]:

$$\mathrm{Addr}_k(x_0, ..., x_{2^k-1}, y_0, ...y_{k-1}) = \mathrm{Addr}_1(x'_0, x'_1, y_{k-1}) \tag{3.27}$$

where

$$x'_0 = \mathrm{Addr}_{k-1}(x_0, ..., x_{2^{k-1}-1}, y_0, ..., y_{k-2}) \tag{3.28}$$

$$x'_1 = \mathrm{Addr}_{k-1}(x_{2^{k-1}}, ..., x_{2^k-1}, y_0, ..., y_{k-2})\,. \tag{3.29}$$

These Addr_{k-1} functions can in turn be decomposed into Addr_{k-2} and Addr_1 functions. The same idea can be applied until there only remains Addr_1 functions, as shown graphically in figure 3.4.

With this decomposition, Alice and Bob distributively compute address functions that become the inputs to other address functions. This means that they need to distributively compute address functions on inputs that are distributed bits rather than

bits. In the next few lines, we explain how the address function can be distributively computed when its inputs are distributed bits. Let

$$d_0 = d_0^{(A)} \oplus d_0^{(B)} \tag{3.30}$$

$$d_1 = d_1^{(A)} \oplus d_1^{(B)} \tag{3.31}$$

be distributed bits, where the $d_i^{(A)}$ are known by Alice and the $d_i^{(B)}$, by Bob. The value $\mathrm{Addr}_1(d_0, d_1, y_0)$ can be decomposed in the following way:

$$\begin{aligned} \mathrm{Addr}_1(d_0, d_1, y_0) &= d_y \\ &= d_y^{(A)} \oplus d_y^{(B)} \\ &= \mathrm{Addr}_1(d_0^{(A)}, d_1^{(A)}, y_0) \oplus d_y^{(B)} \,. \end{aligned} \tag{3.32}$$

Since the bit $d_y^{(B)}$ is trivially computed by Bob who knows $d_0^{(B)}$ and $d_1^{(B)}$, the address function can be computed on distributed bits d_0, d_1 by adding $d_y^{(B)}$ to the distributed computation of the address function on Alice's share of d_0, d_1.

When $\frac{1+\delta}{2}$-isoNLBs are used in the computation of Addr_n with this decomposition, one nonlocal box is required for every Addr_1 function, for a total of

$$\sum_{i=1}^{n} 2^{n-i} = 2^n - 1 \,. \tag{3.33}$$

However, we see from figure 3.4 that only the errors affecting the computation of the address functions in the path from x_y to the top of the tree can have an effect on the outcome. This means that there are only n computations of Addr_1 functions that actually contribute to the outcome. Errors occurring in the computation of these functions cancel in pairs, meaning that, when using $\frac{1+\delta}{2}$-isoNLBs, the success probability of this protocol is $\frac{1+\delta^n}{2}$ [Mor16].

3.4.2 The PPKSWZ protocol

This protocol was first suggested in [PPK+09]. Built around the address function, this protocol is a method that uses $\frac{1+\delta}{2}$-isoNLBs to distributively compute any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with probability $\frac{1+\delta^n}{2}$ without communication.

Let $F(x)$ be the string such that $F(x)_k = f(x,k)$, where we have used k to denote an index as well as the n-bit string corresponding to the binary representation of that index. Then

$$f(x,y) = \mathrm{Addr}_n(F(x)_0, ..., F(x)_{2^n-1}, y_0, ..., y_{n-1}) \,, \tag{3.34}$$

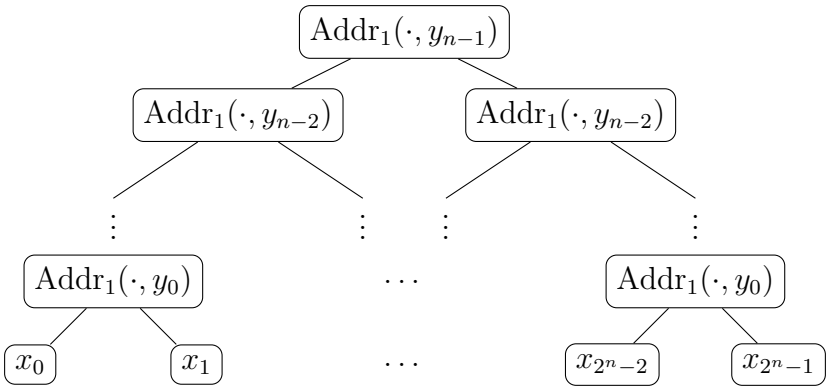


Figure 3.4: Decomposition of Addr_n function into multiple Addr_1 functions. The computation is done from the bottom to the top. The dot $(\cdot)$ in $\mathrm{Addr}_1(\cdot, y_i)$ represents the two elements directly below, meaning that $\mathrm{Addr}_1(\cdot, y_i)$ is equal to the element from the left branch if $y_i = 0$ and to the element from the right branch if $y_i = 1$.

which can be distributively computed with probability $\frac{1+\delta^n}{2}$ using the ideas from section 3.4.1.

In summary, the idea behind the PPKSWZ protocol is to distributively compute the address function where Alice's inputs are the values of the function $f(x, y')$ for each possible values of y'. Bob selects the input corresponding to $f(x, y)$.

3.4.3 Conditions on the decoding function

For a given m-input decoding function g, we consider the success probability of its output as a function of the success probability of its inputs at computing the function f, that is $P\left[g(z_1, ..., z_m) = f(x, y)\right]$, where the z_i are the m initial distributed computations of $f(x, y)$. More precisely, we consider the success bias associated with this probability, as a function of the success bias ε of the initial computation, that we will denote $\mathrm{Bias}_g(\varepsilon)$. We say the function g amplifies a bias ε_0 if $\mathrm{Bias}_g(\varepsilon_0) > \varepsilon_0$.

Since the initial distributed computation of the BBLMTU protocol has a success probability that approaches $1/2$ as n grows, the decoding function must increase arbitrarily-close-to-0 success biases in order to amplify the bias for all n. Following this, we find that, to be usable in the BBLMTU protocol, the decoding function g

must respect the following conditions (see [Mor16] for more details):

$$\mathrm{Bias}_g(0) = 0 \tag{3.35}$$

$$\rho \frac{\mathrm{dBias}_g(\epsilon)}{\mathrm{d}\epsilon} > 1\,, \tag{3.36}$$

where ρ is the success bias associated with the computation of the decoding function g. In [Mor16], it is assumed that g is computed by the PPKSWZ protocol with $\frac{1+\delta}{2}$-isoNLBs, which means $\rho = \delta^n$. The author of [Mor16] also takes into account that in some cases, g is such that its inputs can be compressed and the use of the PPKSWZ protocol will yield a different relationship between ρ and δ. Using these ideas, he shows that the 3-input majority function yields the optimal threshold on nonlocal boxes that make communication complexity trivial with the BBLMTU protocol.

Chapter 4

Expanding the set of nonlocal correlations that are known to violate NTCC

In this chapter, we present our contribution in the search for intuition on the limits of quantum nonlocality. We build on the known results presented in previous sections to improve the understanding of the consequences of stronger-than-quantum nonlocality on the principle of non-trivial communication complexity. From the impossibility result presented in section 3.4, we know that there is little hope of improving the BBLMTU protocol without making major changes. Instead, we study the BBLMTU protocol with more general nonlocal boxes to find new bounds on nonlocal correlations that make communication complexity trivial.

In section 4.1, we present tools that help us compute the success probability of the BBLMTU protocol when it uses general nonlocal boxes. Then, using these tools, we present our main results in sections 4.2, 4.3 and 4.4. Theorem 1 in section 4.2 gives the set of nonlocal correlations from the CHSH-CHSH′ subspace that make communication complexity trivial with the BBLMTU protocol. Theorem 2 in section 4.3 gives a bound from NTCC on correlations that are a convex combination of the PR-box, the $\overline{\text{PR}}$-box and the SR-box. Finally, in section 4.4, we give a new proof that all super-quantum correlated nonlocal boxes make communication complexity trivial. Our proof is different from the existing proof from [BS09] because it relies on a protocol that does not use nonlocal box distillation. This new approach provides an additional tool for the study of nonlocal correlations. Also, since our protocol does not suffer from the same limitations as protocols that use nonlocal box distillation, there is hope that our ideas could be used to further expand the set of nonlocal

correlations that are known to violate the principle of non-trivial communication complexity.

4.1 Success probability of the BBLMTU protocol with general nonlocal boxes

In this section, we present tools that enable us to calculate the success probability of the BBLMTU protocol when it uses general nonlocal boxes, which leads us to our main results, presented in sections 4.2 and 4.3. Among the tools we use to achieve our results, we use tensors to represent the probability of occurrence of certain events. As discussed in section 2.3.3, in our context, a rank-m tensor could be replaced by a real function on m integers, each corresponding to one index. However, we chose the tensor representation because, as will see the reader who is familiar with the concept of tensor networks, tensors can become a powerful tool to adapt our method to study protocols that are more complex than the BBLMTU protocol (see [Orú14] for an introduction to tensor networks).

In the BBLMTU protocol described in section 3.3, two parties wish to compute a value $f(x, y)$ with $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and $x, y \in \{0,1\}^n$. In the error correction phase, the two parties use isotropic nonlocal boxes to distributively compute two multiplications that are required for the computation of the majority function. A p-isoNLB computes a multiplication ij correctly with probability p for every $i, j \in \{0,1\}$, independently of the values i and j. However, for non-isotropic nonlocal boxes, the probability of correctly computing a multiplication ij depends on i and j. In this section, we consider nonlocal boxes that can compute the multiplication ij with probability $q_{i,j}$ and take into account the fact that the inputs to the nonlocal boxes in the BBLMTU protocol are not independent. We do this in order to generalize equation 3.14 that gives the success probability P_k after k layers of concatenation of the repetition code in the BBLMTU protocol.

Recall that the majority function on three distributed bits $A_1 \oplus B_1$, $A_2 \oplus B_2$ and $A_3 \oplus B_3$ is equal to (from equation 3.9):

$$\begin{aligned}\mathrm{Maj}_3(A_1 \oplus B_1, A_2 \oplus B_2, A_3 \oplus B_3) =& \mathrm{Maj}_3(A_1, A_2, A_3) \oplus \mathrm{Maj}_3(B_1, B_2, B_3) \\ &\oplus (A_1 \oplus A_2)(B_2 \oplus B_3) \oplus (A_2 \oplus A_3)(B_1 \oplus B_2)\,.\end{aligned}$$

Two nonlocal boxes are needed to distributively compute the last two terms (see [BBL+06])

$$(A_1 \oplus A_2)(B_2 \oplus B_3) \oplus (A_2 \oplus A_3)(B_1 \oplus B_2)\,. \tag{4.1}$$

If the three distributed bits $A_i \oplus B_i$ are values obtained after $k-1$ layers in the BBLMTU protocol, then

$$A_i \oplus B_i = \begin{cases} f(x,y) & \text{with prob. } P_{k-1} \\ f(x,y) \oplus 1 & \text{with prob. } 1 - P_{k-1} \end{cases} \tag{4.2}$$

by the definition of P_{k-1}. For $k > 1$, the values A_i and B_i come from the distributed computation of the majority function of the layer $k-1 > 0$. Because these values are obtained by adding together outputs from nonlocal boxes, they are locally uniformly random meaning that, when considered locally (with no knowledge of B_i), each value A_i is a random bit. The value B_i can then be expressed as

$$B_i = A_i \oplus f(x,y) \oplus e_i \tag{4.3}$$

where $e_i = 0$ if $A_i \oplus B_i = f(x,y)$ and $e_i = 1$ otherwise. Note that since the distributed bit $A_i \oplus B_i$ is the result of a (imperfect) computation of $f(x,y)$, e_i indicates if the distributed bit $A_i \oplus B_i$ contains an error. The expression 4.1 can now be written as

$$\begin{aligned} &(A_1 \oplus A_2)(B_2 \oplus B_3) \oplus (A_2 \oplus A_3)(B_1 \oplus B_2) \\ &\qquad = (A_1 \oplus A_2)\,(A_2 \oplus f(x,y) \oplus e_2 \oplus B_3 \oplus f(x,y) \oplus e_3) \\ &\qquad \oplus (A_2 \oplus A_3)\,(A_1 \oplus f(x,y) \oplus e_1 \oplus B_2 \oplus f(x,y) \oplus e_2) \\ &\qquad = (A_1 \oplus A_2)(A_2 \oplus A_3 \oplus e_2 \oplus e_3) \oplus (A_2 \oplus A_3)(A_1 \oplus A_2 \oplus e_1 \oplus e_2)\,. \end{aligned} \tag{4.4}$$

Because A_1, A_2 and A_3 are independent random bits, so are $A_1 \oplus A_2$ and $A_2 \oplus A_3$. Define r_1 and r_2 such that

$$r_1 := A_1 \oplus A_2 \tag{4.5}$$

$$r_2 := A_2 \oplus A_3\,. \tag{4.6}$$

Thus, the two multiplications that require the use of nonlocal boxes in the distributed computation of the majority function are

$$r_1(r_2 \oplus e_2 \oplus e_3) \oplus r_2(r_1 \oplus e_1 \oplus e_2)\,. \tag{4.7}$$

For the concatenation layer k in the BBLMTU protocol, we define the rank-5 tensor $T^{(k)}$ such that the element $T^{(k)}_{\alpha\beta\gamma\delta\epsilon}$, with $\alpha, \beta, \gamma, \delta, \epsilon \in \{0,1\}$, is the probability

that the following equations hold:

$$\begin{aligned} e_1 &= \alpha \\ e_2 &= \beta \\ e_3 &= \gamma \\ r_1 &= \delta \\ r_2 &= \epsilon\,. \end{aligned} \tag{4.8}$$

Additionally, we define the rank-5 tensor M such that the element $M_{\alpha\beta\gamma\delta\epsilon}$, again with $\alpha, \beta, \gamma, \delta, \epsilon \in \{0, 1\}$, is the probability that a computation of the majority function on the kth layer gives $f(x, y)$, knowing that the equations 4.8 hold.

Let z_k be the outcome of the BBLMTU protocol after k concatenation layers, known distributively by Alice and Bob. Following the definitions of the tensors $T^{(k)}$ and M, the probability P_k that z_k is equal to $f(x, y)$ is

$$P_k = \sum_{\alpha,\beta,\gamma,\delta,\epsilon} T^{(k)}_{\alpha\beta\gamma\delta\epsilon} M_{\alpha\beta\gamma\delta\epsilon}\,. \tag{4.9}$$

For the BBLMTU protocol, we can express the elements of the tensor $T^{(k)}$ in terms of P_{k-1}. Then the equation 4.9 becomes a one-dimensional map that gives the new success probability after taking the majority (level k) of three independent computations of concatenation layer $k-1$. The fixed points of this map can be analyzed similarly to what is presented in section 3.3.2. Lemma 1 gives an expression for $T^{(k)}$ and Lemma 2 gives an expression for M that will enable us to analyze this map.

Lemma 1. *Let P_{k-1} be the success probability after $k-1$ layers of concatenation in the BBLMTU protocol. The tensor $T^{(k)}$ is given by*

$$T^{(k)}_{\alpha\beta\gamma\delta\epsilon} = \frac{1}{4} P_{k-1}^{3-\alpha-\beta-\gamma} \left(1 - P_{k-1}\right)^{\alpha+\beta+\gamma}\,. \tag{4.10}$$

Proof. Since e_1, e_2 and e_3 indicate if three independent computations contain errors, they each are equal to 0 with probability P_{k-1} and equal to 1 with probability $1-P_{k-1}$. Thus, the probability of getting the value $e_1 = \alpha$ is P_{k-1} if $\alpha = 0$ and $1-P_{k-1}$ if $\alpha = 1$, which can be summarized as $P_{k-1}^{1-\alpha}(1-P_{k-1})^{\alpha}$. The same goes for $e_2 = \beta$ and $e_3 = \gamma$.

Since r_1 and r_2 are uniformly random bits independent of each other and of the values e_i, each pair (r_1, r_2) happens with equal probability, that is $1/4$. Therefore,

the probability of getting the values e_1, e_2, e_3, r_1 and r_2 is the product of the marginal probability of each value, meaning that

$$\begin{aligned} T^{(k)}_{\alpha\beta\gamma\delta\epsilon} &= \frac{1}{4} P_{k-1}^{1-\alpha} P_{k-1}^{1-\beta} P_{k-1}^{1-\gamma} (1-P_{k-1})^{\alpha} (1-P_{k-1})^{\beta} (1-P_{k-1})^{\gamma} \\ &= \frac{1}{4} P_{k-1}^{3-\alpha-\beta-\gamma} \left(1-P_{k-1}\right)^{\alpha+\beta+\gamma} . \end{aligned}$$ □

Lemma 2. *Suppose the computation of the majority function in the BBLMTU protocol is done with two nonlocal boxes as in equation 4.7, each computing the product ij (with $i, j \in \{0,1\}$) with probability $q_{i,j}$, with $q_{i,j} \in [0,1]$. Define $\eta_{i,j} := 2q_{i,j} - 1$, the bias associated with the probability $q_{i,j}$. Then, the tensor M can be written as*

$$M_{\alpha\beta\gamma\delta\epsilon} = \frac{1 + (-1)^{\mathrm{Maj}(\alpha,\beta,\gamma)} \eta_{\delta,(\epsilon\oplus\beta\oplus\gamma)} \eta_{\epsilon,(\delta\oplus\alpha\oplus\beta)}}{2} . \tag{4.11}$$

Proof. In the case of the elements with $\mathrm{Maj}(\alpha,\beta,\gamma) = 0$, at least two of the inputs to the majority function in the BBLMTU protocol are equal to $f(x,y)$, meaning that the outcome of the distributed majority will be equal to $f(x,y)$ if and only if the majority function is correctly computed. To do so, two nonlocal boxes need to be used to compute the expression 4.7. By definition of $q_{i,j}$ and $\eta_{i,j}$, the probability that the nonlocal box correctly computes $r_1(r_2 \oplus e_2 \oplus e_3)$ when $e_1 = \alpha$, $e_2 = \beta$, $e_3 = \gamma$, $r_1 = \delta$ and $r_2 = \epsilon$ is

$$q_{\delta,(\epsilon\oplus\beta\oplus\gamma)} = \frac{1 + \eta_{\delta,(\epsilon\oplus\beta\oplus\gamma)}}{2} \tag{4.12}$$

and similarly for $r_2(r_1 \oplus e_1 \oplus e_2)$:

$$q_{\epsilon,(\delta\oplus\alpha\oplus\beta)} = \frac{1 + \eta_{\epsilon,(\delta\oplus\alpha\oplus\beta)}}{2} . \tag{4.13}$$

Since two nonlocal box outcomes are added together for this computation, the result will be equal to $f(x,y)$ if both or none of the nonlocal boxes fail to compute a multiplication, which happens with probability

$$\begin{aligned} M_{\alpha\beta\gamma\delta\epsilon} &= q_{\delta,(\epsilon\oplus\beta\oplus\gamma)} q_{\epsilon,(\delta\oplus\alpha\oplus\beta)} + (1 - q_{\delta,(\epsilon\oplus\beta\oplus\gamma)})(1 - q_{\epsilon,(\delta\oplus\alpha\oplus\beta)}) \\ &= \frac{1 + \eta_{\delta,(\epsilon\oplus\beta\oplus\gamma)} \eta_{\epsilon,(\delta\oplus\alpha\oplus\beta)}}{2} . \end{aligned} \tag{4.14}$$

In the case of the elements with $\mathrm{Maj}(\alpha,\beta,\gamma) = 1$, at most one of the inputs to the majority function in the BBLMTU protocol is equal to $f(x,y)$. The outcome of the

majority will be equal to $f(x,y)$ if and only if the majority function is incorrectly computed, which happens if exactly one of the nonlocal boxes fails to correctly compute a multiplication. This happens with probability

$$\begin{aligned} M_{\alpha\beta\gamma\delta\epsilon} &= q_{\delta,(\epsilon\oplus\beta\oplus\gamma)}(1 - q_{\epsilon,(\delta\oplus\alpha\oplus\beta)}) + (1 - q_{\delta,(\epsilon\oplus\beta\oplus\gamma)})q_{\epsilon,(\delta\oplus\alpha\oplus\beta)} \\ &= \frac{1 - \eta_{\delta,(\epsilon\oplus\beta\oplus\gamma)}\eta_{\epsilon,(\delta\oplus\alpha\oplus\beta)}}{2} . \end{aligned} \tag{4.15}$$

Combining equations 4.14 and 4.15, we get equation 4.11. □

4.2 Nonlocal boxes from the CHSH-CHSH′ subspace in the BBLMTU protocol

In this section, we consider correlations in the CHSH-CHSH′ subspace of nonsignaling correlations. To facilitate the notation and show what correlations in the CHSH-CHSH′ subspace violate NTCC with the BBLMTU protocol, we split the subspace in two by first considering correlations of the form

$$P(a,b \mid x,y) = c_1 P_{\mathrm{PR}}(a,b \mid x,y) + c_2 P_{\mathrm{PR}'}(a,b \mid x,y) + (1 - c_1 - c_2) P_{\overline{\mathrm{PR}}}(a,b \mid x,y) \tag{4.16}$$

with $c_1, c_2 \in [0,1]$ and $c_1 + c_2 \leq 1$. These boxes are convex combinations of the PR-box, the PR′-box and the $\overline{\mathrm{PR}}$-box defined in section 2.1.3, meaning that they produce correlations that reside in the region $p_{\mathrm{CHSH}'} \geq 1/2$ of the CHSH-CHSH′ subspace. Then, we consider the other half of the CHSH-CHSH′ subspace, correlations of the form

$$P(a,b \mid x,y) = c_1 P_{\mathrm{PR}}(a,b \mid x,y) + c_2 P_{\overline{\mathrm{PR}'}}(a,b \mid x,y) + (1 - c_1 - c_2) P_{\overline{\mathrm{PR}}}(a,b \mid x,y) \tag{4.17}$$

with $c_1, c_2 \in [0,1]$ and $c_1 + c_2 \leq 1$. These correlations are the ones for which $p_{\mathrm{CHSH}'} \leq 1/2$. Lemma 3 describes the probability that a nonlocal box in each half of the CHSH-CHSH′ slice correctly computes multiplications.

Lemma 3. *Let $i,j \in \{0,1\}$. A nonlocal box producing the correlation described in equation 4.16 correctly computes the product ij with probability $q_{i,j}$, with*

$$\begin{aligned} q_{0,0} &= c_1 \\ q_{0,1} &= c_1 + c_2 \\ q_{1,0} &= c_1 + c_2 \\ q_{1,1} &= c_1 . \end{aligned}$$

A nonlocal box producing the correlation of equation 4.17 correctly computes the product ij with probability $q_{i,j}$, with

$$\begin{aligned} q_{0,0} &= c_1 + c_2 \\ q_{0,1} &= c_1 \\ q_{1,0} &= c_1 \\ q_{1,1} &= c_1 + c_2 \,. \end{aligned}$$

Proof. The value $q_{i,j}$ is the probability that the nonlocal box outputs a and b such that $a \oplus b = ij$ on inputs i and j. Therefore,

$$q_{i,j} = \sum_{\substack{a,b \\ \text{s.t. } a \oplus b = ij}} P(a, b \mid i, j) \,. \tag{4.18}$$

For $q_{0,0}$, using the definitions of the PR-box (equation 2.5), the $\overline{\text{PR}}$-box (equation 2.6) and the PR$'$-box (equation 2.7), we get for a box described by equation 4.16:

$$\begin{aligned} q_{0,0} &= P(0,0 \mid 0,0) + P(1,1 \mid 0,0) \\ &= \frac{c_1}{2} + \frac{c_1}{2} \\ &= c_1 \,. \end{aligned} \tag{4.19}$$

Similarly for the other values $q_{i,j}$:

$$\begin{aligned} q_{0,1} &= P(0,0 \mid 0,1) + P(1,1 \mid 0,1) \\ &= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right) \\ &= c_1 + c_2 \end{aligned} \tag{4.20}$$

$$\begin{aligned} q_{1,0} &= P(0,0 \mid 1,0) + P(1,1 \mid 1,0) \\ &= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right) \\ &= c_1 + c_2 \end{aligned} \tag{4.21}$$

$$\begin{aligned} q_{1,1} &= P(0,1 \mid 1,1) + P(1,0 \mid 1,1) \\ &= \frac{c_1}{2} + \frac{c_1}{2} \\ &= c_1 \,. \end{aligned} \tag{4.22}$$

For a box described by equation 4.17, using the definitions of the PR-box (equation 2.5), the $\overline{\text{PR}}$-box (equation 2.6) and the $\overline{\text{PR}'}$-box (equation 2.9), we get:

$$
\begin{aligned}
q_{0,0} &= P(0,0 \mid 0,0) + P(1,1 \mid 0,0) && (4.23)\\
&= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right)\\
&= c_1 + c_2\\
q_{0,1} &= P(0,0 \mid 0,1) + P(1,1 \mid 0,1) && (4.24)\\
&= \frac{c_1}{2} + \frac{c_1}{2}\\
&= c_1\\
q_{1,0} &= P(0,0 \mid 1,0) + P(1,1 \mid 1,0) && (4.25)\\
&= \frac{c_1}{2} + \frac{c_1}{2}\\
&= c_1\\
q_{1,1} &= P(0,1 \mid 1,1) + P(1,0 \mid 1,1) && (4.26)\\
&= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right)\\
&= c_1 + c_2\,. && \square
\end{aligned}
$$

The values $q_{i,j}$ can be used to compute the values $\eta_{i,j} = 2q_{i,j} - 1$, which in turn can be inserted in the expression 4.11 for the tensor M. With these values, the analysis of equation 4.9 leads us to theorem 1, as shown below.

Theorem 1. *Nonlocal boxes producing the correlation described in equation 4.16 and nonlocal boxes producing the correlation described in equation 4.17 violate NTCC if*

$$
6c_1^2 + 3(2c_1 - 1)c_2 + 2c_2^2 - 6c_1 + \frac{3}{2} > 1\,. \tag{4.27}
$$

Proof. From equation 4.9, lemma 1 and lemma 2, we get the following expression for P_k:

$$
\begin{aligned}
P_k &= \sum_{\alpha,\beta,\gamma,\delta,\epsilon} T^{(k)}_{\alpha\beta\gamma\delta\epsilon} M_{\alpha\beta\gamma\delta\epsilon}\\
&= \sum_{\alpha,\beta,\gamma,\delta,\epsilon} \left(\frac{1}{4} P_{k-1}^{3-\alpha-\beta-\gamma} \left(1 - P_{k-1}\right)^{\alpha+\beta+\gamma}\right) \left(\frac{1 + (-1)^{\mathrm{Maj}(\alpha,\beta,\gamma)}\, \eta_{\delta,(\epsilon\oplus\beta\oplus\gamma)}\eta_{\epsilon,(\delta\oplus\alpha\oplus\beta)}}{2}\right).
\end{aligned} \tag{4.28}
$$

Defining $\mu_k := 2P_k - 1$, the success bias associated with P_k and defining the variable $W := 2\eta_{1,1}\left(\eta_{0,0} + \eta_{0,1} + \eta_{1,0}\right)$ to make the expression more manageable, equation 4.28 yields

$$\begin{aligned}\mu_k =& \frac{\mu_{k-1}}{16}\left(3\eta_{0,0}^2 + 2\eta_{0,0}\eta_{0,1} + \eta_{0,1}^2 + 2\left(\eta_{0,0} + 3\eta_{0,1}\right)\eta_{1,0} + \eta_{1,0}^2 + W + 3\eta_{1,1}^2\right) \\ &+ \frac{\mu_{k-1}^3}{16}\left(\eta_{0,0}^2 - 2\eta_{0,0}\eta_{0,1} - \eta_{0,1}^2 - 2\left(\eta_{0,0} - \eta_{0,1}\right)\eta_{1,0} - \eta_{1,0}^2 - W + \eta_{1,1}^2\right) . \quad (4.29)\end{aligned}$$

Combining this with lemma 3, we get, for nonlocal boxes described by equation 4.16:

$$\begin{aligned}\mu_k =& \mu_{k-1}\left(6c_1^2 + 3(2c_1 - 1)c_2 + 2c_2^2 - 6c_1 + \frac{3}{2}\right) \\ &- \mu_{k-1}^3\left(2c_1^2 + (2c_1 - 1)c_2 - 2c_1 + \frac{1}{2}\right) . \quad (4.30)\end{aligned}$$

This is also what we get for nonlocal boxes described by equation 4.17. It turns out that the map 4.30 is the same for both halves of the CHSH-CHSH′ slice, meaning that from this point, our analysis applies to all nonlocal boxes described by equations 4.16 and 4.17.

This map has a fixed point at $\mu_{k-1} = 0$. Just like in the analysis from section 3.3.2, this fixed point needs to be unstable for the success bias to approach a constant greater than 0 with each iteration, which happens when

$$\left.\frac{\mathrm{d}\mu_k}{\mathrm{d}\mu_{k-1}}\right|_{\mu_{k-1}=0} > 1 . \quad (4.31)$$

Direct computation of this derivative leads to the following condition on the nonlocal boxes:

$$6c_1^2 + 3(2c_1 - 1)c_2 + 2c_2^2 - 6c_1 + \frac{3}{2} > 1 . \quad (4.32)$$

This is valid for both nonlocal boxes described by equations 4.16 and 4.17 since in both cases, the map 4.30 is the same. □

We can formulate the condition 4.27 in terms of the parameters p_{CHSH} and $p_{\mathrm{CHSH}'}$ by performing a change of variable. Noting that

$$p_{\mathrm{CHSH}} = \frac{1}{4}\left(q_{0,0} + q_{0,1} + q_{1,0} + q_{1,1}\right) \quad (4.33)$$

$$p_{\mathrm{CHSH}'} = \frac{1}{4}\left(1 - q_{0,0} + q_{0,1} + q_{1,0} + 1 - q_{1,1}\right) . \quad (4.34)$$

we find that the condition on nonlocal boxes from the CHSH-CHSH′ subspace that violate NTCC with the BBLMTU protocol is

$$6p_{\text{CHSH}}^2 + 2p_{\text{CHSH}'}^2 - 6p_{\text{CHSH}} - 2p_{\text{CHSH}'} + 2 > 1\,. \tag{4.35}$$

The nonlocal boxes in the CHSH-CHSH′ slice that respect this condition are represented in figure 4.1.

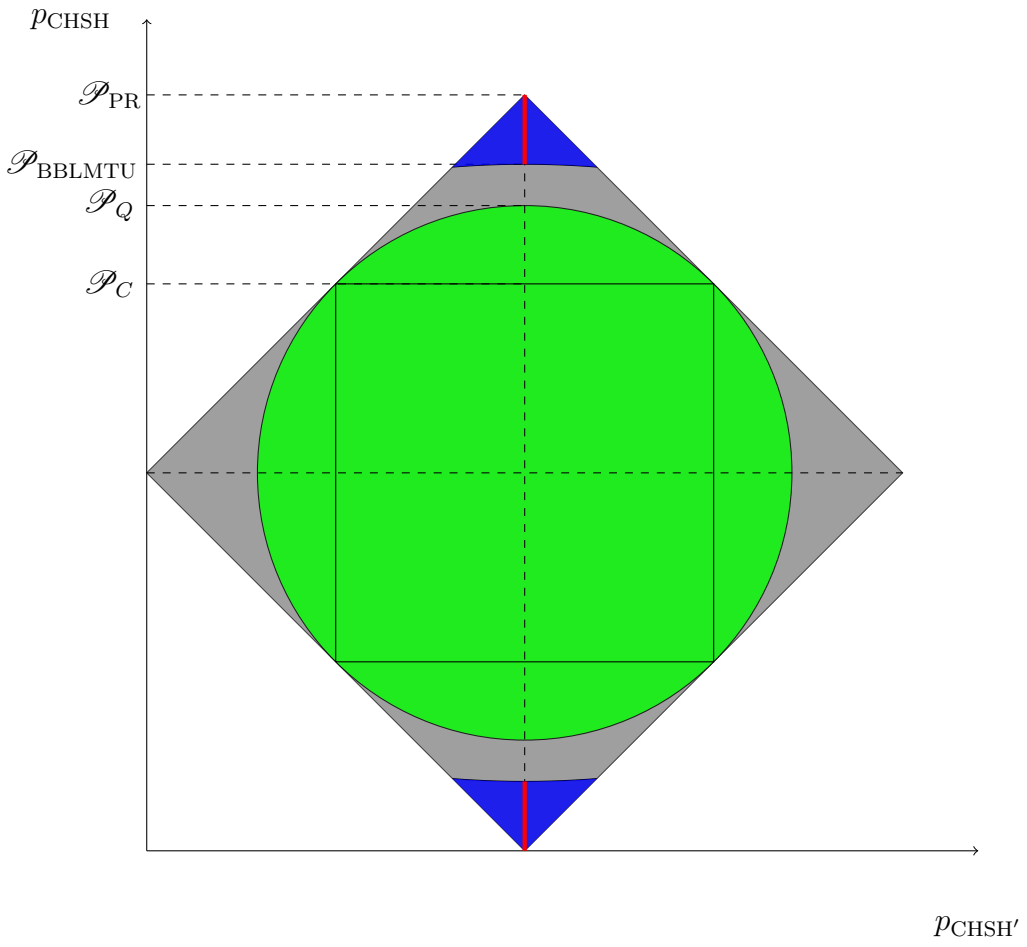


Figure 4.1: Nonlocal boxes that violate NTCC with the BBLMTU protocol (blue and red). In red is the region from [BBL+06] and the blue region is our contribution.

4.2.1 Notable case

The case $c_2 = 0$ is the case of isotropic nonlocal boxes. Equation 4.27 becomes

$$6c_1^2 - 6c_1 + \frac{3}{2} > 1 \tag{4.36}$$

for which the solutions are

$$c_1 > \frac{3+\sqrt{6}}{6} \tag{4.37}$$

$$c_1 < \frac{3-\sqrt{6}}{6}\,. \tag{4.38}$$

As expected, these conditions correspond to the threshold on p-isoNLBs, $\mathscr{P}_{\text{BBLMTU}}$ from [BBL+06], presented in section 3.3.2.

4.3 Generalized correlated nonlocal boxes in the BBLMTU protocol

Now, consider nonlocal boxes that are convex combinations of the PR-box (equation 2.5), the $\overline{\text{PR}}$-box (equation 2.6) and the SR-box (equation 2.10). These boxes produce correlations of the form

$$P(a,b \mid x,y) = c_1 P_{\text{PR}}(a,b \mid x,y) + c_2 P_{\text{SR}}(a,b \mid x,y) + (1-c_1-c_2) P_{\overline{\text{PR}}}(a,b \mid x,y) \tag{4.39}$$

with $c_1, c_2 \in [0,1]$ and $c_1 + c_2 \leq 1$. These correlations are not in the CHSH-CHSH′ subspace when $c_2 \neq 0$. They correspond to the correlations that are studied in [BS09] for nonlocal box distillation. In this work, we call the nonlocal boxes that generate these correlations *generalized correlated nonlocal boxes*. In order to find a condition on the nonlocal boxes of this type that make communication complexity trivial with the BBLMTU protocol, we need to compute the values $\eta_{i,j}$ for those boxes. Lemma 4 gives the probability of correctly computing multiplications with such a nonlocal box, $q_{i,j}$, from which we can find $\eta_{i,j}$.

Lemma 4. *Let $i, j \in \{0, 1\}$. A nonlocal box producing the correlation described in equation 4.39 correctly computes the product ij with probability $q_{i,j}$, with*

$$\begin{aligned} q_{0,0} &= c_1 + c_2 \\ q_{0,1} &= c_1 + c_2 \\ q_{1,0} &= c_1 + c_2 \\ q_{1,1} &= c_1 \,. \end{aligned}$$

Proof. This proof is similar to the proof of lemma 3. Using the definitions of the PR-box (equation 2.5), the $\overline{\text{PR}}$-box (equation 2.6) and the SR-box (equation 2.10), we can compute

$$q_{i,j} = \sum_{\substack{a,b \\ \text{s.t. } a \oplus b = xy}} P(a, b \mid i, j) \tag{4.40}$$

which yields the four values $q_{i,j}$:

$$\begin{aligned} q_{0,0} &= P(0,0 \mid 0,0) + P(1,1 \mid 0,0) && (4.41) \\ &= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right) \\ &= c_1 + c_2 \\ q_{0,1} &= P(0,0 \mid 0,1) + P(1,1 \mid 0,1) && (4.42) \\ &= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right) \\ &= c_1 + c_2 \\ q_{1,0} &= P(0,0 \mid 1,0) + P(1,1 \mid 1,0) && (4.43) \\ &= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_1}{2} + \frac{c_2}{2}\right) \\ &= c_1 + c_2 \\ q_{1,1} &= P(0,1 \mid 1,1) + P(1,0 \mid 1,1) && (4.44) \\ &= \frac{c_1}{2} + \frac{c_1}{2} \\ &= c_1 \,. \end{aligned}$$

□

Similar to theorem 1, we can use these values $q_{i,j}$ to find a condition on nonlocal boxes that make communication complexity trivial with the BBLMTU protocol.

Theorem 2. *Nonlocal boxes producing the correlation described in equation 4.39 violate NTCC if*

$$6c_1^2 + \frac{9}{2}(2c_1 - 1)\, c_2 + \frac{15}{4}c_2^2 - 6c_1 + \frac{3}{2} > 1\,. \tag{4.45}$$

Proof. Recall the map given by 4.29, which gives μ_k in terms of μ_{k-1} and the values $\eta_{i,j}$. Combining this equation with lemma 4, we get the recursion relation for the success bias of the kth round in the BBLMTU protocol:

$$\begin{aligned}\mu_k =& \mu_{k-1}\left(6c_1^2 + \frac{9}{2}(2c_1 - 1)\, c_2 + \frac{15}{4}c_2^2 - 6c_1 + \frac{3}{2}\right) \\ &- \mu_{k-1}^3\left(2c_1^2 + \frac{3}{2}(2c_1 - 1)c_2 - \frac{3}{4}c_2^2 - 2c_1 + \frac{1}{2}\right)\,.\end{aligned} \tag{4.46}$$

This map has a fixed point at $\mu_{k-1} = 0$ and it is unstable when

$$\left.\frac{\mathrm{d}\mu_k}{\mathrm{d}\mu_{k-1}}\right|_{\mu_{k-1}=0} > 1\,. \tag{4.47}$$

which happens when

$$6c_1^2 + \frac{9}{2}(2c_1 - 1)\, c_2 + \frac{15}{4}c_2^2 - 6c_1 + \frac{3}{2} > 1\,. \tag{4.48}$$

Therefore, when this condition is fulfilled, a success bias greater than 0 will approach a constant greater than 0 with each layer of concatenation of the repetition code in the BBLMTU protocol. □

The condition 4.45 can be written in terms of p_{CHSH} and $p_{\mathrm{CHSH}'}$. Using equations 4.33 and 4.34, we get

$$6p_{\mathrm{CHSH}}^2 + 6p_{\mathrm{CHSH}'}^2 - 6p_{\mathrm{CHSH}} - 6p_{\mathrm{CHSH}'} + 3 > 1\,. \tag{4.49}$$

The nonlocal boxes described by equation 4.39 that make communication complexity trivial with the BBLMTU protocol are indicated in figure 4.2.

4.3.1 Notable cases

The case $c_2 = 0$ is the case of isotropic nonlocal boxes. Here again, like for theorem 1, we recover the bound from [BBL+06] since the condition 4.45 with $c_2 = 0$

is respected when one of the following conditions are met

$$c_1 > \frac{3+\sqrt{6}}{6} \tag{4.50}$$

$$c_1 < \frac{3-\sqrt{6}}{6}\,. \tag{4.51}$$

The case $c_1 + c_2 = 1$ is the case of correlated nonlocal boxes. Indeed, a nonlocal box described by equation 4.39 with $c_1 + c_2 = 1$ is a c_1-corNLB. From [BS09], c_1-corNLBs are known to violate NTCC when $c_1 > 0$. Theorem 2 shows that the BBLMTU protocol proves a weaker bound, since equation 4.45 leads to the threshold on c_1-corNLBs:

$$c_1 > \sqrt{\frac{1}{3}}\,. \tag{4.52}$$

In the next section, we give a new proof that c_1-corNLBs are known to violate NTCC when $c_1 > 0$.

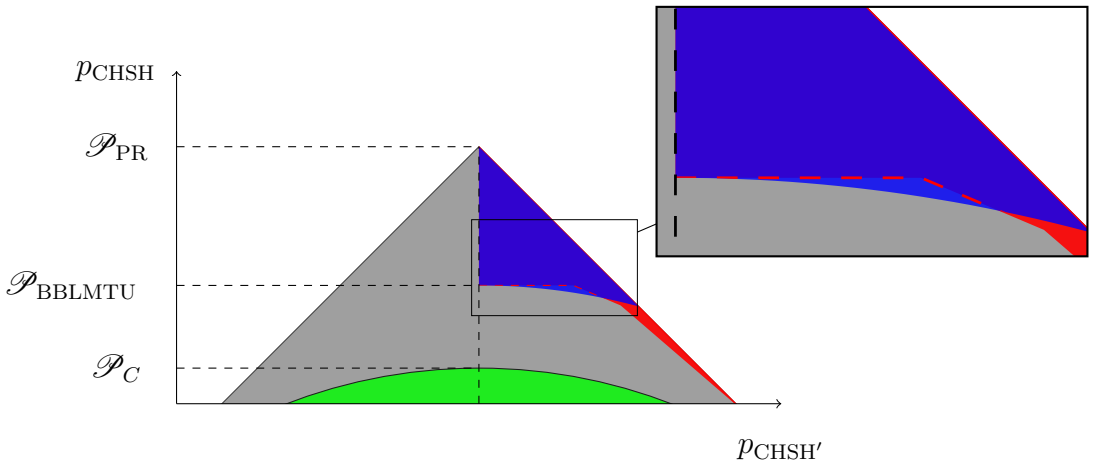


Figure 4.2: Generalized correlated boxes that violate NTCC, projected onto the CHSH-CHSH′ slice. The red region is the one presented in figure 3.3 and comes from [BS09]. The blue region is our contribution, the generalized correlated boxes that make communication complexity trivial with the BBLMTU protocol. The dashed red line indicates the boundary of the red region to show how we expanded the set.

4.4 NTCC violation with p-corNLB if $p > 0$

It is known that p-corNLBs can be distilled arbitrarily close to PR-boxes when $p > 0$, meaning that they make communication complexity trivial [BS09]. However, it is also known that isotropic nonlocal boxes cannot be distilled [BG15]. This means that any proof of trivial communication complexity based on nonlocal box distillation cannot apply to isotropic nonlocal boxes. We give a new proof that correlated nonlocal boxes violate NTCC by giving a protocol that achieves trivial communication complexity using correlated nonlocal boxes. Because our protocol does not use distillation, it provides additional tools for the study of the consequences of super-quantum correlations on NTCC and there is hope that it could be adapted to work with isotropic nonlocal boxes.

Our protocol provides a method to distributively compute any value $f(x, y)$ with $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with a constant probability and without communication. It is based on the PPKSWZ protocol, presented in section 3.4.2 and takes advantage of the fact that a c_1-corNLB computes the multiplication ij with probability $q_{i,j}$:

$$\begin{aligned} q_{0,0} &= 1 \\ q_{0,1} &= 1 \\ q_{1,0} &= 1 \\ q_{1,1} &= c_1 \,. \end{aligned}$$

We call this new protocol the *biased* PPKSWZ protocol since it is the PPKSWZ protocol modified such that at most one of the multiplications can have the value 1.

The biased PPKSWZ protocol. In this protocol, Alice computes the 2^n values $f(x, k)$ for $k \in \{0,1\}^n$, corresponding to the value of the function for each possible input for Bob. Noting $\tilde{k} = \sum_{i=0}^{n-1} k_i 2^i$ the decimal representation of the binary string k, Alice stores the values $f(x, k)$ in bits $x'_{\tilde{k}}$ such that $x'_{\tilde{k}} = f(x, k)$. Define $y'_{\tilde{k}}$ such that

$$y'_{\tilde{k}} = \begin{cases} 1 & \text{if } k = y \\ 0 & \text{otherwise.} \end{cases} \tag{4.53}$$

Note that there is exactly one value $\tilde{k}$ for which $y'_{\tilde{k}} = 1$. Alice and Bob distributively compute Z_1 such that

$$Z_1 = \mathrm{Addr}_1\left(x'_0, x'_1, y'_1\right) = x'_0 \oplus y'_1 \left(x'_0 \oplus x'_1\right) \tag{4.54}$$

using the protocol described in section 3.4.1 to distributively compute the address function on distributed inputs. Then, for $i \in \{1, ..., 2^n\}$, they distributively compute

$$\begin{aligned} Z_i &= \mathrm{Addr}_1\left(Z_{i-1}, x'_i, y'_i\right) \\ &= Z_{i-1} \oplus y'_i \left(Z_{i-1} \oplus x'_i\right) . \end{aligned} \tag{4.55}$$

This is illustrated in figure 4.3. Each multiplication requires one nonlocal box. If an even number of nonlocal boxes fail to correctly compute a multiplication, then Z_{2^n} is a distributed bit equal to $f(x, y)$.

To study the success probability of this protocol, we denote $Z_i^{(A)}$ and $Z_i^{(B)}$ Alice's and Bob's bit such that

$$Z_i^{(A)} \oplus Z_i^{(B)} = Z_i \tag{4.56}$$

$$= \mathrm{Addr}_1\left(Z_{i-1}, x'_i, y'_i\right) . \tag{4.57}$$

For $i > 1$, they use a nonlocal box with inputs $\left(Z_{i-1}^{(A)} \oplus x'_i\right)$ and y'_i. We denote the outputs a_i and b_i. Then, $Z_i^{(A)}$ and $Z_i^{(B)}$ are computed as follows:

$$Z_i^{(A)} = Z_{i-1}^{(A)} \oplus a_i \tag{4.58}$$

$$Z_i^{(B)} = Z_{i-1}^{(B)} \oplus b_i \oplus y'_i Z_{i-1}^{(B)} . \tag{4.59}$$

For the values i such that $y'_i = 0$, the computation of $Z_i^{(A)}$ and $Z_i^{(B)}$ is done without error since correlated nonlocal boxes always correctly compute multiplications when at least one input is 0. For the value i that corresponds to y ($i = \sum_{j=0}^{n-1} y_j 2^j$), we have $y'_i = 1$. Then if $Z_{i-1}^{(A)} = x'_i$, Z_{i-1} is correctly computed since one input to the nonlocal box is 0. However, if $Z_{i-1}^{(A)} \neq x'_i$, then the computation is only correct with probability c_1. Also, since $Z_{i-1}^{(A)} = Z_{i-2}^{(A)} \oplus a_{i-1}$, it is uniformly random and $Z_{i-1}^{(A)}$ is equal to x'_i with probability $1/2$. Therefore, when $y'_i = 1$, Z_i is correctly computed with probability $\frac{1}{2} + \frac{c_1}{2}$.

However, if $i = 1$ is the value that corresponds to Bob's input y (meaning that $y'_1 = 1$), then Bob's input for the nonlocal box is $y'_1 = 1$ and Alice's input is $x'_0 \oplus x'_1$, which is not uniformly random for a given function f. To avoid a situation where the computation of this multiplication has a success probability less than $\frac{1}{2} + \frac{c_1}{2}$, they can replace the value x'_0 by the distributed bit $Z_0 = Z_0^{(A)} \oplus Z_0^{(B)}$, with

$$Z_0^{(A)} = x'_0 \oplus r \tag{4.60}$$

$$Z_0^{(B)} = r , \tag{4.61}$$

where r is a shared random bit. With this trick, the success probability of the computation of the multiplication for the value i that corresponds to Bob's input y is $\frac{1}{2} + \frac{c_1}{2}$ even if this i is 1.

Since all the other multiplications are correctly computed, the final success probability of this protocol is $\frac{1}{2} + \frac{c_1}{2}$, which is a constant greater than 1/2 for all $c_1 > 0$, meaning that communication complexity is trivial with c_1-corNLBs when $c_1 > 0$.

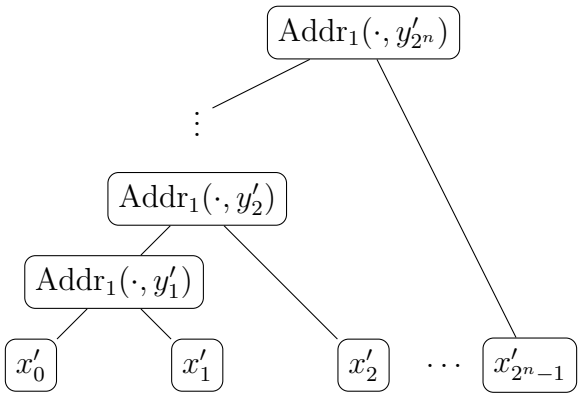


Figure 4.3: In this representation of the biased PPKSWZ protocol, the computation is done from the bottom to the top. The dot $(\cdot)$ in $\mathrm{Addr}_1(\cdot, y'_i)$ represents the two elements directly below, meaning that $\mathrm{Addr}_1(\cdot, y'_i)$ is equal to the element from the left branch if $y'_i = 0$ and to the element from the element from the right branch if $y'_i = 1$. At most one of the y'_is has value 1, the others have value 0.

Chapter 5

Conclusion

5.1 Summary of contributions

Our main contribution is to expand the set of nonlocal correlations that are known to make communication complexity trivial. This is a step forward in the search for intuition in quantum mechanics since it provides an explanation for the impossibility of some stronger-than-quantum correlations. Furthermore, we presented prior results in a unified notation and we provided a framework to study a well-known protocol that we call the BBLMTU protocol [BBL+06] with any nonlocal boxes. Our method can be adapted to other protocols that use error correction techniques by modifying the tensors T and M accordingly (see section 4.1).

Additionally, we have described a protocol that enabled us to give a new proof that all super-quantum correlated nonlocal boxes violate the *non-trivial communication complexity* principle (NTCC). Our proof is different from the existing one [BS09] because it is based on a protocol that does not rely on nonlocal box distillation. Therefore, our protocol is an additional tool to study the consequences of super-quantum correlations.

5.2 Future work

Although we have expanded the set of nonlocal correlations that are known to make communication complexity trivial, it is still unknown what boundaries of the set of quantum correlations can be explained by the NTCC principle. There are multiple avenues that are worth considering to answer this question.

First, the impossibility result by [Mor16] presented in section 3.4 only applies for decoding functions that amplify an arbitrarily small bias. By using a protocol different from BBLMTU, it could be possible to perform error correction at different stages of the computation in such a way that the bias that needs to be amplified would not be arbitrarily small. The conditions on the decoding function would then be different and the impossibility result would no longer be applicable.

Second, one could consider a different encoding for error correction, other than the repetition code. It is possible to choose an encoding such that errors are not independent and are less likely to happen in multiple places at once, making the majority decoding more effective. This might yield a threshold on isotropic nonlocal boxes different from the one in [BBL+06], $\mathscr{P}_{\text{BBLMTU}} = \frac{3+\sqrt{6}}{6}$.

Third, one could hope to find an information theoretic proof similar to what is done in [EP98], where an upper bound on a threshold in a seemingly unrelated context is shown, surprisingly, to be equal to $\mathscr{P}_Q = \frac{2+\sqrt{2}}{4}$. This threshold is not related to communication complexity but some ideas behind the proof might be applicable to our problem.

The above questions were the starting point of our work. Although they remain open at this point, these questions are what led us to the results presented in chapter 4. This is, of course, not an exhaustive list as there exist many more approaches to this problem. It would also be interesting to use our method to find bounds from the BBLMTU protocol for other nonlocal boxes than the ones we have considered, in order to find the whole set of non-signaling correlations that make communication complexity trivial with the BBLMTU protocol.

Appendix A

The CHSH and CHSH′ probabilities for nonlocal boxes in the CHSH-CHSH′ subspace

A general nonlocal box in the CHSH-CHSH′ subspace can be described as a linear combination of a PR-box, a $\overline{\text{PR}}$-box, a PR′-box and a $\overline{\text{PR}'}$-box:

$$\begin{aligned} P(a,b \mid x,y) =& \alpha P_{\text{PR}}(a,b \mid x,y) + \beta P_{\overline{\text{PR}}}(a,b \mid x,y) \\ &+ \gamma P_{\text{PR}'}(a,b \mid x,y) + \delta P_{\overline{\text{PR}'}}(a,b \mid x,y) \end{aligned} \tag{A.1}$$

with $\alpha, \beta, \gamma, \delta \in [0,1]$ and $\alpha + \beta + \gamma + \delta = 1$. The choice of parameters α, β, γ and δ may not be unique to specify a nonlocal box. In fact, a nonlocal box in the CHSH-CHSH′ subspace can be specified using only two parameters. We choose p_{CHSH} and $p_{\text{CHSH}'}$, the winning probabilities for these boxes at the CHSH and the CHSH′ games. These two parameters can be written in terms of α, β, γ and δ.

Lemma 5. *A nonlocal box producing the correlation*

$$\begin{aligned} P(a,b \mid x,y) =& \alpha P_{PR}(a,b \mid x,y) + \beta P_{\overline{PR}}(a,b \mid x,y) \\ &+ \gamma P_{PR'}(a,b \mid x,y) + \delta P_{\overline{PR'}}(a,b \mid x,y) \end{aligned} \tag{A.2}$$

wins the CHSH game with probability $p_{CHSH} = \alpha + \frac{\gamma+\delta}{2}$.

Proof. The winning probability for this correlation is given by the sum of the probabilities of outputs that respect the CHSH condition $a \oplus b = xy$, weighted by the

probability of each pair of inputs (x, y):

$$p_{\text{CHSH}} = \frac{1}{4} \sum_{\substack{a,b,x,y \\ \text{s.t. } a\oplus b=xy}} P(a, b \mid x, y) \tag{A.3}$$

where the factor $1/4$ is the probability of each input pair. This sum can be written explicitly:

$$\begin{aligned} p_{\text{CHSH}} =& \frac{1}{4}P(0,0 \mid 0,0) + \frac{1}{4}P(1,1 \mid 0,0) + \frac{1}{4}P(0,0 \mid 0,1) + \frac{1}{4}P(1,1 \mid 0,1) \\ &+ \frac{1}{4}P(0,0 \mid 1,0) + \frac{1}{4}P(1,1 \mid 1,0) + \frac{1}{4}P(0,1 \mid 1,1) + \frac{1}{4}P(1,0 \mid 1,1)\,. \end{aligned} \tag{A.4}$$

Each term can be computed using equation A.1 and the definition of the nonlocal boxes from equations 2.5, 2.6, 2.7 and 2.9. We get

$$\begin{aligned} p_{\text{CHSH}} &= \frac{\alpha+\delta}{8} + \frac{\alpha+\delta}{8} + \frac{\alpha+\gamma}{8} + \frac{\alpha+\gamma}{8} + \frac{\alpha+\gamma}{8} + \frac{\alpha+\gamma}{8} + \frac{\alpha+\delta}{8} + \frac{\alpha+\delta}{8} \\ &= \alpha + \frac{\gamma+\delta}{2}\,. \end{aligned}$$

□

Lemma 6. *A nonlocal box producing the correlation*

$$\begin{aligned} P(a, b \mid x, y) =& \alpha P_{PR}(a, b \mid x, y) + \beta P_{\overline{PR}}(a, b \mid x, y) \\ &+ \gamma P_{PR'}(a, b \mid x, y) + \delta P_{\overline{PR'}}(a, b \mid x, y) \end{aligned} \tag{A.5}$$

wins the CHSH′ game with probability $p_{CHSH'} = \gamma + \frac{\alpha+\beta}{2}$.

Proof. The proof is very similar to the proof of Lemma 5. The CHSH condition is replaced with the CHSH′ condition $a \oplus b = (x \oplus 1)(y \oplus 1)$:

$$p_{\text{CHSH}'} = \frac{1}{4} \sum_{\substack{a,b,x,y \\ \text{s.t. } a\oplus b=(x\oplus 1)(y\oplus 1)}} P(a, b \mid x, y)\,. \tag{A.6}$$

This sum can be written explicitly:

$$\begin{aligned} p_{\text{CHSH}'} =& \frac{1}{4}P(0,1 \mid 0,0) + \frac{1}{4}P(1,0 \mid 0,0) + \frac{1}{4}P(0,0 \mid 0,1) + \frac{1}{4}P(1,1 \mid 0,1) \\ &+ \frac{1}{4}P(0,0 \mid 1,0) + \frac{1}{4}P(1,1 \mid 1,0) + \frac{1}{4}P(0,0 \mid 1,1) + \frac{1}{4}P(1,1 \mid 1,1)\,. \end{aligned} \tag{A.7}$$

Each term can be computed using equation A.1 and the definition of the nonlocal boxes from equations 2.5, 2.6, 2.7 and 2.9. We get

$$\begin{aligned} p_{\text{CHSH}'} &= \frac{\gamma+\beta}{8} + \frac{\gamma+\beta}{8} + \frac{\gamma+\alpha}{8} + \frac{\gamma+\alpha}{8} + \frac{\gamma+\alpha}{8} + \frac{\gamma+\alpha}{8} + \frac{\gamma+\beta}{8} + \frac{\gamma+\beta}{8} \\ &= \gamma + \frac{\alpha+\beta}{2}\,. \end{aligned}$$

□

Appendix B

Bias of the combination of processes when errors cancel in pairs

For completeness, we present a proof for a well-known simplification that is used throughout this thesis and in [Mor16]. Consider a protocol combining N bits that come from processes with independent success bias β in such a way that errors cancel in pairs. The success probability of this protocol is the probability that an even number of errors occur in these N processes. This probability is given by

$$P = \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{2i} \left(\frac{1+\beta}{2}\right)^{N-2i} \left(\frac{1-\beta}{2}\right)^{2i} .$$

Lemma 7 gives a simplification for this expression.

Lemma 7. *The probability given by*

$$P = \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{2i} \left(\frac{1+\beta}{2}\right)^{N-2i} \left(\frac{1-\beta}{2}\right)^{2i} \tag{B.1}$$

can be simplified to

$$P = \frac{1+\beta^N}{2} . \tag{B.2}$$

Proof. From the well-known Binomial Theorem (see [AS72]), we know that, for $a, b \in \mathbb{R}$ and $N \in \mathbb{N}$,

$$(a+b)^N = \sum_{i=0}^{N} \binom{N}{i} a^{N-i} b^i \,. \tag{B.3}$$

By making the change of variables $b' := -b$, we see that the terms where i is odd gain a minus sign:

$$(a+b')^N = \sum_{i=0}^{N} \binom{N}{2i} a^{N-i} b'^i \tag{B.4}$$

$$(a-b)^N = \sum_{i=0}^{N} \binom{N}{2i} a^{N-i} (-b)^i \tag{B.5}$$

$$= \sum_{i=0}^{N} \binom{N}{2i} (-1)^i a^{N-i} b^i \,. \tag{B.6}$$

Thus, we have that

$$\begin{aligned} \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{2i} a^{N-2i} b^{2i} &= \sum_{\substack{i=0 \\ i \text{ even}}}^{N} \binom{N}{i} a^{N-i} b^i \\ &= \frac{1}{2} \sum_{i=0}^{N} \left(\binom{N}{i} a^{N-i} b^i + \binom{N}{2i} (-1)^i a^{N-i} b^i \right) \\ &= \frac{1}{2} \left((a+b)^N + (a-b)^N \right) \end{aligned} \tag{B.7}$$

where the last equality comes from equations B.3 and B.5.

Let $a = \frac{1+\beta}{2}$ and $b = \frac{1-\beta}{2}$, then we see from equation B.7 that equation B.1 becomes

$$\begin{aligned} P &= \sum_{i=0}^{\lfloor \frac{N}{2} \rfloor} \binom{N}{2i} \left(\frac{1+\beta}{2} \right)^{N-2i} \left(\frac{1-\beta}{2} \right)^{2i} \\ &= \frac{1}{2} \left(1^N + \beta^N \right) \\ &= \frac{1+\beta^N}{2} \,. \end{aligned} \tag{B.8}$$

□

Bibliography

[AGG82] A. Aspect, P. Grangier, and R. Gérard. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment : A new violation of Bell's inequalities. *Physical Review Letters*, 49(2): 91–94, 1982. DOI: 10.1103/PhysRevLett.49.91.

[AS72] M. Abramowitz and I. A. Stegun. Elementary analytical methods. In *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, page 10. Dover Publications, Inc, 1972.

[BBL+06] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96(25): 250401, 2006. DOI: 10.1103/PhysRevLett.96.250401.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2): 419–478, 2014. DOI: 10.1103/RevModPhys.86.419.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics 1*, pages 195–200, 1964. Online: http://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf.

[BG15] S. Beigi and A. Gohari. A monotone measure for non-local correlations. *IEEE Transactions on Information Theory*, 61(9): 5185–5208, 2015. DOI: 10.1109/TIT.2015.2452253.

[BLM+05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Nonlocal correlations as an information-theoretic resource. *Physical Review A*, 71(2): 022101, 2005. DOI: 10.1103/PhysRevA.71.022101.

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

[Bra11] C. Branciard. Detection loophole in Bell experiments: How postselection modifies the requirements to observe nonlocality. *Physical Review A*, 83(3): 032123, 2011.
DOI: 10.1103/PhysRevA.83.032123.

[Bro16] A. Broadbent. Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation. *Physical Review A*, 94(2): 022318, 2016.
DOI: 10.1103/PhysRevA.94.022318.

[BS09] N. Brunner and P. Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Physical Review Letters*, 102(16): 160403, 2009.
DOI: 10.1103/PhysRevLett.102.160403.

[CHSH69] J. F. Clauser, M. A. Horne., A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15): 880–884, 1969.
DOI: 10.1103/PhysRevLett.23.880.

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

[CvDNT13] R. Cleve, W. van Dam, M. Nielson, and A. 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.

[EP98] W. Evans and N. Pippenger. On the maximum tolerable noise for reliable computation by formulas. *IEEE Transactions on Information Theory*, 44(3): 1299–1305, 1998.
DOI: 10.1109/18.669417.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*

Letters, 47(10): 777–780, 1935.
DOI: 10.1103/physrev.47.777.

[FC72] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28(14): 938–941, 1972.
DOI: 10.1103/PhysRevLett.28.938.

[FWW09] M. Forster, S. Winkler, and S. Wolf. Distilling nonlocality. *Physical Review Letters*, 102(12): 120401, 2009.
DOI: 10.1103/PhysRevLett.102.120401.

[GKW+18] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani. Geometry of the set of quantum correlations. *Physical Review A*, 97(2): 022104, 2018.
DOI: 10.1103/PhysRevA.97.022104.

[GWAN11] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués. Quantum correlations require multipartite information principles. *Physical Review Letters*, 107(21): 210403, 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: 682–686, 2015.
DOI: 10.1038/nature15759.

[LHBR10] Y.-C. Liang, N. Harrigan, S. D. Bartlett, and T. Rudolph. Nonclassical correlations from randomly chosen local measurements. *Physical Review Letters*, 104(5): 050401, 2010.
DOI: 10.1103/PhysRevLett.104.050401.

[LPSW07] N. Linden, S. Popescu, A. J. Short, and A. Winter. Quantum nonlocality and beyond: Limits from nonlocal computation. *Physical Review Letters*, 99(18): 180502, 2007.
DOI: 10.1103/PhysRevLett.99.180502.

[MAG06] L. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A*, 73(1): 012112, 2006.
DOI: 10.1103/PhysRevA.73.012112.

[MMM+08] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe. Bell inequality violation with two remote atomic qubits. *Physical Review Letters*, 100(15): 150404, 2008.
DOI: 10.1103/PhysRevLett.100.150404.

[Mor16] R. Mori. Three-input majority function as the unique optimal function for the bias amplification using nonlocal boxes. *Physical Review A*, 94(5): 052130, 2016.
DOI: 10.1103/PhysRevA.94.052130.

[NW09] M. Navascués and H. Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 2009.
DOI: 10.1098/rspa.2009.0453.

[Orú14] R. Orús. A practical introduction to tensor networks: Matrix product states and projected entangled pair states. *Annals of Physics*, 349: 117–158, 2014.
DOI: 10.1016/j.aop.2014.06.013.

[Pop14] S. Popescu. Nonlocality beyond quantum mechanics. *Nature Physics*, 10: 264–270, 2014.
DOI: 10.1038/NPHYS2916.

[PPK+09] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nature*, 461(7267): 1101–1104, 2009.
DOI: 10.1038/nature08400.

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

[SMSC+15] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma,

C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong loophole-free test of local realism. *Physical Review Letters*, 115(25): 250402, 2015.
DOI: 10.1103/PhysRevLett.115.250402.

[Str18] S. H. Strogatz. One-dimensional maps. In *Nonlinear Dynamics and Chaos*, pages 355–404. CRC press, 2018.

[SUK+10] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger. Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences*, 107(46): 19708–19713, 2010.
DOI: 10.1073/pnas.1002780107.

[vD13] W. van Dam. Implausible consequences of superstrong nonlocality. *Natural Computing*, 12(1): 9–12, 2013.
DOI: 10.1007/s11047-012-9353-6.

[vN56] J. von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. In *Automata Studies*, pages 43–98. Princeton University Press, 1956.