Bounds on quantum nonlocality

PhD Thesis

Gláucia Murta Guimarães

Tese apresentada ao Programa de Pós-Graduação em Física da Universidade Federal de Minas Gerais, como requisito parcial para a obtenção do título de Doutora em Física.

February 2016

"Que beleza é conhecer o desencanto
e ver tudo bem mais claro no escuro"

— Tim Maia

Acknowledgements

Em um país onde educação superior é um provilégio para poucos, começo agradecendo aos meus pais, Nilma e Francisco, que sempre se empenharam em encontrar os meios para garantir que eu tivesse todas as oportunidades para chegar até aqui.

Secondly, I thank my supervisor Marcelo Terra Cunha for almost 6 years of supervision. I am grateful for all the stimulating discussions we had during this time and for all you taught me about research and life. For your guidance through my first research steps, for encouragement during important decisions and for always being ready to support me in the difficult (academic and personal) moments[1].

Many thanks to Fernando Brandão (again) for the first course in quantum information, and for playing a fundamental rule in the international opportunities that I had during the PhD.

I am grateful to Michał Horodecki for receiving me for a one-year 'sandwich' PhD in KCIK. This time was extremely valuable for my development as a researcher and crucial for many of the results presented in this thesis.

From the great researchers I interacted with during my PhD I would like to specially thank: Daniel Cavalcanti, for being a role model since my Master's; Adán Cabello, for participating in my first steps in science and for all enthusiastic discussions; Marcin Pawłowski, for always transmitting such a great excitement about science, for great trip adventures and funny discussions, and for the opportunity to come back to KCIK for a few more months[2]; Karol Horodecki, for a really nice collaboration from which I learned a lot; and Paweł Horodecki, for many enlightening discussions.

A lot of the work presented in this thesis would not have been possible if it was not for the careful guidance of Ravishankar Ramanathan. I am grateful for all I have learned from you during this time. Much of the researcher I became

[1] E claro, pelos açaís, pelos cafés, e por me apresentar várias músicas que hoje são parte da minha trilha sonora favorita.

[2] And of course, for making me watch the Indiana Jones trilogy with Polish dubs and English subtitles.

was shaped by our collaboration.

Dziękuję bardzo to all the people from KCIK for such nice atmosphere at work. In special I thank all the inhabitants of room 'sto dwa' for all the physics and specially the non-physics discussions. Pankaj Joshi, thanks for all the "sweet food" you made me try, and Paweł Mazurek, thanks for the dance! And to Ania and Czarek, thanks for making me feel home 10.000 km away. This year in Poland was an amazing time from which I carry many good memories.

A todos os integrantes do Departamento de Física da UFMG, muito obrigada por serem minha segunda casa nos últimos 10 anos. À PG Física por todo apoio administrativo e acadêmico. À Shirley por estar sempre pronta para nos assistir e por tornar a Biblioteca do Departamento de Física um lugar de apoio para a pesquisa e ensino realizados no departamento.

Às mulheres do departamento de Física, obrigada por serem exemplo e inspiração.

Agradeço aos integrantes do corredor do doutorado e aos vizinhos da astrofísica pela ótima convivência, e em especial aos que contribuíram para que as edições do 'Bar da Gláucia' fossem um sucesso! Aos meus colegas de Sala, Mangos, Mychel e Rapaiz, muito obrigada pela melhor sala de todas (e me desculpem por todas as vezes que troquei vocês pelo ar condicionado). Em especial agradeço ao Mangos, pelo ombro amigo em muitos momentos difíceis.

Aos Terráqueos contemporâneos: Bárbara Amaral[3], Cristhiano Duarte[4], Natália Móller[5], Leonardo Guerini[6], Gabriel Fagundes[7], Marcello Nery[8], Jessica Bavaresco[9], Tassius Maciel[10] e José Roberto Pereira Júnior[11], e os contemporâneos de mestrado Mateus Araújo[12] e Marco Túlio Quintino[13], muito obrigada por fazerem parte dessa etapa. E por compartilharem tantas discussões, almoços, dúvidas, festas, reuniões, cafés, Paratys ...

Aos membros do EnLight, professores, pós-docs e alunos, muito obrigada por todo o conhecimento compartilhado durante esses anos. Em especial, agradeço ao Carlos Parra por me lembrar ocasionalmente, durante a escrita desta Tese, de manter minha sanidade mental. E ao Pierre-Louis de Assis, por oca-

[3]Exemplo de irmã mais velha.

[4]Certamente contribuiu para me tornar uma pessoa menos pura. Que horror!

[5]Fico feliz de você ser minha primeira co-autora!

[6]Léo, valeu por todas as nossas conversas não-locais sobre a vida :)

[7]Gabriel! Nunca dá pra trás num evento, e ainda traz a caixa de som.

[8]Marcellooow, ainda tô esperando você se redimir por não ir na(s) minha(s) festa(s).

[9]Viu, obrigada pela amizade, pelas saídas em BH e pela super força na reta final!

[10]Fonte das histórias mais trolls que eu já ouvi.

[11]Grande filósofo.

[12]Mateus! É sempre muito massa discutir com você!

[13]Mais importante que todas as nossas conversar de física, obrigada por sempre tomar conta de mim :)

sionalmente[14] me fazer perdê-la com suas interrupções inconvenientes (das quais já sinto saudades). Ao Dudu (Eduardo Mascarenhas), obrigada por cuidar de mim nos momentos difíceis e por ser um exemplo como pesquisador.

I thank Marcus Huber, Fabien Clivaz, and Atul Mantri for the very nice collaborations initiated during my PhD, from which I certainly profit a lot.

I am grateful to all the quantum friends I have made during this time. It is always pleasant to meet you somewhere in the world. In special I thank Alexia Salavrakos, Joe Bowles, and Flavien Hirsch for so many special moments.

À minha irmã Bizy, agradeço por sempre me apoiar. Por ser exemplo e inspiração. E por me alimentar durante a escrita desta Tese.

This Thesis was significantly improved due to the careful reading of my supervisor Marcelo Terra Cunha and Jessica Bavaresco. I also thank Mateus Araújo, Marco Túlio Quintino, and Hakob Avetisyan for comments and feedback in earlier versions. I thank the referees of this Thesis: Daniel Cavalcanti, Reinaldo Oliveira Vianna, Fernando de Melo, Raphael Campos Drumond, and Andreas Winter for very nice discussions and feedbacks. I owe a special thanks to Jessica Bavaresco and Thiago Maciel[15] for the technical support, making it possible to have an international committee in my PhD defense.

Finally, I acknowledge CNPq for my first year scholarship and I am greatful to Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) for the remaining three years of scholarship, for the sandwich PhD program which opened so many doors for me, and for financial support to many conferences. I also acknowledge support from NCN grant 2013/08/M/ST2/00626, Polish MNiSW Ideas-Plus Grant IdP2011000361, ERC Advanced Grant QOLAPS and National Science Centre project Maestro DEC- 2011/02/A/ST2/00305.

[14] Na verdade, frequentemente.

[15] Tchê, obrigada também por sempre estar disponível para tirar minhas dúvidas numéricas (e foram inúmeras) ao longo desses anos.

Resumo

Não-localidade é um dos aspectos mais intrigantes da teoria quântica, que revela que a natureza é intrinsecamente diferente da nossa visão clássica do mundo. Um dos principais objetivos no estudo de não-localidade é determinar a máxima violação obtida por correlações quânticas em um cenário de Bell. Entretanto, dada uma desigualdade de Bell, nenhum algoritmo geral é conhecido para calcular esse máximo. Como um passo intermediário, o desenvolvimento de cotas eficientemente computáveis para o valor quântico de desigualdades de Bell tem tido um papel importante para o desenvolvimento da área. Nessa tese, apresentamos nossas contribuições explorando cotas eficientemente computáveis, baseada na norma de certas matrizes, para o valor quântico de uma classe particular de desigualdades de Bell: os jogos lineares. Na primeira parte introduzimos os pré-requisitos necessários para os resultados principais: Conceitos e resultados das teorias de otimização e complexidade de computação, com foco em problemas de não-localidade; O formalismo de jogos não-locais como um caso particular de desigualdades de Bell; E a abordagem de grafos para não-localidade. Na segunda parte apresentamos nossos resultados principais sobre a caracterização de condições necessárias e suficientes para um jogo XOR não ter vantagem quântica, e provamos uma cota eficientemente computável para o valor quântico de jogos lineares. Os principais resultados apresentados aqui são: (i) Determinação da capacidade de Shannon para uma nova família de grafos; (ii) Generalização, para funções com d possíveis valores, do princípio de não-vantagem em computação não-local; (iii) Um método sistemático de gerar testemunha de emaranhamento genuíno independente de dispositivo para sistemas tripartidos.

Abstract

Nonlocality is one of the most intriguing aspects of quantum theory which reveals that nature is intrinsically different than our classical view of the world. One of the main goals in the study of quantum nonlocality is to determine the maximum violation achieved by quantum correlations in a Bell scenario. However, given a Bell inequality, there is no general algorithm to perform this task. As an intermediate step, the development of efficiently computable bounds has played an important role for the advance of the field. In this thesis we present our contributions exploring efficiently computable bounds, based on a norm of some matrices, to the quantum value of a particular class o Bell inequalities: the linear games. In the first part of the thesis we introduce the necessary background to follow the main results: Concepts and results of optimization and computational complexity theories, focusing on nonlocality problems; The framework of nonlocal games as a particular class of Bell inequalities; And the graph-theoretic approach to nonlocality. In the second part we present our main results concerning the characterization of necessary and sufficient conditions for an XOR game to have no quantum advantage, and we prove an efficiently computable upper bound to the quantum value of linear games. The main outcomes of the research presented in this thesis are: (i) The determination of the Shannon capacity for a new family of graphs; (ii) A larger alphabet generalization of the principle of no-advantage for nonlocal computation; (iii) And a systematic way to design device-independent witnesses of genuine multipartite entanglement for tripartite systems.

List of papers

The content of this Thesis is based on results developed in the following papers:

1. *Characterizing the Performance of* XOR *Games and the Shannon Capacity of Graphs*
   R. Ramanathan, A. Kay, **G. Murta** and P. Horodecki
   Phys. Rev. Lett., 113, 240401, (2014).

2. *Generalized* XOR *games with d outcomes and the task of nonlocal computation*
   R. Ramanathan, R. Augusiak, and **G. Murta**
   Phys. Rev. A, 92, 022333 (2016).

3. *Quantum bounds on multiplayer linear games and device-independent witness of genuine tripartite entanglement*
   G. Murta, R. Ramanathan, N. Móller, and M. Terra Cunha
   Phys. Rev. A, 93, 022305, (2016).

The author also contributed to the work:

- *Bounds on quantum nonlocality via partial transposition*
  K. Horodecki and **G. Murta**
  Phys. Rev. A, 92, 010301(R), (2015).

A summary of the results developed in this work is presented in Appendix B.

Contents

Prologue

One of the most intriguing aspects of quantum theory is the fact that it is intrinsically probabilistic. This probabilistic character led Einstein, Podolsky, and Rosen, in the remarkable EPR paper of 1935 [EPR35], to question whether quantum theory was an incomplete theory, and therefore this probabilistic character would emerge from our lack of knowledge of some variables. These questionings were answered in a negative way by Bell in 1964 [Bel64]. With a mathematical formulation of the EPR paradox, Bell showed that if we were able to complete quantum mechanics in the way proposed by EPR then we should not observe some phenomenon (the violation of a Bell inequality) that we actually do! The work of Bell does not imply that quantum theory is the ultimate theory, however no such refinement as the one pursued by EPR can exist.

Even worse than this probabilistic character, what is really intriguing about quantum theory is the fact that, up to the moment, there is no set of physical principles that fully characterizes it. If we consider special relativity, this theory has some surprising predictions that goes against our daily life experiences. However as weird as they seem, all these predictions can be derived from two physical principles: (i) The laws of physics are the same in all inertial reference frames; (ii) The speed of light in vacuum is c in all inertial reference frames. Once we accept these principles (and I do not claim this is an easy task!) there is no mystery, and we are able to explain all the phenomena that arise from the theory.

Quantum theory is very well established by a bunch of mathematical axioms that tells us how to predict the statistics of the results of experiments. However we still do not have many clues on which are the physical principles behind this purely mathematical formulation. In his famous quotation, Feynman (in the prestigious 'Messenger Lectures' at Cornell University [Fey65]) said

> *"There was a time when the newspaper said that only twelve men understood the theory of relativity. I do not believe there ever was such a time. There might have been a time when only one man did, because he was the only guy who caught on, before he wrote his paper. But after people read the paper a lot of people understood the theory of relativity in some way or*

other, certainly more than twelve. On the other hand, I think I can safely say that nobody understands quantum mechanics."

This lack of principles receives a clear formulation in the study of nonlocality. When defining the sets of local and no-signaling correlations, we have clear mathematical constraints that delimit them, and, additionally, these constraints have a physical (information theoretic) interpretation. For example, the no-signaling principle states, in an information theoretic language, that if Alice and Bob do not communicate no information can be obtained about the other party by analyzing only the local statistics. The additional constraints imposed to the set of local correlations also have a physical interpretation. However, when it concerns the set of quantum correlations all that we know is that the probability distributions can be described by positive operator valued measures applied to a trace-one positive operator that acts on a Hilbert space $\mathcal{H}$. Which, definitely, does not sound very physical! And this is why Feynman says that *"nobody understands quantum mechanics"*.

Almost a century has passed since the questionings of EPR and we still do not have a satisfactory description of quantum theory in terms of physical axioms. However, in the mean time we have developed technologies based on quantum effects and explored in many different ways the novelties brought by quantum theory. In the quantum nonlocality domain people found a way to explore Bell inequality violations in order to develop secure cryptographic protocols that do not rely in any assumption about the specific description of the system, but rather only on the statistics of the results of experiments, the called device-independent paradigm. And besides the manipulation of quantum effects, we have also achieved some understanding on the consequences and limitations due to the mathematical formulation of the theory.

So at this point I should apologize and warn the reader that unfortunately the following pages will not make you *understand quantum mechanics*. However, if you keep going you might have a glance on the subject of quantum nonlocality, which highlights one of the weirdest aspects of quantum theory in a very clear and simple scenario: where Alice and Bob, space-like separated, perform local measurements on their systems, and the only thing that matters is the statistics of their inputs and outputs. This simple scenario opens space for a rich discussion of the fundamental aspects of quantum theory. The analysis of the performance of Alice and Bob in some particular tasks when they have access to quantum resources or not gives us a framework to explore the extent and limitations of the theory. This thesis is devoted to the study of the task of evaluating the quantum value of a Bell expression. We will discuss the difficulty of this problem putting it into the language of computational complexity and optimization theories. And we will present our contributions concerning

bounds on the quantum value of a particular class of Bell expressions: the linear games. At the end of the day, I hope the reader *enjoy it*!

Outline[16]

In Part I we introduce the necessary background to follow the results presented here. In Chapter 1 we present a brief introduction to nonlocality stating some concepts and general results. Chapter 2 introduces optimization and computational complexity theories. Chapter 3 presents the framework of nonlocal games, which can be seen as a particular class of Bell expressions, focusing on linear games which are the main subject of study of this thesis. In Chapter 4 we introduce the graph-theoretic approach to nonlocality, showing how some graph invariants are related to the classical, quantum and no-signaling values of Bell expressions.

Part II is devoted to the results developed by the author, together with collaborators, during the last four years.

- In Chapter 5 we focus on XOR games. We present a necessary and sufficient condition for an XOR game to have no quantum advantage and, exploring this result, we are able to determine the Shannon capacity of a broad new family of graphs.
- In Chapter 6 we present an efficiently computable upper bound to the quantum value of linear games. We explore it re-deriving a recently discovered bound to the CHSH-d game. We also show that these bounds can exclude the existence of some no-signaling boxes that would lead to the trivialization of communication complexity. As the main outcome of the introduced bound, we derive a larger alphabet generalization of the principle of no-advantage for nonlocal computation.
- In Chapter 7 we extend the previous bound to n-player linear games. We also derive an upper bound to the quantum value of a multipartite version of the CHSH-d game and we extend the result concerning no-quantum realization of no-signaling boxes that would lead to the trivialization of communication complexity in a multipartite scenario. Finally, we present a systematic way to derive device-independent witnesses of genuine multipartite entanglement for tripartite systems.

> *"So do not take the lecture too seriously, feeling that you really have to understand in terms of some model what I am going to describe, but just relax and enjoy it."* (Feynman [Fey65])

[16] This Thesis was revised in March/2017 and Journal references were updated.

Part I

Preliminaries

Chapter 1

Nonlocality

Let us analyze the following story:

> *Alice and Bob went abroad for their PhD studies and now they are flatmates. After some months living together Bob noticed a strange behavior of Alice: every time Bob wakes up looking forward to tell Alice the news from his hometown, she coincidently wakes up particularly grumpy, even though in general she is a very easy going and talkative person. When Bob realizes that this grumpy behavior of Alice is recurrent, but only happens in the specific days he has some news to tell, he tries to find out what could be the cause of this strange correlation.*
> *He is sure that this cannot be caused by himself, since they meet every evening when they get back home, and everything is fine before they go to their respective rooms until the next day. Moreover, this situation happens in random days but coincidently every time Bob wants to tell news during the breakfast.*
> *After a long analysis he finally finds out the explanation for this correlation: the phone call to his family the evening before. Every time he made a phone call, the Internet of the house stopped working. And this was happening because their wireless router was settled to the same frequency as the one used by their wireless phone. Alice, on the other hand, checks her computer simulations at home every evening (accessing her working computer remotely). Because the internet fails to work for the hours Bob spend in the phone, she is only able to finish her work very late at night, which causes a big grump!*
> *By adjusting the router's frequency, the problem was solved and Alice and Bob lived happily ever after...*

At first the correlation between Alice and Bob may sound very strange, however when we become aware of the previously "hidden" fact that the frequency of their wireless router was interfering with the frequency of their wireless phone, causing all the trouble, everything looks pretty natural.

That is the idea of a **local hidden variable model**: To find an explanation for correlations in terms of some common cause (the term local will become clear soon). However, as we will see, there exist correlations in nature which cannot be explained by a local hidden variable model, these correlations are then called **nonlocal correlations**. Nonlocal correlations are one of the most intriguing aspects of nature. And besides their foundational interest, these correlations have also shown to be very useful in cryptographic and information processing tasks as, for example, device-independent randomness amplification and expansion [CR12, PAM+10], device-independent quantum key distribution [Eke91, PAB+09, MPA11, VV14], and reduction of communication complexity [vD13, BBL+06, BCMdW10].

In the study of nonlocality we consider the following scenario: Alice and Bob are far away from each other[1] and they are going to observe things that happen around them, *i.e.* they are going to ask questions to their systems (or in a more scientific language, they are going to perform experiments/measurements in their respective laboratories). The set of possible questions that Alice can ask to her system is denoted Q_A and the set of possible questions that Bob can ask is denoted Q_B. The sets of possible answers (outcomes) to these questions[2] are denoted respectively $\mathcal{O}_A$ and $\mathcal{O}_B$. An example of a question that can be asked is *'Is it raining now?'*, which has two possible outcomes: *'yes'* or *'no'*. They can also throw a dice and observe the upper face, which has six possible outcomes: 1, 2, 3, 4, 5 and 6.

We also consider that Alice and Bob can ask their systems only one question at a time (*i.e.* Alice is not allowed to check if it is raining and throw a dice at the same time[3]). The motivation for this restriction is that, when we consider quantum theory, we might deal with incompatible observables, as for example a measurement of spin in the $\hat{x}$-direction and a measurement of spin in the $\hat{z}$-direction, hence we have questions that cannot be asked together.

[1] In technical words, we want Alice and Bob to be space-like separated.

[2] For simplicity, here we focus on the case where each experiment that Alice and Bob perform has the same set of outputs, but this need not to be the case. Nevertheless, most of the results are straightforward generalized to the asymmetric case.

[3] Of course in a classical world there is no restriction in performing this task. One can perfectly go outdoors and trow a dice obtaining at the same time a number and the answer about the weather. However we cannot assert this for a quantum system, and there exist pairs of questions such an experiment to determine the output of one disturbs the output of the other.

Our goal is to analyze the joint probability distribution that Alice performs the experiment $x \in Q_A$ and obtains the outcome $a \in \mathcal{O}_A$ and Bob observes $y \in Q_B$ and obtains the outcome $b \in \mathcal{O}_B$:

$$P(a, b|x, y). \tag{1.1}$$

Since we are only concerned with the statistics of the outputs given the inputs, and nothing else matters for us, we can model any such experiment as a black box (see Figure 1.1): which has some buttons as inputs (the possible questions) and a set of light bulbs as outputs (the possible answers to the question). This is called a **device-independent** scenario, where we do not make any assumption over the internal mechanisms of the devices used for the experiment.

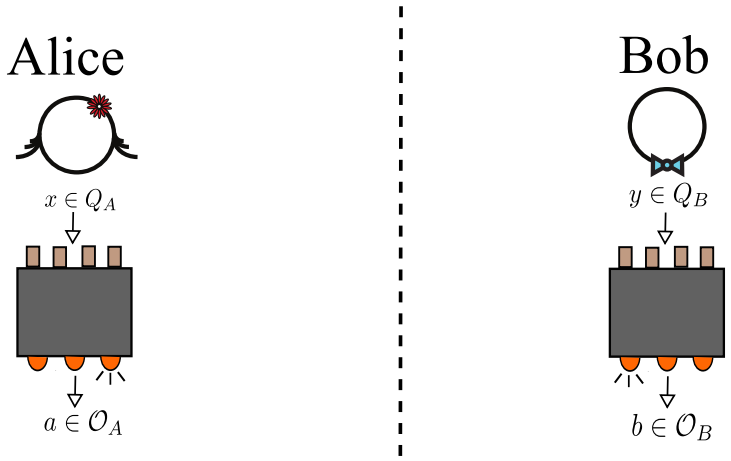


Figure 1.1: **Nonlocality scenario:** Alice and Bob are far apart and they are going to perform experiments on their respective laboratories. Their experiments can be described as black boxes: the upper buttons are the possible inputs and the lower light bulbs are the possible outputs.

A **box** $\vec{P}(a, b|x, y)$ is a vector specifying all the joint probability distributions of a particular scenario[4]. In the following sections we are going to analyze which properties the set of boxes $\vec{P}(a, b|x, y)$ satisfies.

[4]For the particular case where Alice and Bob have two possible inputs with two outputs, $a, b, x, y \in \{0, 1\}$, $\vec{P}(a, b|x, y)$ is the sixteen-component vector:

$$\vec{P}(a, b|x, y) = (P(00|00), P(01|00), P(10|00), P(11|00), P(00|01), \ldots, P(11|11)).$$

In this Chapter we are going to give a brief overview of the concepts and main results in the study of nonlocality. For an introduction to nonlocality, with detailed proofs of many results, the reader is referred to Ref. [Mur12] (only in Portuguese) or Ref. [Qui12]. A nice review, from 2014, contains the references for many important results on the field of nonlocality [BCP+14].

1.1 Local correlations

In the study of nonlocality we are considering a scenario where Alice and Bob are far away from each other during the course of their experiments. We also assume that their choices of which experiment they are going to perform are made when they are already far apart. Our classical intuition leads us to expect that, whichever correlations they observe, they have to be explained by a common cause that does not depend on which experiment they chose to perform (since this choice was made when they were far apart). The boxes that capture this classical intuition are called **local** boxes.

Definition 1.1.1 (Local correlations)**.** *Local correlations are the ones that can be explained by a local hidden variable model, i.e. a box $\vec{P}(a,b|x,y)$ is local if there exists a variable $\lambda \in \Lambda$, independent of the choice of inputs of Alice and Bob, such that*

$$P(a,b|x,y) = \int_{\Lambda} q(\lambda)p(a|x,\lambda)p(b|y,\lambda)d\lambda \tag{1.2}$$

where $q(\lambda)$ is a probability distribution.

The definition of a local box states that all the correlations observed by Alice and Bob in their experiments are due to the lack of knowledge of some hidden variable $\lambda \in \Lambda$. Note that in Definition 1.1.1 we do not make any assumption over the nature of the variable λ, it can be a continuous variable, it can be a set of variables and so on . . . The only assumption is that λ is not correlated with the choices of inputs of Alice and Bob[5] (**measurement independence**). Another important assumption in Definition 1.1.1 is that, conditioning on all variables that could have a causal relation with a particular event, the probability of this event is independent of any other variable. This is often refereed to as **local causality**. Therefore for each value of λ the local probability distribution on Alice's outcome is independent of Bob's experiment, *i.e.* $p(a|b,x,y,\lambda) = p(a|x,\lambda)$, and the

[5]This assumption is also referred as **free will**, as, if Alice and Bob can freely make their choices, this assumption will be satisfied. Since here we do not want to make any metaphysical discussion, let us just assume that this independence (between the hidden variable and the choice of inputs) holds, no matter what justifies it.

same holds for Bob's local distribution. This captures the interpretation that the hidden variable λ would be a common cause in the past that is responsible for generating the correlations.

There are other equivalent ways to formulate Definition 1.1.1, see, for example, Ref. [Fin82]. Moreover, Eq. (1.2) can be derived from a slightly different set of assumptions. But it is important to have in mind that there is always a set of assumptions (measurement independence and local causality in the previous discussion) present in the definition of local correlations, and the violation of a Bell inequality do not tell us which particular assumption is being invalidated. For a very nice discussion on the assumptions implicit in the definition of *locality* we refer the reader to Ref. [Ara][6]. Therefore whenever we use the term **nonlocal** in this thesis we refer to the impossibility of writing a joint probability distribution in the form of Eq. (1.2).

Definition 1.1.1 reflects the intuition we learn from our daily life experience and it also expresses the predictions of classical theories (as classical mechanics and special relativity), which were the theories that prevailed before the advent of quantum theory.

The local polytope

The set of all boxes $\vec{P}(a,b|x,y)$ that can be written in the form (1.2) is called the **local set** of correlations, $\mathcal{L}$. For any scenario that we consider, *i.e.* for any finite set of inputs Q_A and Q_B and any finite set of outputs $\mathcal{O}_A$ and $\mathcal{O}_B$, the local set is a **polytope**. A polytope is a convex set with a finite number of extremal points. The extremal points of the local polytope are the deterministic local boxes:

$$P(a,b|x,y) = D(a|x)D(b|y), \tag{1.3}$$

where $\vec{D}(a|x), D(a|x) \in \{0,1\}$, is a deterministic probability distribution, and analogously for $\vec{D}(b|y)$. One can actually derive that every box $\vec{P}(a,b|x,y)$ that satisfies Eq. (1.2) can be written as a convex combination of deterministic probability distributions, Eq. (1.3)[7].

Proposition 1.1.1 (Local polytope)**.** *The local polytope is the convex hull of the deterministic local boxes:*

$$\mathcal{L} := \left\{ \vec{P}(a,b|x,y) \mid P(a,b|x,y) = \sum_i c_i D_i(a|x) D_i(b|y) \right\} \tag{1.4}$$

[6]This nonlocal reference was added in the revised version of the thesis.

[7]For this reason Definition 1.1.1 is also called **local realism** or **local determinism**.

where $c_i \geq 0$, $\sum_i c_i = 1$, *and* i *runs over all possible deterministic boxes of the scenario.*

For a scenario with $|Q_A| = |Q_B| = m$ and $|\mathcal{O}_A| = |\mathcal{O}_B| = d$, the local set is a convex polytope of dimension[8] $m^2(d-1)^2 + 2m(d-1)$ with d^{2m} vertices [Pir04].

A convex polytope is fully characterized by its vertices, but an equivalent characterization is given by its facets[9]. The facets are hyperplanes that delimit the set. The nontrivial facets[10] of the local polytope are called **tight Bell inequalities** [Bel64]. A **Bell inequality** is a condition that is necessarily satisfied by all local correlations. It can be a tight condition and correspond to a facet of the local polytope, or else it may correspond to faces of the local polytope with lower dimension, or may even not touch the polytope.

In the scenario where Alice and Bob each can chose one between two possible inputs $Q_A = Q_B = \{0,1\}$ and each input has two possible outputs $\mathcal{O}_A = \mathcal{O}_B = \{0,1\}$, the local polytope has as its unique nontrivial facet (up to relabeling of inputs and outputs) the notorious CHSH inequality [CHSH69].

Consider the following expression:

$$\mathcal{S}^{CHSH} = \langle A_0, B_0\rangle + \langle A_1, B_0\rangle + \langle A_0, B_1\rangle - \langle A_1, B_1\rangle\,, \tag{1.5}$$

where $\langle A_x, B_y\rangle = P(a = b|x,y) - P(a \neq b|x,y)$. A substitution of Eq. (1.2) into the RHS of Eq. (1.5) shows that

$$\mathcal{S}^{CHSH} \leq 2 \tag{1.6}$$

for any local box.

The CHSH inequality (1.6) is the simplest and most well explored of all the Bell inequalities. It was introduced in 1969 by Clauser, Horne, Shimony and Holt [CHSH69]. After the work of Bell [Bel64], which finally opened the possibility to formalize in a mathematical way the concepts of local realism first discussed by Einstein, Podolsky and Rosen [EPR35], the CHSH inequality was proposed as a condition that could be experimentally tested. Inequality (1.6) was used in the first experiment that closed the locality loophole [ADR82], performed by Aspect's group, and also in the recent groundbreaking loophole-free Bell experiment by Hensen *et al.*[HBD+15]. A variant of the CHSH inequality (the CH-Eberhard inequality[11] [CH74, Ebe93]) was used in the subsequent ex-

[8] The dimension of the polytope is determined by taking into account the normalization of the probability distributions, and the no-signaling condition that we are going to specify soon.

[9] This is the **Main Theorem for polytopes**, see Theorem 1.1 in Ref. [Zie95].

[10] The trivial ones are the positivity condition of the probabilities: $P(a,b|x,y) \geq 0\ \forall\ a,b,x,y$.

[11] The CH-Eberhard inequality is a reformulation of the CHSH inequality which is more suitable for taking into account detection efficiencies.

periments by Giustina *et al.*[GVW+15] and Shalm *et al.*[SMSC+15]. These last three experiments have finally ruled out local realism in nature[12].

1.2 No-signalling correlations

We may be less picky and not seek a local hidden variable model to explain our correlations, but we want to keep some minimal assumptions about the possible boxes: If Alice and Bob are far away from each other and do not communicate during their experiments, it is reasonable to expect that Bob can get no information about what happens in Alice's laboratory and vice-versa. This is the no-signaling principle and the most general boxes we are going to deal with are the ones that at least satisfy this constraint. More formally, the no-signaling principle states that the marginals of the local experiments do not depend on the other part's experiment.

Definition 1.2.1 (No-signaling condition)**.** *A box $\vec{P}(a,b|x,y)$ is no-signaling iff*

$$\sum_b P(a,b|x,y) = \sum_b P(a,b|x,y') \quad \forall\, y,y' \in Q_B\ ,\ \forall x \in Q_A\ ,\ \forall a \in \mathcal{O}_A, \tag{1.7a}$$

$$\sum_a P(a,b|x,y) = \sum_a P(a,b|x',y) \quad \forall\, x,x' \in Q_A\ ,\ \forall y \in Q_B\ ,\ \forall b \in \mathcal{O}_B. \tag{1.7b}$$

Note that the no-signaling condition implies that local marginal probabilities are well defined:

$$P(a|x) := \sum_b P(a,b|x,y) \quad \forall y, \tag{1.8a}$$

$$P(b|y) := \sum_a P(a,b|x,y) \quad \forall x. \tag{1.8b}$$

The boxes that satisfy the no-signaling condition (1.7) form the set of no-signaling correlations $\mathcal{NS}$. $\mathcal{NS}$ is also a convex polytope (as only linear constraints were made to the probability distributions), which contains the classical polytope. This can be easily seen by checking that local boxes (1.2) satisfy the no-signaling condition (1.7), hence

$$\mathcal{L} \subseteq \mathcal{NS}. \tag{1.9}$$

Later we are going to see (Section 1.4) that, in general, this inclusion can be a strict relation.

[12] Up to some stronger loopholes, as the super-determinism, that by definition cannot scientifically be ruled out.

The no-signaling polytope is much easier to characterize than the local polytope since $\mathcal{NS}$ is fully characterized by Eqs. (1.7) (and by the trivial conditions of positivity and normalization of the probability distributions) which are linear constraints that can be easily checked. Although $\mathcal{L}$ is also delimited by linear constraints, the tight Bell inequalities are not easy to derive and we are left with a description in terms of the deterministic points, which is an integer quadratic problem (see Section 2.2).

1.3 Quantum correlations

Quantum correlations are boxes $\vec{P}(a,b|x,y)$ that can be described as quantum local measurements being performed in a shared quantum state (see Appendix A for an overview of concepts and definitions in quantum theory).

Definition 1.3.1 (Quantum correlation)**.** *A box $\vec{P}(a,b|x,y)$ is quantum if there exist a quantum state $\rho \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ and local POVMs $\{M_x^a\}_a$ and $\{M_y^b\}_b$ acting on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, such that*

$$P(a,b|x,y) = \mathrm{Tr}\left(M_x^a \otimes M_y^b\, \rho\right), \tag{1.10}$$

for arbitrary Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$.

The set of all boxes $\vec{P}(a,b|x,y)$ that admit a description as Eq. (1.10) is the set of quantum correlations $\mathcal{Q}$. Note that in Definition 1.3.1 we do not put any restriction on the dimension of the system.

The set of quantum correlations contains the local polytope $\mathcal{L}$. This is expected by the fact that quantum theory is a generalization of classical theory, hence $\mathcal{L} \subseteq \mathcal{Q}$. Some facts concerning the relation of $\mathcal{Q}$ and $\mathcal{L}$ are:

- Local measurements in **separable** quantum states only generate correlations in $\mathcal{L}$.
- If the local measurements of one of the parties are **jointly measurable**[13] then the correlations generated are in $\mathcal{L}$.

[13] Two sets of POVMs $\{E^i\}_{i=1}^m$ and $\{F^j\}_{j=1}^n$ are jointly measurable if there exists a third POVM $\{G^{i,j}\}_{i,j=1}^{m,n}$ such that

$$\sum_j \mathrm{Tr}\, G^{i,j}\rho = \mathrm{Tr}\, E^i\rho \quad \text{and} \quad \sum_i \mathrm{Tr}\, G^{i,j}\rho = \mathrm{Tr}\, F^j\rho$$

for every quantum state ρ. This means that the statistics of the original measurements can be obtained by the marginals of the statistics for the POVM $\{G^{i,j}\}_{i,j=1}^{m,n}$.

Therefore, in order to observe correlations beyond the classical polytope one necessarily needs entanglement and not joint measurability. Whether these conditions are sufficient to generate nonlocal correlations is a fruitful field of research. In the standard Bell scenario, it is known that some entangled quantum states can only generate classical correlations [Wer89, Bar02] (a systematic method to check whether entangled states admit a local model was recently derived in Refs. [CGRS16, HQV+16]). Partial results concerning joint measurability can be found in Refs. [WPGF09, QBHB16]. More general scenarios were introduced in the study of nonlocality: The **hidden nonlocality scenario** [Pop95, ZHHH98] where Alice and Bob are allowed to pre-process one copy of their state by a local filtering operation before starting the Bell test; The **many-copy scenario** where many copies of a state are shared between Alice and Bob [Pal12, CABV13]; And the **network scenario** [CASA11, CRS12] where copies of a bipartite quantum state ρ are distributed in a network of arbitrary shape and number of parties. These general scenarios were shown to be more powerful than the standard one [HQBB13, CASA11, CRS12] and even the phenomena of super-activation of nonlocality was exhibited [Pal12, CABV13]. However, whether nonlocality, entanglement and not joint measurability are equivalent in these general scenarios remains an open problem.

In Ref. [HM15] we show that the value achieved by a quantum state in a Bell scenario is bounded by a term related to its distinguishability from the set of separable states by means of a restricted class of operations. We also propose quantifiers for the nonlocality of a quantum state in the asymptotic scenarios where many copies and filter operations are allowed, and we show that these quantities can be bounded by the relative entropy of entanglement of the state (or the partially transposed state, in the case of PPT states). A summary of the results of Ref. [HM15] is presented in Appendix B.

Concerning the relation between $\mathcal{Q}$ and $\mathcal{NS}$, we can straightforwardly verify that quantum correlations satisfy the no-signaling condition (1.7):

$$\begin{aligned}\sum_b P(a,b|x,y) &= \mathrm{Tr}\left(M_x^a \otimes \left(\sum_b M_y^b\right)\rho\right)\\ &= \mathrm{Tr}\left(M_x^a \otimes \mathbb{1}\,\rho\right)\\ &= \mathrm{Tr}\left(M_x^a\,\rho_A\right)\\ &=: P(a|x),\end{aligned} \tag{1.11}$$

where ρ_A is the reduced state of Alice (as defined in (A.5)), and analogously for Bob's marginal.

In summary, we have

$$\mathcal{L} \subseteq \mathcal{Q} \subseteq \mathcal{NS}, \tag{1.12}$$

and we are going to see in the next Section that all these inclusions can be strict in a general Bell scenario.

Even though the quantum set lies in between two polytopes, in general $\mathcal{Q}$ is not a polytope. The characterization of the quantum set of correlations is the main open problem in the field of nonlocality, and it is not even known for the simplest scenario of two inputs and two outputs[14]. We know that $\mathcal{Q}$ is a convex set[15], but it is not known if this set is closed[16]. An alternative way to define the quantum set of correlations is to impose commutativity of every measurement of Alice with every measurement of Bob, in place of the tensor product structure. The set of correlations generated by these assumptions is denoted $\mathcal{Q}'$. It is clear that $\mathcal{Q} \subseteq \mathcal{Q}'$, and for finite dimensional Hilbert spaces we have equivalence, but whether or not these two sets[17] are equivalent for the infinite dimensional case is known as the Tsirelson's problem[18] [NCPGV12] (this problem is equivalent to a long standing open problem in $\mathbb{C}^*$-algebra, called the Connes' embedding conjecture, see [JNP+11]). An infinite hierarchy of well characterized sets that converges to the set $\mathcal{Q}'$, called **NPA hierarchy**, was introduced by Navascués, Pironio and Acín in Ref. [NPA08] (see more in Section 2.4). This constitutes one of the most powerful tools to deal with problems in the field of quantum nonlocality.

When we are dealing with a particular nonlocality scenario and given a particular Bell expression, as for example $\mathcal{S}^{CHSH}$, we might be interested in knowing which value can be achieved if Alice and Bob have access to quantum boxes (as we will see later, they can reach $\mathcal{S}^{CHSH} = 2\sqrt{2} > 2$). Due to the lack of characterization of the quantum set of correlations, this is in general a very hard problem. More than that: it is not even known whether the quantum value of a Bell inequality is computable in general, since there is a priori no restriction on the dimension of the Hilbert space for the quantum state and measurements. Only for some particular instances it is possible to compute the value exactly or to find efficient approximations. The NPA hierarchy [NPA08] is typically

[14] A partial result characterizes the border of the quantum set in the simplest two-input two-output scenario in the correlation representation [Mas03], *i.e.* when we consider only the correlators $\langle A_x B_y \rangle = P(a = b|x, y) - P(a \neq b|x, y)$ instead of the probabilities $P(a, b|x, y)$.

[15] It is not hard to show that the convex combination of two quantum boxes can be expressed as a quantum box with measurements and state in a Hilbert space of higher dimension.

[16] A set X is closed if every converging sequence of points in X converges to a point of X.

[17] Actually Tsirelson's statement is concerned with the equivalence of the closure of the sets.

[18] See Tsirelson's comments on the problem in: http://www.tau.ac.il/~tsirel/Research/bellopalg/main.html.

used to get upper bounds on the quantum bound of Bell expressions. However the quality of approximation achieved by these bounds remains unknown and the number of parameters to be optimized in each level of the hierarchy increases exponentially. Lower bounds are usually obtained by the called *see-saw* iterative method, where we fix the dimension of the system and recursively optimize over a small set of the variables (the quantum state or one of the party's measurements) fixing the value of the other variables as obtained in the previous step (see Ref. [WW01b]). Each step of the see-saw is an SDP and can be efficiently solved, however this procedure is not guaranteed to converge not even to the global maximum of the fixed dimension. Hence a central problem of great importance in nonlocality theory is to find easily computable and good bounds to handle general classes of Bell inequalities. In Chapters 5, 6 and 7 we present our contributions in this direction.

1.4 The CHSH scenario

We now illustrate the concepts introduced in the previous Sections exploring the simplest scenario that can exhibit nonlocal correlations: the CHSH scenario [CHSH69]. In the CHSH scenario Alice and Bob each has two possible inputs $Q_A = Q_B = \{0,1\}$ and each input has two possible outputs $\mathcal{O}_A = \mathcal{O}_B = \{0,1\}$.

The local polytope $\mathcal{L}$ for this scenario can be characterized by the 16 deterministic local boxes or equivalently by its facets. Up to relabel of inputs and outputs the only nontrivial facet of the local polytope is the CHSH inequality $\mathcal{S}^{CHSH} \leq 2$. Let us write

$$\mathcal{S}_c^{CHSH} = 2, \tag{1.13}$$

to denote the maximum value attainable by classical (local) theories for the CHSH expression. We have already introduced the CHSH expression $\mathcal{S}^{CHSH}$ in Eq. (1.5) and now we evaluate it for quantum and no-signaling boxes.

In quantum theory, in order to calculate the expected values $\langle A_x B_y \rangle$, we can associate an observable to the measurements of Alice and Bob in the following way

$$\begin{aligned} \mathbf{A}_x &:= M_x^0 - M_x^1, \\ \mathbf{B}_y &:= M_y^0 - M_y^1, \end{aligned} \tag{1.14}$$

where $\{M_x^0, M_x^1\}$ are the POVM elements associated to experiment x performed by Alice, and analogously for $\mathbf{B}_y$. Hence we have that the correlator $\langle A_x B_y \rangle$ is equivalent to the expected value of the operator $\mathbf{A}_x \otimes \mathbf{B}_y$:

$$\langle A_x B_y \rangle \equiv \langle \mathbf{A}_x \otimes \mathbf{B}_y \rangle = \mathrm{Tr}\left[(\mathbf{A}_x \otimes \mathbf{B}_y)\, \rho \right]. \tag{1.15}$$

Now, consider that Alice and Bob share the maximally entangled singlet state

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{1.16}$$

and they perform the measurements associated with the following observables:

$$\begin{gathered}\mathbf{A}_0 = \sigma_Z \ , \ \mathbf{A}_1 = \sigma_X \\ \mathbf{B}_0 = \frac{1}{\sqrt{2}}\sigma_Z + \frac{1}{\sqrt{2}}\sigma_X \ , \ \mathbf{B}_1 = \frac{1}{\sqrt{2}}\sigma_Z - \frac{1}{\sqrt{2}}\sigma_X.\end{gathered} \tag{1.17}$$

A direct calculation gives $\mathcal{S}^{CHSH} = 2\sqrt{2}$ for this experiment.

It was shown by Tsirelson [Cir80] that this is actually the maximum value we can achieve with quantum correlations, hence we have

$$\mathcal{S}_q^{CHSH} = 2\sqrt{2}, \tag{1.18}$$

where $\mathcal{S}_q^{CHSH}$ denotes the maximum value attainable by quantum theory for the CHSH expression.

Now let us consider the following box $\vec{P}(a,b|x,y)$:

$$P(a,b|x,y) = \begin{cases} \frac{1}{2} & \text{if } \ a \oplus b = x \cdot y, \\ 0 & \text{otherwise.} \end{cases} \tag{1.19}$$

All the marginals are well defined $P(a|x) = P(b|y) = 1/2 \ \forall \ a,b,x,y$ and hence this box is no-signaling. However this box is not quantum since one can straightforwardly verify that the value achieved in the CHSH expression is $\mathcal{S}^{CHSH} = 4$. This is actually the maximum possible value (note that the expected values $\left\langle A_x B_y \right\rangle$ are numbers in the interval $[-1,1]$), therefore

$$\mathcal{S}_{NS}^{CHSH} = 4. \tag{1.20}$$

The box (1.19) was first introduced in Ref. [KT85] and it became well known after the work of Popescu and Rorlich (and hence denoted PR-box) [PR94], where they discussed whether the no-signaling principle was sufficient to limit the nonlocality of quantum theory, showing that actually no-signaling correlations can go far beyond.

So in the simplest nontrivial scenario we have seen that there exist quantum correlations that can violate the locality assumption, hence they cannot be explained by a local hidden variable model. Also we can conclude that the no-signaling principle (1.7) is not enough to set the limits of quantum theory, as it

can give rise to correlations much more general than the ones restricted by the quantum formalism. In Chapters 6 and 7 we are going to discuss a bit of the implications of these extremal no-signaling boxes in the scenario of communication complexity.

1.5 Multipartite scenarios

In the study of nonlocality we can also consider scenarios with many parties involved, $A_1, \ldots, A_N$, all of them performing experiments far away from each other. In these scenarios, our objects of study are the multipartite boxes $\vec{P}(a_1, \ldots, a_N|x_1, \ldots, x_N)$, where $a_i \in \mathcal{O}_{A_i}$ represent the output of part i when she/he performs the experiment $x_i \in Q_{A_i}$

The **locality** condition is straightforwardly generalized for the case of N parties:

Definition 1.5.1. *A multipartite box $\vec{P}(a_1, \ldots, a_N|x_1, \ldots, x_N)$ is local if there exists a local hidden variable model that reproduces the correlations, i.e. if there exists a variable $\lambda \in \Lambda$, independent of the choice of inputs of the parties, such that*

$$P(a_1, \ldots, a_N|x_1, \ldots, x_N) = \int_\Lambda q(\lambda) p(a_1|x_1, \lambda) \ldots p(a_N|x_N, \lambda) d\lambda \tag{1.21}$$

where $q(\lambda)$ is a probability distribution.

The no-signaling condition is a bit trickier, since now we want to assure no-signaling among all parties.

Definition 1.5.2. *A multipartite box $\vec{P}(a_1, \ldots, a_N|x_1, \ldots, x_N)$ is no-signaling if the no-signaling condition is satisfied by all bi-partition of the parties. More formally, consider a subset of the parties $S \subset \{A_1, \ldots, A_N\}$, hence the no-signaling condition states that*

$$\sum_{\vec{a}_{S^c}} P(\vec{a}_S, \vec{a}_{S^c}|\vec{x}_S, \vec{x}_{S^c}) = \sum_{\vec{a}_{S^c}} P(\vec{a}_S, \vec{a}_{S^c}|\vec{x}_S, \vec{x'}_{S^c}) := P(\vec{a}_S|\vec{x}_S), \tag{1.22a}$$

for all $\vec{x}_{S^c}, \vec{x'}_{S^c} \in Q_{S^c}$, $\vec{x}_S \in Q_S$, $\vec{a}_S \in \mathcal{O}_S$, and all proper subset S of the parties, where $\vec{x}_S = (x_{i_1}, \ldots, x_{i_k})$ and $Q_S = Q_{i_1} \times \ldots \times Q_{i_k}$, for $A_{i_j} \in S$.

Concerning multipartite nonlocality, we have now different levels of correlations. Analogously to the case of multipartite entanglement (see Appendix A.2.3), where we have the concept of **genuine multipartite entanglement** (GME), for multipartite Bell scenarios we have the concept of **genuine multipartite nonlocality**.

Definition 1.5.3. *A N-partite box $\vec{P}(a_1,\ldots,a_N|x_1,\ldots,x_N)$ is genuine N-partite nonlocal if it* ***cannot*** *be written as*

$$P(a_1,\ldots,a_N|x_1,\ldots,x_N)=\sum_i \tilde{q}(i)\int_\Lambda q_i(\lambda)P(\vec{a}_{S_i}|\vec{x}_{S_i},\lambda)P(\vec{a}_{S_i^c}|\vec{x}_{S_i^c},\lambda)\,d\lambda \quad (1.23)$$

for any hidden variables λ_i, where $\tilde{q}(i)$ and $q_i(\lambda_i)$ are probability distributions, and i runs over all proper subset of the parties. Moreover, each $P(\vec{a}_S|\vec{x}_{S_i},\lambda_i)$ are no-signaling probability distributions[19].

Bi-separable quantum states (see Eq. (A.22)) can only generate correlations of the form (1.23), hence if an N-partite quantum state ρ exhibits genuine N-partite nonlocality, we can conclude that ρ is genuinely N-partite entangled. However the converse is not true, and there exist genuinely N-partite entangled states that do not exhibit genuine multipartite nonlocality [ADTA15, BFF+16]. In Ref. [Sve87] Svetlichny proposed a method of detecting genuine multipartite nonlocality, designing a tripartite "Bell-like" inequality that was satisfied for all correlations of the form (1.23) but could be violated for genuinely nonlocal correlations. These results were later generalized for multipartite systems in Refs. [CGP+02, SS02]. Other references on the subject are [BBGP13, BBGL11, ACSA10].

Multipartite nonlocality is still poorly explored and the characterization of these scenarios is less known than the bipartite case. In Chapter 7 we are going to present bounds for the quantum value of a particular class of multipartite Bell inequalities and, as an application of these bounds, we present a systematic way to design device independent witnesses of genuine tripartite entanglement.

[19] In the first time the concept of genuine multipartite nonlocality was introduced [Sve87] no assumptions was made about the joint probability distributions. Nowadays, different definitions are considered, see [BBGP13] for a discussion.

Chapter 2

A glance at Optimization and Complexity theories

In our daily life we are constantly dealing with constrained optimization problems. As for example, when we go to the cinema with a group of friends. We want to have the best seats (the more central ones in the upper rows of the cinema room, so that we do not have to tilt our heads to watch the movie), but at the same time we want to seat all together, so this is not always an easy problem to solve. And while we choose among the vacant seats, taking into account the pros and cons of the available options and choosing the one that will give a higher gain (which can be accounted by the number of happy people minus the number of unsatisfied people), we are mentally solving this hard optimization problem.

In science the situation is not different and many of the interesting problems can be phrased as an optimization problem. In Chapter 1 we have discussed the concept of nonlocality and how linear expressions (Bell expressions) can be designed to differentiate classical theories (with a local hidden variable model), to quantum theory, and these ones from no-signaling theories. Therefore in the study of nonlocality an important question we recurrently ask is:

> *Given a Bell expression, what is the maximum value one can achieve if subjected to local/quantum/no-signaling correlations?*

The answers to these optimization problems have fundamental importance, since the gaps between the classical and quantum, and the quantum and no-signaling optimal values show an intrinsic difference between these theories. Also these gaps have practical applications for the development of quantum algorithms for information processing tasks.

In this chapter we introduce some concepts and theoretical results in optimization and computational complexity theories.

2.1 Computability and computational complexity

In this Section we present some basic concepts of computability and computational complexity. Our goal is only to give an intuitive idea on the subject. For a formal introduction see [GJ90, AB09] (and also [Kav] for a quick overview).

Uncomputability/Undecidability

Given an problem that we want to solve, the first step in computability theory is to try to design an algorithm which is a systematic way to deal with the problem. For any instance[1] (input) of the problem, the algorithm follows a number of specified steps in order to reach the final answer. A problem is said to be computable if there exists an algorithm that, for every input, returns the (approximately) right answer in a finite number of steps.

Definition 2.1.1 (Computability)**.** *A problem (P) is computable if there exists an algorithm such that, for every instance $\mathcal{I}$ and for every $\epsilon > 0$, there exists an integer $N_0 = N_0(\mathcal{I}, \epsilon)$ such that for $N > N_0$ steps the algorithm returns a value ϵ-close[2] to the correct value.*

In Definition 2.1.1 we consider that the problem might have a continuum of possible answers. For problems with a finite set of possible solutions, ϵ-closeness is reduced to exact computation. A very important class of problems with a finite set of solutions are the **decision problems**. A decision problem is a problem with only two possible answers:"YES" or "NO".

A remarkable result is that there exist **uncomputable/undecidable**[3] problems, *i.e.* there exist problems for which it is impossible to construct a single algorithm that for every input will compute the answer in a finite number of steps.

One of the first problems shown to be undecidable was the **halting problem**. The halting problem is the problem of determining, for a given algorithm $\mathcal{A}$ and input x, whether the algorithm stops (*i.e.* it gives the output in a finite number of steps), or if it continues running forever. The proof of undecidability was presented by Turing [Tur37] in the same work where he introduced the idea of a universal computing machine: the Turing machine (for a nice presentation and discussion of the halting problem, see [Pen89]).

[1] An instance is a particular input of the problem. In our example of the cinema problem, the problem itself is specified by the parameters: number of people and available seats. A particular instance of the cinema problem is, for example, four people and the two first rows available.

[2] By ϵ-close we mean $|p^* - p_N| \leq \epsilon$, where p^* is the optimal value and p_N is the value obtained after N steps.

[3] Decidability is the term used for the particular case of decision problems.

Computational complexity

Computable problems can be classified according to the amount of resources required to solve them. And by resources we mean time, memory, energy, and so on. The problems are then classified according to the minimum amount of resources required by the best possible algorithm that solves it.

The classes of computational complexity are usually defined in terms of decisions problems. Every optimization problem has a counterpart decision problem associated to it, for example, instead of asking *'What is the maximum value of a function f?'*, we could ask *'Is the maximum value of f greater than c?'*. The associated decision problem can be no more difficult than the optimization problem itself (since we could simply solve the optimization problem finding the maximum of f and then compare it with c), but interestingly many decision problems can be shown to be no easier than their corresponding optimization problems [GJ90]. Therefore the restriction to decision problems does not lose much generality.

Here we are going to consider the classification of the problems in terms of the time required for the solution of the problem. Given an input of length n, the **time complexity** function of an algorithm, $T(n)$, is the largest amount of time needed by the algorithm to solve a problem with input size n. Usually time complexity is expressed in the 'big O notation' which describes the limiting behavior of a function. We say $T(n) = \mathcal{O}(g(n))$ if there exists n_0 and a constant c such that $T(n) \leq cg(n)$ for all $n \geq n_0$.

A problem is considered **easy**, **tractable** or **feasible** if there exists an algorithm that solves the problem using a polynomial in n amount of time. In case there is no such polynomial time algorithm, the problem is said to be **hard**, **intractable** or **infeasible**.

The first complexity class we are going to define is the **class P**, which is the class of problems that can be solved by an algorithm with time complexity polynomial in the size of the input.

Definition 2.1.2 (The complexity class P)**.** *A decision problem* **P** *belongs to the complexity class P if there exists an algorithm $\mathcal{A}$, with time complexity $T(n) = \mathcal{O}(p(n))$ (where $p(n)$ is a polynomial in n), such that for any instance x of the problem, $|x| = n$,*

- *if* $\mathbf{P}(x) =$*"YES" then* $\mathcal{A}(x) =$*"YES",*
- *if* $\mathbf{P}(x) =$*"NO" then* $\mathcal{A}(x) =$*"NO".*

The class P was introduced by Cobham in 1964 [Cob65] and suggested to be a reasonable definition of an efficient algorithm. A similar suggestion was made

by Edmonds in Ref. [Edm87]. The belief that the class P constitutes the class of efficiently computable problems[4] is called the **Cobham–Edmonds thesis**.

Another important class is the **class NP**. NP is the class of decision problems that can be efficiently verified[5], *i.e.* once a proof y is provided together with the input x, one can check in polynomial time whether the answer is "YES".

Definition 2.1.3 (The complexity class NP)**.** *A decision problem* **P** *belongs to the complexity class NP if there exists an algorithm* $\mathcal{V}$*, of time complexity* $T(n) = \mathcal{O}(p(n))$ *(where* $p(n)$ *is a polynomial in* n*), such that for any instance of the problem* x*,* $|x| = n$*,*

- *if* $\mathbf{P}(x) =$*"YES" then there is a proof* y *such that* $\mathcal{V}(x, y) =$*"YES",*
- *if* $\mathbf{P}(x) =$*"NO" then for all proofs* y $\mathcal{V}(x, y) =$*"NO",*

It is easy to see that P$\subseteq$ NP, since for a problem in P one can simply ignore the proof and solve the problem in polynomial time. But whether or not P=NP is one of the biggest open problems in computer science.

Complete and hard problems

Many researches believe P$\neq$NP, based on the fact that some problems in NP seems to be intrinsically more difficult than the problems in P. However up to now no formal proof in any direction was ever found. An intermediate advance in the classification of NP problems was made by the introduction of the concept of a **polynomial time reduction**, which allowed to select the hardest problems of the class NP. These hardest problems are the ones for which it is most unlikely to find an efficient algorithm, and in case P$\neq$NP these problems definitely belong to the non-intersecting region.

Definition 2.1.4 (Polynomial time reduction)**.** *A problem* $\mathbf{P}_1$ *is polynomial time reducible to* $\mathbf{P}_2$*, if there exists a polynomial time algorithm* $\mathcal{R}$ *such that for every input*

[4]Note that a polynomial time algorithm of complexity n^{100} seconds would take many orders of magnitude more than the age of the Universe for an input of size 10, while the exponential algorithm of complexity 2^n would take only about 17 minutes for the same input size. However the Cobham–Edmonds thesis is supported by many examples of natural problems and how they scale with the input size. Furthermore, polynomial time algorithms involve a deep knowledge of the structure of the problem, in contrast with exponential time algorithms which are usually a mere brute-force search over all possibilities. Here we are just going to assume that the class P is a reasonable definition of efficient (for more discussion on this point, see [AB09, GJ90]).

[5]Originally the class NP was defined in terms of non-deterministic Turing machines (a very abstract computational model), and only later it was recognized as the class of problems that can be easily verified (see [Kav]).

x of problem $\mathbf{P}_1$

$$\mathbf{P}_1(x) = \mathbf{P}_2(\mathcal{R}(x)), \tag{2.1}$$

and in this case we say $\mathbf{P}_1 \preceq_{\mathcal{R}} \mathbf{P}_2$.

The idea of a reduction is to map a problem $\mathbf{P}_1$ into another problem $\mathbf{P}_2$, such that by solving $\mathbf{P}_2$ one is able to get the solution of $\mathbf{P}_1$. However, since we are concerned with efficiency, a good reduction is one that can be performed in polynomial time. With that in mind, by Definition 2.1.4 we see that if problem $\mathbf{P}_2$ is efficiently solvable then $\mathbf{P}_1$ is also efficiently solvable[6]. And if $\mathbf{P}_1$ is not efficiently solvable, we can conclude that $\mathbf{P}_2$ cannot be efficiently solvable, otherwise we would have a contradiction. Therefore if $\mathbf{P}_1 \preceq_{\mathcal{R}} \mathbf{P}_2$, then we can say that $\mathbf{P}_2$ is at least as hard as $\mathbf{P}_1$.

Definition 2.1.5 (NP-hard problems)**.** *A problem* $\mathbf{P}$ *is NP-hard if there exists a polynomial time reduction of every problem* $\mathbf{P}' \in NP$ *to problem* $\mathbf{P}$*:*

$$\mathbf{P}' \preceq_{\mathcal{R}} \mathbf{P} \quad \forall \mathbf{P}' \in NP. \tag{2.2}$$

Definition 2.1.6 (NP-complete problems)**.** *A problem* $\mathbf{P}$ *is NP-complete if* $\mathbf{P}$ *is NP-hard and if* $\mathbf{P} \in NP$.

The NP-complete problems are the hardest problems of the NP class, since by finding a polynomial time algorithm for solving an NP-complete problem one automatically solves any problem in NP in polynomial time (and then would have proved P=NP!).

Note that once we identify an NP-complete problem $\mathbf{P}_1$, by reducing it to an NP problem $\mathbf{P}_2$, we automatically prove that $\mathbf{P}_2$ is also NP-complete. Hence the concept of reduction opens the possibility of many proofs of hardness in the field of computational complexity. The first proof of NP-completeness was given by Stephen Cook in Ref. [Coo71], where he showed that the SAT problem[7] is NP-complete (known as the Cook-Levin theorem[Coo71, Lev73]).

In Ref. [Kar72], Richard Karp uses Cook-Levin theorem in order to show that there is a polynomial reduction from the SAT problem to each of 21 combinatorial and graph theoretical computational problems. In particular a $\{0,1\}$-integer programming and the calculus of the independence number of a graph (that we are going to discuss later) are NP-complete problems.

[6] We simply have to apply the reduction algorithm $\mathcal{R}$ which takes polynomial time, and then we solve $\mathbf{P}_2$ which also takes polynomial time.

[7] The SAT (satisfiability problem) is the problem of determining whether there exists a consistent assignment for the variables of a particular Boolean circuit such that the whole expression is evaluated as true. For example, the Boolean circuit $(x_1 \vee x_2) \wedge x_3$ can be evaluated as true with the assignment x_1 =true, x_2 =false, and x_3 =true.

2.2 Optimization problems

In the previous Section we presented the concepts of computability and uncomputability. Also, we have seen that the computable problems can be divided in classes of complexity which classify the problems according to how many resources are necessary to solve it. In this section we discuss a bit of the theory of optimization following approaches of Refs. [BTN13] and [BV04].

Let us consider an optimization problem where we want to minimize a function f_0 subjected to some constraints:

$$(P): \begin{cases} \min & f_0(x) \\ \text{s.t.} & f_i(x) \geq 0\ ,\ i = 1, \ldots, m \\ & h_i(x) = 0\ ,\ i = 1, \ldots, p \end{cases} \tag{2.3}$$

where

- $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$: is the **optimization variable**,
- f_0 : is an n-variable real function called **objective function**,
- $f_i,\ h_i$: are n-variable real functions called **constraint functions**.

The set of points for which the objective and constraint functions are defined is called the **domain** of the problem (P):

$$\mathcal{D} = \bigcap_{i=0}^{m} \text{dom}\ f_i \cap \bigcap_{i=1}^{p} \text{dom}\ h_i. \tag{2.4}$$

A point $x \in \mathcal{D}$ is **feasible** if it satisfy all the constraints, *i.e.* $f_i(x) \geq 0\ ,\ i = 1, \ldots, m$ and $h_i(x) = 0\ ,\ i = 1, \ldots, p$. The set of all feasible points is called the **feasible set** $\mathcal{F}$,

$$\mathcal{F} = \{x \mid x \in \mathcal{D},\ f_i(x) \geq 0\ ,\ i = 1, \ldots, m\ ,\ h_i(x) = 0\ ,\ i = 1, \ldots, p\}\,. \tag{2.5}$$

The **optimal value** p^* of problem (P) is the infimum of f_0 over the feasible points

$$p^* = \inf_{x \in \mathcal{F}} f_0(x). \tag{2.6}$$

If the optimal value is achieved by a feasible point then the problem is said to be **solvable**. However, for some problems the optimal value may not be achieved by any feasible point.

The simplest optimization problem is the **linear programming** (LP) where the objective and constraints are affine functions[8]. For an LP the numerical method of **interior-point**[9], developed in the 1980s, can solve it efficiently with $\mathcal{O}(nm^2)$ operations, where n is the number of variables and m the number of inequality constraints. Therefore LP $\in$ P.

Many advances in numerical methods for solving optimization problems are due to the recognition that the interior-point method can also be used to solve other **convex optimization** problems efficiently. Convex optimization problems are the ones where the objective and constraint functions are convex[10]. Hence a convex optimization problem is usually considered a tractable one, whereas non-convex problems are in general hard. Fortunately many interesting problems in many areas: physics, mathematics, engineering and so on, can be phrased as a convex optimization problem.

A particular case of convex optimization problem is the semidefinite programming (SDP). For SDPs, algorithms which utilize the method of interior-point are well established, therefore, these problems can also be solved efficiently (in polynomial time in the number of variables). For more general convex problems the numerical methods are not so well established as for LP and SDP, still the interior-point methods work well in practice.

As nicely pointed by Boyd and Vandenberghe [BV04] these numerical methods for solving these problems are so well structured that they can be considered a technology:

> *"Solving* [LP and SDP] *is a technology that can be reliably used by many people who do not know, and do not need to know, the details."*

In this Section, we present the formal definitions of linear programming (LP), semidefinite programming (SDP), and integer programming (IP).

Linear optimization

A linear programming (LP) is an optimization problem (2.3) where the objective and constraint functions are affine. An LP can be expressed as

$$(LP): \begin{cases} \min & \langle c|x\rangle \\ \text{s.t.} & A\,|x\rangle \geq |b\rangle \end{cases} \tag{2.7}$$

[8] A function f is affine if $f(ax+by) = af(x) + bf(y)\ \forall\ a+b=1$.

[9] For details of the interior-point method see Ref. [BV04].

[10] A function f is convex if $f(ax+by) \leq af(x) + bf(y)\ \forall\ a,b \geq 0, a+b=1$.

where all the constraint functions are expressed in a unique vector inequality[11], $A|x\rangle \geq |b\rangle$, which represents a component-wise relation $|a\rangle \geq |b\rangle \Leftrightarrow a_i \geq b_i,\ \forall\ i.\ |x\rangle \in \mathbb{R}^n$, $|c\rangle \in \mathbb{R}^n$, $|b\rangle \in \mathbb{R}^m$, and A is a $m \times n$ matrix. We are making use of Dirac's notation[12] for consistency with the other chapters.

Semi-definite programming

In order to generalize an LP one can relax the linearity condition of the objective or the constraint functions. However another way to generalize an LP that leads to a class of very interesting problems is to keep the objective and constraint functions linear but to relax the meaning of $\geq$ in the inequality constraints.

The order relation $\geq$ in an LP, Eq. (2.7), is a coordinate-wise relation where $|a\rangle = (a_1, \ldots, a_n)$ and $|b\rangle = (b_1, \ldots, b_n)$ satisfy

$$|a\rangle \geq |b\rangle \Leftrightarrow \{a_i \geq b_i,\ \forall\ i = 1, \ldots, m\}\,. \tag{2.8}$$

However a partial order relation $\geq$ can be defined in a more general framework. A good partial ordering is completely determined by a subset K, of a vector space E, where the relation $\geq_K$ is defined as:

$$a \geq_K b \Leftrightarrow a - b \geq_K 0 \Leftrightarrow a - b \in K, \tag{2.9}$$

and K determines the set of positive elements:

$$K = \{a \in E \mid a \geq 0\}\,. \tag{2.10}$$

In order to satisfy some expected properties (see [BTN13] for more details) the set K cannot be arbitrary and it has to be a **pointed cone**, *i.e.*

(i) K is nonempty and closed under addition: $a, a' \in K \Rightarrow a + a' \in K$.

(ii) K is a conic set: $a \in K, \lambda \geq 0 \Rightarrow \lambda a \in K$.

(iii) K is pointed: $a \in K$ and $-a \in K \ \Rightarrow\ a = 0$.

An optimization problem whose constraints are defined by the partial ordering $\geq_K$, for a set K satisfying properties (i)-(iii), is called a **conic problem**.

[11] And remember that an equality constraint $a = b$ can always be expressed as two inequality constraints: $a \geq b$ and $a \leq b$.

[12] The called "braket" notation, used in quantum theory, was introduced by Dirac in Ref. [Dir39].

Now let K be the cone of symmetric positive semidefinite $m \times m$ matrices S_+^m, this defines a semidefinite programming (SDP):

$$(SDP): \begin{cases} \min & \langle c|x\rangle \\ \text{s.t.} & \mathcal{A}(|x\rangle) - B \geq_{S_+^m} 0 \end{cases} \tag{2.11}$$

where $\mathcal{A} : \mathbb{R}^n \longrightarrow S^m$ is a linear map from vectors in $\mathbb{R}^n$ to the space of symmetric $m \times m$ matrices S^m. $B \in S^m$, and $|c\rangle$ and $|x\rangle$ are vectors in $\mathbb{R}^n$.

The standard form of an SDP (and the one we are going to deal with in the following chapters) is

$$(SDP): \begin{cases} \min & \mathrm{Tr}(CX) \\ \text{s.t.} & \mathrm{Tr}(A_i X) = b_i,\ i = 1, \ldots, r \\ & X \geq_{S_+^m} 0 \end{cases} \tag{2.12}$$

where $X, C, A_i \in S^m$.

The formulations (2.11) and (2.12) are equivalent, and a problem in form (2.11) can always be rephrased into the from (2.12) and vice-versa[BV04].

From now on we are going to omit the subscript in the ordering relation $\geq_{S_+^m}$, but from the context it will be clear which ordering relation is being applied.

Integer programming

An integer programming (or integer linear programming) is a problem where the objective and constraint functions are affine functions but the variables are restricted to be integers[13]. $\{0,1\}$-integer programming is the particular case of integer programming where the variables are restricted to assume the values 0 or 1. A general $\{0,1\}$-integer programming (IP) can be written as

$$(SDP): \begin{cases} \min & \langle c|x\rangle \\ \text{s.t.} & A\,|x\rangle - |b\rangle \geq 0 \\ & \vec{x} \in \{0,1\}^n \end{cases} \tag{2.13}$$

where $|b\rangle \in \mathbb{R}^m$ and A is an $m \times n$ real matrix.

Problems of the form (2.13) appear in the study of nonlocality, in the calculus of the classical value of a Bell expression. Note that a Bell expression is a linear function of the joint probability distributions $P(a,b|x,y)$, and one can easily check that imposing no-signaling constraints (which are linear constraints)

[13] This restriction can be seen as a non-linear constraint, for example, if x is restricted to assume values $\{-1,1\}$, this is equivalent to require the quadratic constraint $x^2 = 1$ to be satisfied.

together with determinism, *i.e.* $P(a,b|x,y) \in \{0,1\}$, is equivalent to impose deterministic locality: $P(a,b|x,y) = D(a|x)D(b|y)$. Consequently, the search over all deterministic local boxes, which is sufficient to obtain the classical value of a Bell expression (see Chapter 1), is a $\{0,1\}$-integer programming.

As previously mentioned, $\{0,1\}$-integer programming was shown to be an NP-complete problem [Kar72], therefore the task of obtaining the classical value of a Bell inequality is hard in general.

2.3 Duality

The idea of the dual of a problem (P) is to play with the constraint inequalities (summing equations, adding trivial inequalities $1 > 0$ and so on) in order to obtain a quantity that is always smaller then the optimal value of problem (P). In this Section we will study the theory of **Lagrange duality** [BV04].

Given an optimization problem (P):

$$(P): \begin{cases} \min & f_0(x) \\ \text{s.t.} & f_i(x) \geq 0\ ,\ i = 1,\dots,m \\ & h_i(x) = 0\ ,\ i = 1,\dots,p \end{cases} \tag{2.14}$$

the **Lagrangian function**, $L : \mathcal{D} \times \mathbb{R}^m \times \mathbb{R}^p \longrightarrow \mathbb{R}$, is defined as

$$L(x,\lambda,\nu) = f_0(x) - \sum_{i=1}^{m} \lambda_i f_i(x) + \sum_{i=1}^{p} \nu_i h_i(x). \tag{2.15}$$

where $\lambda = (\lambda_1,\dots,\lambda_m)$ and $\nu = (\nu_1,\dots,\nu_p)$. Note that if $\lambda \geq 0$, for every feasible point $x \in \mathcal{F}$ of (P) we have $L(x,\lambda,\nu) \leq f_0(x)$.

Now we define the **dual function**, $g : \mathbb{R}^m_+ \times \mathbb{R}^p \longrightarrow \mathbb{R}$ as

$$g(\lambda,\nu) = \inf_{x\in\mathcal{D}} L(x,\lambda,\nu). \tag{2.16}$$

The dual function g is the point-wise infimum of a family of affine functions of the variables (λ,ν), and hence $g(\lambda,\nu)$ is always concave[14] even though no structure was assumed about the problem (P).

[14] A point-wise infimum of an affine function over variable λ can in general be written as $g(\lambda) = \inf_x a(x)\lambda + b(x)$. Now, taking $c_1, c_2 \geq 0$, $c_1 + c_2 = 1$ we have

$$\begin{aligned} g(c_1\lambda_1 + c_2\lambda_2) &= \inf_x \left[c_1(a(x)\lambda_1 + b(x)) + c_2(a(x)\lambda_2 + b(x))\right] \\ &\geq c_1 \inf_x \left[a(x)\lambda_1 + b(x)\right] + c_2 \inf_x \left[a(x)\lambda_2 + b(x)\right] \\ &= c_1 g(\lambda_1) + c_2 g(\lambda_2). \end{aligned}$$

Let p^* be the optimal solution of the problem (P). By construction we have that

$$g(\lambda,\nu) = \inf_{x\in\mathcal{D}} L(x,\lambda,\nu) \leq \inf_{x\in\mathcal{F}} L(x,\lambda,\nu) \leq \inf_{x\in\mathcal{F}} f_0(x) = p^*. \tag{2.17}$$

And therefore $g(\lambda,\nu)$ is always a lower bound to the value of problem (P). One can then look for the best lower bound that can be obtained from g, and that is the idea of the **Lagrange dual problem** (D):

$$(D): \begin{cases} \max & g(\lambda,\nu) \\ \text{s.t.} & \lambda \geq 0 \end{cases}. \tag{2.18}$$

Note that the Lagrange dual problem is the maximization of a concave function subjected to linear constraints. The maximization of g is equivalent to the minimization of $-g$, which is then a convex function. Therefore (D) is a convex optimization problems.

Theorem 2.3.1 (Weak duality)**.** *Let p^* be the optimal value of a problem (P), and (D) be the corresponding Lagrange dual problem with optimal value d^*. It holds that*

$$d^* \leq p^*. \tag{2.19}$$

*Where $p^* - d^* \geq 0$ is the **duality gap**.*

The Weak duality Theorem follows by construction of the dual problem. Weak duality holds in general for any kind of optimization problem, as no restriction on the nature of the objective and constraint functions was made for the construction of the Lagrangean. However for many convex problems an even stronger result holds, that the optimal value of the dual is actually equal to the optimal value of the problem (P). This is stated by Slater's condition.

Theorem 2.3.2 (Strong duality- Slater's condition)**.** *Given a convex optimization problem (P) of the form*

$$(P): \begin{cases} \min & f_0(x) \\ s.t. & f_i(x) \geq_K 0\ ,\ i = 1,\dots,m \\ & Ax - b = 0 \end{cases} \tag{2.20}$$

where f_0 is a convex function bounded below and $f_1,\dots,f_m$ are K-convex functions[15].

[15] A function f is K-convex if $f(cx + (1-c)y) \leq_K cf(x) + (1-c)f(y)$, for $0 \leq c \leq 1$.

If there exists a ***strictly feasible*** *point*[16]

$$x \in relint(\mathcal{D}) \;\; s.t. \;\; f_i(x) >_K 0 \;, \; i = 1, \ldots, m \;\; and \;\; Ax - b = 0, \tag{2.22}$$

then $d^* = p^*$.

There are other results which establishes conditions for strong duality for non-convex problems. These conditions are in general called **constraint qualifications** [BV04].

2.4 SDP relaxations of hard problems

The idea of a relaxation is the following: In an optimization problem (P) we want to find the optimum value of a function $f_0(x)$ searching over the domain $\mathcal{F}$, which is determined by the constraints of the problem. However even when the function $f_0(x)$ is simple (a linear function for example), it might be the case (and it is the case in many interesting problems) that the domain $\mathcal{F}$ is extremely hard to characterize. An alternative way to deal with this difficulty is to consider the problem (P'), where, instead of searching for the minimum of $f_0(x)$ over the set $\mathcal{F}$, we make the search over a bigger (relaxed) set $\mathcal{F}'$ (see Figure 2.1), $\mathcal{F} \subseteq \mathcal{F}'$, which is simpler to describe.

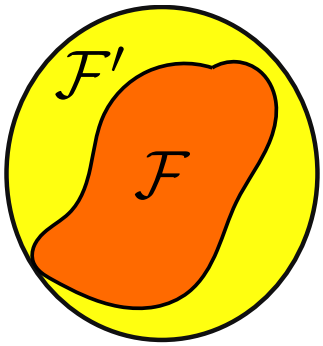


Figure 2.1: The idea of a relaxation: Instead of optimizing $f_0(x)$ over the set $\mathcal{F}$, one considers the problem of finding the optimum value of $f_0(x)$ over the simpler set $\mathcal{F}'$.

[16] A point x belongs to the relative interior of a set $C \subseteq \mathbb{R}^n$, $x \in \text{relint}(C)$ if

$$\exists r > 0 \text{ s.t. } \forall y \in \text{Aff}(C), |y - x| < r \text{ then } y \in C. \tag{2.21}$$

where $\text{Aff}(C) = \{x | x = \lambda x_1 + (1-\lambda)x_2, \text{ for } x_1, x_2 \in C, \lambda \in \mathbb{R}\}$.

Since $\mathcal{F} \subseteq \mathcal{F}'$, the optimal value obtained for problem (P') is smaller than or equal the optimal value obtained for problem (P). Hence a relaxation is a way to get lower bounds for an optimization problem (P).

A relaxation is wanted to satisfy two features: it should be *efficiently solvable* (*i.e.* the relaxed set has to be nicely characterized), and at the same time it should be *good* meaning that the value obtained in the relaxation is close to the actual value (we do not want a relaxation that gives a completely non-informative result).

As an example let us consider the problem of finding the independence number of a graph $\mathcal{G}(V, E)$[17] with n vertices, which can be formulated as the following $\{0, 1\}$-integer programming:

$$\alpha = \begin{cases} \max & \sum_{i=1}^{n} x_i \\ \text{s.t.} & x_i + x_j \leq 1 \text{ if } \{x_i, x_j\} \in E \\ & x_i \in \{0, 1\} \ \forall i. \end{cases} \tag{2.23}$$

As we have argued before, this is an NP-complete problem and hence considered intractable for large n. A simple relaxation can be derived by just turning the nonlinear constraint $x_i \in \{0, 1\}$ into a linear one

$$\alpha' = \begin{cases} \max & \sum_{i=1}^{n} x_i \\ \text{s.t.} & x_i + x_j \leq 1 \text{ if } \{x_i, x_j\} \in E \\ & 0 \leq x_i \leq 1 \ \forall i. \end{cases} \tag{2.24}$$

We have that $\alpha' \geq \alpha$ for every graph $\mathcal{G}(V, E)$, since we now allow x_i to assume all the values between 0 and 1. Moreover, problem (2.24) is a linear program which can be efficiently solved.

For a long time the only known practical relaxations were the LP ones. However, with the advent, over the last decades, of techniques for efficiently solving semidefinite programs, it came the possibility of exploring semidefinite relaxations, which has become a fruitful area of research[18]. Semidefinite relaxations have been shown to be particularly useful for combinatorial problems. We are going to see, in Section 4.1, an SDP relaxation for the independence number problem (2.23) (the Lovász number).

NPA hierarchy

We have stated that calculating the classical value of a Bell inequality is a $\{0, 1\}$-integer programming, and thus it is NP-hard. For the quantum value

[17] The independence number of a graph is the maximum number of vertices such that no two of each are connected by an edge (see Chapter 4).

[18] For a detailed discussion see the Preface of Ref. [BTN13].

the situation is even worse! Note that in Chapter 1, when we define the quantum boxes, we make no restriction over the dimension of the system, and hence to obtain the quantum value one should optimize over all possible states and measurements in all possible dimensions. There is no known algorithm to determine the quantum value of a general Bell inequality[19] in a finite number of steps and therefore this problem may even be uncomputable (In Ref. [AFLS15] the authors conjecture that it is actually non-computable.).

The most general method known to deal with this intractable problem was introduced by Navascués, Pironio and Acín, in Ref. [NPA08]: the **NPA hierarchy**. The NPA hierarchy is a hierarchy of semidefinite programs where each level corresponds to an optimization over a tighter relaxation of the quantum set of correlations. These sets are nicely constrained by a $\geq_{S_m^+}$ relation and therefore calculating the optimal value of a Bell inequality over a level of the hierarchy is a semidefinite program. The hierarchy is proved to converge to the set Q' which is defined as following:

Definition 2.4.1. *The set Q' is the set of boxes $\vec{P}(a,b|x,y)$ such that*

$$P(a,b|x,y) = \langle\psi| E_x^a E_y^b |\psi\rangle \tag{2.25}$$

for some state $|\psi\rangle \in \mathcal{H}$ and projective measurements[20] $\{E_x^a\}$ and $\{E_y^b\}$, acting on $\mathcal{H}$, satisfying

$$\left[E_x^a, E_y^b\right] = 0 \ \forall a,b,x,y. \tag{2.26}$$

Note that the set of quantum correlations Q is contained in Q', since all local measurements of Alice commutes with local measurements of Bob. But whether or not $Q = Q'$ is an open problem known as Tsirelson's problem [NCPGV12] (see discussion in Section 1.3).

The NPA hierarchy constitutes one of the most powerful tools in the field of nonlocality, and it has led to the derivation of innumerous results. However the quality of the approximation achieved by these bounds remains unknown in general. Moreover for a Bell inequality with m inputs and d outputs per party, the n-th level of the hierarchy involves a matrix of size $O((2md)^n)$ as an SDP variable, so, in general, the complexity increases exponentially with the level of the hierarchy.

[19] We are going to see in Chapter 3 that for a particular class of Bell inequalities, the XOR games, the quantum value can be determined efficiently by an SDP.

[20] Since we do not fix dimension, there is no loss of generality in restrict to pure states and projective measurements. This is due to Naimark's Theorem, see https://cs.uwaterloo.ca/~watrous/CS766/LectureNotes/05.

Chapter 3

Nonlocal games

Some Bell inequalities can be naturally phrased in the framework of a game. A **nonlocal game** is a cooperative task where the players receive questions from a referee and they are supposed to give answers in order to maximize some previously defined payoff function. Upon starting the game, the players are not allowed to communicate anymore, therefore any strategy has to be agreed in advance.

Nonlocal games have a wide range of applications. They play an important role in the study of communication complexity [BCMdW10, BZPZ04] (and vice-versa) and in the formulation of device-independent cryptographic protocols [Eke91, CR12].

In a computer science language, a nonlocal game with n players can be seen as the particular case of **multiprover interactive proof systems** with n provers and one round. An interactive proof system consists of an all powerful[1], but untrusted, prover who wants to convince a verifier, who has limited computational power, of the truth of some statement by exchanging messages in many rounds. A multiprover interactive proof system is an interactive proof system with many provers, who may be bounded not to communicate during the proof. Multiprover interactive proof systems were introduced in Ref. [BOGKW88] as an alternative to allow for the performance of some cryptographic tasks without relying on extra assumptions, such as the existence of one-way functions[2] or limitations on the computational power. With the introduction of many provers these extra assumptions can be replaced by the condition of physical separation of the provers during the course of the protocols. For further remarks on the

[1] Powerful in a computational sense, meaning that the prover has unbounded resources, although only classical resources, and unlimited computational power.

[2] A one-way function f is a function that can be computed in polynomial time for any input x, however the function f is hard to invert. The existence of one-way functions would imply that P$\neq$NP.

connection of interactive proof systems with entangled provers and the quantum value of nonlocal games see Ref. [CHTW04].

In this chapter we present definitions and results on nonlocal games. In the first sections we restrict the presentation to the case of 2-player games. The case of n-player games is discussed in Section 3.4. For a nice introduction to nonlocal games see Ref. [CHTW04].

3.1 Definitions

Definition 3.1.1 (Nonlocal Game). *A nonlocal game $g(V,p)$ is a cooperative task where 2 players, Alice and Bob, who are not allowed to communicate after the game starts, receive respectively questions $x \in Q_A$ and $y \in Q_B$, chosen from a probability distribution $p(x,y)$ by a referee. Upon receiving the questions, Alice is supposed to give an answer $a \in \mathcal{O}_A$ and Bob $b \in \mathcal{O}_B$. The winning condition of the game is defined by the payoff function $V(a,b|x,y)$ which assumes value 1 to indicate when the players win and value 0 to indicate when they lose.*

Given a particular strategy applied by the players, which is specified by a box $\vec{P}(a,b|x,y)$, the figure of merit that we are interested in analyzing is the **average probability of success** given by

$$\omega(g) = \sum_{a,b,x,y} p(x,y)V(a,b|x,y)P(a,b|x,y). \tag{3.1}$$

Note that $\omega(g)$ can be regarded as a Bell expression, since it is a linear function of the joint probability distributions $P(a,b|x,y)$.

Classical strategies

The maximum average probability of success optimizing over all possible classical strategy is the **classical value** of the game, denote $\omega_c(g)$. In order to obtain $\omega_c(g)$ we have to optimize over the local boxes of the particular Bell scenario defined by the game. As we argued before, the maximum value of $\omega(g)$ is attained by a deterministic strategy, hence:

$$\omega_c(g) = \max_{\vec{D}(a|x),\vec{D}(b|y)} \sum_{a,b,x,y} p(x,y)V(a,b|x,y)D(a|x)D(b|y), \tag{3.2}$$

where $\vec{D}(a|x)$ and $\vec{D}(b|y)$ are deterministic probability distributions. The number of possible deterministic strategies for a particular game is $|\mathcal{O}_A|^{|Q_A|} \times |\mathcal{O}_B|^{|Q_B|}$, which increases exponentially with the number of inputs.

Quantum strategies

A general quantum strategy is described by the players sharing a bipartite quantum state ρ of arbitrary dimension and giving their answers according to the result of local measurements, $\{M_x^a\}$ and $\{M_y^b\}$, that they perform in their systems:

$$P(a,b|x,y) = \mathrm{Tr}\left[(M_x^a \otimes M_y^b)\rho\right]. \tag{3.3}$$

Since we do not make any restriction on the Hilbert space dimension of the system we can actually restrict ourselves to pure states and projective measurements[3]. Therefore, the **quantum value** of the game, $\omega_q(g)$, which is the maximum average probability of success of players applying a quantum strategy, is given by:

$$\omega_q(g) = \sup_{|\psi\rangle,\{M_x^a\},\{M_y^b\}} \sum_{a,b,x,y} p(x,y)V(a,b|x,y)\,\langle\psi|\, M_x^a \otimes M_y^b\,|\psi\rangle\,. \tag{3.4}$$

where $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, for arbitrary Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, and $\{M_x^a\}$ and $\{M_y^b\}$ are projective measurements.

As discussed before, we do not put any restriction on the dimension of the system and, as a particular class of Bell inequalities, it is not known if the quantum value of a nonlocal game is computable in general (see Section 2.4).

No-signaling strategies

We also define the **no-signaling value** of the game, denoted ω_{NS}

$$\omega_{NS}(g) = \max_{\vec{P}(a,b|x,y)\in\mathcal{NS}} \sum_{a,b,x,y} p(x,y)V(a,b|x,y)P(a,b|x,y). \tag{3.5}$$

The no-signaling value is easily calculated by a linear programming, since we have a linear function of the variables $P(a,b|x,y)$, subjected to linear constraints given by the no-signaling conditions (1.7).

3.2 XOR games

In this Section we focus on the so-called XOR games, introduced in Ref. [CHTW04]. XOR games are the simplest class of nonlocal games where the

[3] It is a consequence of Naimark's Theorem that an arbitrary POVM on a system of Hilbert space $\mathcal{H}$ is equivalent to a global projective measurement in $\mathcal{H} \otimes \mathcal{H}'$, where $\mathcal{H}'$ is the Hilbert space of an auxiliary system. See https://cs.uwaterloo.ca/~watrous/CS766/LectureNotes/05.

players have two possible answers, $a, b \in \{0,1\}$, and the payoff function only depends on the sum modulo two[4] of their outputs:

$$V(a,b|x,y) = \begin{cases} 1 & \text{if } a \oplus b = f(x,y) \\ 0 & \text{otherwise,} \end{cases} \tag{3.6}$$

for some function $f : Q_A \times Q_B \longrightarrow \{0,1\}$.

Definition 3.2.1 (XOR games)**.** *An* XOR *game, $g^{\oplus}(f,p)$ is a nonlocal game where Alice and Bob receive respectively questions $x \in Q_A$ and $y \in Q_B$, chosen from a probability distribution $p(x,y)$ by a referee. Upon receiving the questions, Alice outputs a bit a and Bob outputs bit b. The players win the game if $a \oplus b = f(x,y)$.*

The **average probability of success** (3.1) for an XOR game can be written as[5]

$$\omega(g^{\oplus}) = \frac{1}{2} + \frac{1}{2}\left(\sum_{x,y} p(x,y)(-1)^{f(x,y)} \left[P(a \oplus b = 0|x,y) - P(a \oplus b = 1|x,y)\right]\right). \tag{3.8}$$

The first $\frac{1}{2}$ on the RHS of Eq. (3.8) can be interpreted as the probability of success of the players when they apply a totally random strategy (*i.e.* if upon receiving her input Alice tosses a coin to determine her output a, and Bob does the same).

The bias of the game represents how much a particular strategy is better (or worse) than the completely random strategy, and is defined as:

$$\begin{aligned} \epsilon &:= 2\omega - 1 \\ &= \sum_{x,y} p(x,y)(-1)^{f(x,y)} \left[P(a \oplus b = 0|x,y) - P(a \oplus b = 1|x,y)\right]. \end{aligned} \tag{3.9}$$

In expression (3.8) we see that $\omega(g^{\oplus})$ is related to the expected value of binary observables (see Eq. (1.15)), $\langle A_x B_y \rangle = P(a \oplus b = 0|x,y) - P(a \oplus b = 1|x,y)$. Therefore XOR games are equivalent to the important class of Bell expressions that involve only terms with correlators $\langle A_x B_y \rangle$, the **full-correlation Bell inequalities**, which is a widely studied class of Bell inequalities [Weh06, WW01a]. The CHSH inequality (1.5) being the most remarkable example of a full-correlation Bell inequality.

[4] The sum modulo 2 is equivalent to the logical operation exclusive or, also denoted XOR, that is the reason for the name of the games.

[5] Where we have used the fact that

$$P(a \oplus b = f(x,y)|x,y) = \frac{1}{2} + \frac{P(a \oplus b = f(x,y)|x,y) - P(a \oplus b \neq f(x,y)|x,y)}{2}. \tag{3.7}$$

The game matrix

To every XOR game we can associate a $|Q_A| \times |Q_B|$ matrix, the **game matrix** Φ, which carries all the information necessary to describe the game: the inputs' probability distribution and the winning condition specified by $f(x,y)$:

$$\Phi = \sum_{x,y} p(x,y)(-1)^{f(x,y)} |x\rangle\langle y| , \tag{3.10}$$

where $\{|x\rangle\}$ and $\{|y\rangle\}$ define orthonormal basis and x and y run over the inputs of Alice and Bob respectively.

SDP characterization of the quantum value of an XOR game

For the particular class of bipartite XOR games, a theorem due to Tsirelson [Tsi80, Tsi87], leads to the result that the quantum value of these games can be computed efficiently by a semidefine program [CHTW04, Weh06].

Theorem 3.2.1 (Tsirelson [Tsi80]). *Let $\mathbf{A}_1, \ldots, \mathbf{A}_m$ and $\mathbf{B}_1, \ldots, \mathbf{B}_n$ be observables with eigenvalues in the interval $[-1,1]$ acting on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Then, for any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, there exist unit vectors $|u_1\rangle, \ldots, |u_m\rangle, |v_1\rangle, \ldots, |v_n\rangle \in \mathbb{R}^{m+n}$ such that*

$$\langle\psi| \mathbf{A}_x \otimes \mathbf{B}_y |\psi\rangle = \langle u_x|v_y\rangle . \tag{3.11}$$

Conversely, let $\{|u_x\rangle\}_{x=1}^m$, $\{|v_y\rangle\}_{y=1}^n \in \mathbb{R}^N$ be unit vectors. Then, for the maximally entangled state $|\Phi^+\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, with $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^d$, $d = 2^{\lceil \frac{N}{2} \rceil}$, there exist ± 1-observables, $\{\mathbf{A}_x\}$ acting on $\mathcal{H}_A$ and $\{\mathbf{B}_y\}$ acting on $\mathcal{H}_B$, such that

$$\langle u_x|v_y\rangle = \langle\Phi^+| \mathbf{A}_x \otimes \mathbf{B}_y |\Phi^+\rangle . \tag{3.12}$$

Tsirelson's Theorem establishes a one-to-one relation between quantum strategies and the inner product of real vectors.

From now on let us set $|Q_A| = m_A$ and $|Q_B| = m_B$. The optimal quantum strategy of an XOR game is given, in general, by Alice and Bob measuring ± 1 observables $\mathbf{A}_x$ and $\mathbf{B}_y$ on a shared pure quantum state $|\psi\rangle$ of arbitrary dimension. By Tsirelson's theorem 3.2.1 the expected value of these observables can be replaced by the inner product $\langle u_x|v_y\rangle$ of unit vectors in $\mathbb{R}^{m_A+m_B}$. This implies that calculating the quantum value of an XOR game can be formulated as a semidefinite program $(\mathcal{P})$ [Weh06].

Theorem 3.2.2. *The optimal quantum bias, ϵ_q, of an* XOR *game with game matrix Φ is given by*

$$\epsilon_q = \begin{cases} \max & \operatorname{Tr} \Phi_s \mathcal{X} \\ s.t. & diag(\mathcal{X}) = |\mathbf{1}\rangle, \\ & \mathcal{X} \geq 0, \end{cases} \tag{3.13}$$

*where $diag(\mathcal{X})$ is a vector whose entries are the diagonal elements of matrix $\mathcal{X}$, $|\mathbf{1}\rangle$ is the all 1's vector, $\Phi_s = \begin{pmatrix} 0 & \frac{1}{2}\Phi \\ \frac{1}{2}\Phi^T & 0 \end{pmatrix}$ and $\mathcal{X} = \begin{pmatrix} A & S \\ S^T & B \end{pmatrix}$. S is the **strategy matrix** defined as $S_{x,y} = \langle u_x | v_y \rangle$. The matrices A, B with $A_{x,x'} = \langle u_x | u_{x'} \rangle$ and $B_{y,y'} = \langle v_y | v_{y'} \rangle$ represent local terms.*

Proof. Let us consider an XOR game with $|Q_A| = m_A$ questions for Alice, $|Q_B| = m_B$ questions for Bob, associated game matrix Φ, and winning condition determined by function $f(x, y)$. We have that

$$\epsilon = \sum_{x,y} p(x,y)(-1)^{f(x,y)} \left[P(a \oplus b = 0|x,y) - P(a \oplus b = 1|x,y) \right], \tag{3.14}$$

and for a quantum strategy where Alice and Bob perform the measurements $\{M_x^0, M_x^1\}$ and $\{M_y^0, M_y^1\}$, respectively, in a quantum state $|\psi\rangle$

$$P(a \oplus b = 0|x,y) - P(a \oplus b = 1|x,y) = \langle \psi | \mathbf{A}_x \otimes \mathbf{B}_y | \psi \rangle, \tag{3.15}$$

where $\mathbf{A}_x$ and $\mathbf{B}_y$ are defined as in Eq. (1.14). Hence

$$\epsilon = \sum_{x,y} p(x,y)(-1)^{f(x,y)} \langle \psi | \mathbf{A}_x \otimes \mathbf{B}_y | \psi \rangle. \tag{3.16}$$

Now we can define the vectors

$$\begin{aligned} |u_x\rangle &:= \mathbf{A}_x \otimes \mathbb{1} |\psi\rangle, \\ |v_y\rangle &:= \mathbb{1} \otimes \mathbf{B}_y |\psi\rangle, \end{aligned} \tag{3.17}$$

so that

$$\epsilon = \sum_{x,y} p(x,y)(-1)^{f(x,y)} \langle u_x | v_y \rangle. \tag{3.18}$$

Let

$$S := \sum_{x,y} \langle u_x | v_y \rangle |x\rangle\langle y|. \tag{3.19}$$

be the **strategy matrix** that represents this particular strategy. Together with the game matrix given by Eq. (3.10) we have that

$$\epsilon = \mathrm{Tr}\,\Phi S^T = \mathrm{Tr}\,\Phi^T S. \tag{3.20}$$

Now let us define the matrix whose columns are composed by the vectors $\{|u_x\rangle\}$ and $\{|v_y\rangle\}$:

$$X = \begin{pmatrix} |u_1\rangle & \dots & |u_{m_A}\rangle & |v_1\rangle & \dots & |v_{m_B}\rangle \end{pmatrix}, \tag{3.21}$$

and set $\mathcal{X} = X^\dagger X$. $\mathcal{X}$ is the so-called **Gram matrix** of the set of vectors $\{|u_x\rangle, |v_y\rangle\}$, and $\mathcal{X} = \begin{pmatrix} A & S \\ S^T & B \end{pmatrix}$. Note that if the vectors $\{|u_x\rangle, |v_y\rangle\}$ are normalized, all the diagonal elements of $\mathcal{X}$ are equal to 1. By defining $\tilde{\Phi}_s = \begin{pmatrix} 0 & \frac{1}{2}\Phi \\ \frac{1}{2}\Phi^T & 0 \end{pmatrix}$ we have

$$\mathrm{Tr}\,\tilde{\Phi}_s \mathcal{X} = \frac{1}{2}\mathrm{Tr}\,\Phi S^T + \frac{1}{2}\mathrm{Tr}\,\Phi^T S = \epsilon. \tag{3.22}$$

Finally, we use the fact that $\mathcal{X} \geq 0$ iff it is the Gram matrix of a set of vectors [HJ12], in order to guarantee that, for every feasible $\mathcal{X}$ in problem $(\mathcal{P})$, there exist a set of normalized vectors $\{|u_x\rangle\}$, $\{|v_y\rangle\} \in \mathbb{R}^N$, for some N. And by Tsirelson's theorem 3.2.1, each solution $\mathcal{X}$ can then be described by ± 1-observables applied to a quantum state $|\psi\rangle$. Which ends the proof. □

For a classical deterministic strategy, all vectors $|u_x\rangle$ and $|v_y\rangle$ are equal to $\pm|w\rangle$, for a single unit vector $|w\rangle$, since the expected values $\langle A_x B_y\rangle$ assume values ± 1. The strategy matrix S_c of a classical deterministic strategy is thus a matrix with ± 1 entries with all columns (and rows) being proportional to each other.

An upper bound to the quantum value of XOR games

We now show that the quantum value of an XOR game can be upper bounded by a quantity related to the spectral norm of the game matrix Φ.

Theorem 3.2.3. *Given a bipartite* XOR*-game, with m_A inputs for Alice, m_B inputs for Bob, and an associated game matrix Φ, the quantum value is upper bounded by*

$$\omega_q^{\oplus} \leq \frac{1}{2}\left(1 + \sqrt{m_A m_B}\|\Phi\|\right), \tag{3.23}$$

where $\|\Phi\|$ is the maximum singular value, or the spectral norm, of the matrix Φ.

Proof. We follow the approach of Ref. [LPSW07]. Given a bipartite XOR-game, $g^{\oplus}(f,p)$, its quantum value is given by

$$\omega_q = \max_{|\psi\rangle,\{\mathbf{A}_x\},\{\mathbf{B}_y\}} \frac{1}{2}\left(1+\sum_{x,y} p(x,y)(-1)^{f(x,y)} \langle\psi| \mathbf{A}_x \otimes \mathbf{B}_y |\psi\rangle\right). \tag{3.24}$$

Note that we have replaced the supremum of Eq. (3.4) by a maximum, since Tsirelson's Theorem 3.2.1 guarantees that the optimal quantum value for XOR games is always achieved by a quantum strategy (and even more, that this strategy involves a finite dimensional system).

Now let $|\psi'\rangle, \{\mathbf{A}'_x\}, \{\mathbf{B}'_y\}$ be the quantum state and observables corresponding to the optimal strategy for the game $g^{\oplus}(f,p)$, and let us define the unit vectors

$$|\alpha\rangle = \frac{1}{\sqrt{m_A}} \sum_{x=1}^{m_A} \mathbf{A}'_x \otimes \mathbb{1}_B \otimes \mathbb{1}_x |\psi'\rangle \otimes |x\rangle, \tag{3.25a}$$

$$|\beta\rangle = \frac{1}{\sqrt{m_B}} \sum_{y=1}^{m_B} \mathbb{1}_A \otimes \mathbf{B}'_y \otimes \mathbb{1}_y |\psi'\rangle \otimes |y\rangle. \tag{3.25b}$$

So that we have

$$\begin{aligned}\omega_q &= \frac{1}{2}\left(1+\sqrt{m_A m_B}\,\langle\alpha|\,\mathbb{1}_{AB}\otimes\Phi\,|\beta\rangle\right)\\ &\leq \frac{1}{2}\left(1+\sqrt{m_A m_B}\,\|\mathbb{1}_{AB}\otimes\Phi\|\right)\\ &= \frac{1}{2}\left(1+\sqrt{m_A m_B}\,\|\Phi\|\right).\end{aligned} \tag{3.26}$$

□

The bound (3.23) was also derived and studied in details in Ref. [EKB13], where the authors provide necessary and sufficient conditions for the bound to be tight. For the case of $m_A = m_B = m$, Theorem 3.2.3 can be derived from the dual $(\mathcal{D})$ of problem (3.13). One can show that $m\|\Phi\|$ is a feasible solution to the dual problem $(\mathcal{D})$, and hence, by the weak duality theorem 2.3.1, it is an upper bound on the quantum bias ϵ_q [Weh06] (see Appendix E.1).

No-signaling value of an XOR game

An XOR-game can always be won with certainty by a no-signaling strategy, *i.e.* $\omega^{\oplus}_{NS} = 1$.

In order to see that, consider the strategy defined by

$$P(a,b|x,y) := \begin{cases} \frac{1}{2} & \text{if } a \oplus b = f(x,y), \\ 0 & \text{otherwise.} \end{cases} \tag{3.27}$$

This strategy is no-signaling, because all the marginals are uniform

$$P(a|x) = P(b|y) = \frac{1}{2} \; \forall a,b,x,y, \tag{3.28}$$

and by construction it wins the game with certainty. The no-signaling boxes defined by Eq. (3.27) are the generalization of the PR-boxes (Eq. (1.19)), introduced in Chapter 1, for the case of more inputs per party.

3.3 Linear games

Another class of games that we are going to consider are the called **linear games**. They are a generalization of XOR games to a larger alphabet output size. Linear games constitute a particular case of a more general class of nonlocal games, the **unique games**.

Unique games have been extensively used in the study of hardness of approximation of some NP-complete problems, in attempts to identify the existence of polynomial time algorithms to approximate the optimal solution of the problem to within a constant factor [Hås01, KKMO07]. Unique games is the class of nonlocal games where for each pair of questions, (x,y), there is an associated permutation and the players win the game iff Bob's output corresponds to the permutation of Alice's output. Linear games constitute the particular case of unique games where all the associated permutations commute and therefore it can be defined in terms of an Abelian group $(G,+)$.

Definition 3.3.1. *A two-player linear game $g^{\ell}(G,f,p)$ is a nonlocal game where two players Alice and Bob receive questions x, y from sets Q_A and Q_B respectively, chosen from a probability distribution $p(x,y)$ by a referee. They reply with respective answers $a,b \in G$ where $(G,+)$ is a finite Abelian group with associated operation $+$. The winning condition of the game is defined by a function $f : Q_A \times Q_B \to G$, such that $V(a,b|x,y) = 1$ if $a+b = f(x,y)$ and 0 otherwise.*

Some concepts and formal definitions on groups are stated in Appendix C.

The average probability of success of the players in a linear game $g^{\ell}(G,f,p)$ can be written as

$$\omega(g^{\ell}) = \sum_{x,y} p(x,y) P(a+b = f(x,y)|x,y). \tag{3.29}$$

An XOR game can be seen as a linear game with $(G,+) = \mathbb{Z}_2$. We can also define the generalized XOR games, **XOR-d games**, denoted $g^{\oplus_d}$, as the class of linear games associated to the cyclic group $\mathbb{Z}_d$ (the set $[d] = \{0,\ldots,d-1\}$ with the operation of addition modulo d).

Perfect no-signaling strategy for linear games

The existence of a perfect no-signaling strategy that wins the game with probability 1 also holds for linear games. For every linear game $g^{\ell}(G,f,p)$ there exist a no-signaling strategy that perfectly wins the game:

$$\omega_{NS}(g^{\ell}) = 1. \tag{3.30}$$

Such a strategy is defined as

$$P(a,b|x,y) = \begin{cases} \frac{1}{|G|} & \text{if } a+b = f(x,y) \\ 0 & \text{otherwise.} \end{cases} \tag{3.31}$$

The strategy (3.31) clearly wins the game, and also it is no-signaling since all the marginals are fully random:

$$P(a|x) = \sum_b P(a,b|x,y) = \sum_b \frac{1}{|G|}\delta_{b,f(x,y)-a} = \frac{1}{|G|} \quad \forall\, y, \tag{3.32}$$

and analogously for $P(b|y)$.

3.4 n-player games

In this Section we present the generalization of the previous definitions for games with n players.

Definition 3.4.1 (n-player nonlocal Game)**.** *An n-player nonlocal game $g_n(V,p)$ is a cooperative task where n players $A_1,\ldots,A_n$, who are not allowed to communicate after the game starts, receive respectively questions $x_1,\ldots,x_n$, where $x_i \in Q_i$, chosen from a probability distribution $p(x_1,\ldots,x_n)$ by a referee. Upon receiving question x_i player A_i is supposed to answer $a_i \in \mathcal{O}_i$. The winning condition of the game is defined by a payoff function $V(a_1,\ldots,a_n|x_1,\ldots,x_n)$ which assumes value 1 to indicate when the players win and value 0 to indicate when they lose.*

The probability of success of the players for a particular strategy defined by the box $\vec{P}(a_1,\ldots,a_n|x_1,\ldots,x_n)$ is given by

$$\omega(g_n) = \sum_{\vec{a}\in\mathcal{O},\vec{x}\in Q} p(\vec{x})V(\vec{a}|\vec{x})P(\vec{a}|\vec{x}), \tag{3.33}$$

where $\vec{x} = (x_1, \ldots, x_n)$ denotes the input string, $Q = Q_1 \times \ldots \times Q_n$ and analogously for $\vec{a}$ and $\mathcal{O}$.

The definition of linear games can be straightforwardly generalized for an n-player game in the following way:

Definition 3.4.2. *An n-player linear game $g_n^\ell(G, f, p)$ is a nonlocal game where the players answer with $a_1, \ldots, a_n \in G$, where $(G, +)$ is a finite Abelian group with associated operation $+$, and the predicate function V only depends on the sum of the players outputs:*

$$V(\vec{a}|\vec{x}) = \begin{cases} 1\ , \ \textit{if } a_1 + \ldots + a_n = f(x_1, \ldots, x_n) \\ 0\ , \ \textit{otherwise} \end{cases} \tag{3.34}$$

for $f : Q \longrightarrow G$.

The probability of success of a particular strategy in a n-player linear game g_n^ℓ is given by

$$\omega(g_n^\ell) = \sum_{\vec{x} \in Q} p(\vec{x}) P(a_1 + \ldots + a_n = f(\vec{x})|\vec{x}). \tag{3.35}$$

The classical value of an n-player game

The classical value of an n-player nonlocal game $\omega_c(g_n)$ is obtained by an optimization over deterministic local strategies

$$\omega_c(g_n) = \max_{\left\{\vec{D}(a_i|x_i)\right\}} \sum_{\vec{a},\vec{x}} p(\vec{x}) V(\vec{a}|\vec{x}) D(a_1|x_1) \ldots D(a_n|x_n) \tag{3.36}$$

where $\vec{D}(a_i|x_i)$ represents a deterministic probability distribution.

The number of possible deterministic strategies also increases exponentially with the number of parties. For a game with n players, $|Q|$ questions per player and $|\mathcal{O}|$ outputs per question, the number of deterministic strategies is $|\mathcal{O}|^{n \times |Q|}$.

The quantum value of an n-player game

A general n-partite quantum strategy can be described by the players sharing an n-partite pure state $|\psi\rangle$ of arbitrary dimension and performing local measurements $\left\{M_{x_i}^{a_i}\right\}$ on it. The quantum value of the n-player game g_n is then given by

$$\omega_q(g_n) = \sup_{|\psi\rangle, \{M_{x_i}^{a_i}\}} \sum_{\vec{a},\vec{x}} p(\vec{x}) V(\vec{a}|\vec{x}) \left\langle \psi \right| M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_n}^{a_n} \left| \psi \right\rangle . \tag{3.37}$$

The case of multiplayer games is even more challenging than the bipartite case. For bipartite XOR games, we have seen that Tsirelson's theorem (Theorem 3.2.1) guarantees that the best performance of quantum players can be calculated exactly and efficiently using a semidefinite program, Eq. (3.13). For three players, even for the case of XOR games the quantum value is known to be NP-hard[6] to approximate [Vid13].

In chapter 5 we deal with bipartite XOR games and present results of Ref. [RKMH14] concerning games with no-quantum advantage and results on the Shannon capacity of XOR-game graphs. In Chapter 6 we provide an upper bound to the quantum value of a 2-player linear game and present results of Ref. [RAM16]. In Chapter 7 we generalize the results for n-player linear games presenting the results of Ref. [MRMT16].

[6] In terms of the number of possible questions.

Chapter 4

Graph theoretic approach to nonlocality

The graph theoretic approach to quantum correlations was introduced by Cabello, Severini and Winter [CSW10, CSW14] in the framework of contextuality scenarios[1], where Bell scenarios can be seen as a particular case of it. Further refinements to the particular case of nonlocality scenarios where made in Refs. [AFLS15, CMSS14, RDLT+14]. In this chapter, we will see how the classical, quantum, and no-signaling values of a Bell expression can be associated to graph parameters.

4.1 A bit of zero-error information theory

In 1956 Shannon [Sha56] studied the concept of zero-error capacity of a communication channel. The zero-error capacity C_0 is defined as the maximum rate at which it is possible to transmit information with zero probability of error through a channel $\mathcal{C}$.

A channel is described by a set of input letters $i \in \mathcal{I}$, a set of output letters $o \in \mathcal{O}$, and the transition probabilities $p_i(o)$ that represents the probability that an input i will generate an output o. In the analysis of zero-error capacity we are not interested in the particular values of the transition probabilities but only whether they are zero or not. In order to deal with the important properties of the zero-error capacity C_0, we can associate a graph $\mathcal{G}$ to the channel in

[1] In a contextuality scenario we do not necessarily have parties. The hypothesis in question is whether an observable $\mathbf{O}$ that belongs to two different sets of mutually commuting observables, called the **contexts**, $\mathbf{O} \in \mathcal{C}_1$ and $\mathbf{O} \in \mathcal{C}_2$, can have a description independent of the context. In a Bell scenario the commutation of observables that form each context is guaranteed by the tensor product structure of the parties' experiments.

consideration.

Definition 4.1.1 (Confusability Graph)**.** *The confusability graph associated to a channel $\mathcal{C}$ is a graph $\mathcal{G}(V, E)$ where each input letter of the channel corresponds to a vertex*

$$V = \{i \,|\, i \in \mathcal{I}\}, \tag{4.1}$$

and there is an edge connecting two vertices i and j if these inputs can be confused by the channel

$$\{i, j\} \in E \;\; \textit{iff} \;\; \exists\, o \in \mathcal{O} \;\; s.t. \;\; p_i(o) \neq 0 \;\; \textit{and} \;\; p_j(o) \neq 0. \tag{4.2}$$

An alternative quantity that carries all the information contained in the graph $\mathcal{G}$ is the **adjacency matrix**.

Definition 4.1.2 (Adjacency Matrix)**.** *The adjacency matrix $[\mathcal{A}_{ij}]$ associated to a graph $\mathcal{G}(V, E)$ is defined as*

$$\mathcal{A}_{i,j} = \begin{cases} 1 & \textit{if } \{i, j\} \in E, \\ 0 & \textit{otherwise.} \end{cases} \tag{4.3}$$

The maximal number of 1-letter messages, $M_0(1)$, which can be sent through a channel $\mathcal{C}$ without confusion can be extracted directly from a graph invariant. A bit of thinking[2] leads us to conclude that $M_0(1)$ is equal to the independence number of the confusability graph $\mathcal{G}$:

$$M_0(1) = \alpha(\mathcal{G}). \tag{4.4}$$

The independence number of a graph is the cardinality of the maximal independent set, which is a subset of vertices such that none of which are adjacent . It is described by the optimization problem (2.23).

Formally, the zero-error capacity C_0 is defined as

$$C_0 = \sup_n \frac{1}{n} \log M_0(n), \tag{4.5}$$

where $M_0(n)$ is the largest number of n-letter messages that can be sent through the channel without confusion. The number of non-confusable n-letter messages is given by the independence number of the graph $\mathcal{G}^n$:

$$M_0(n) = \alpha(\mathcal{G}^n), \tag{4.6}$$

where $\mathcal{G}^n$ denotes the **strong product** of graph $\mathcal{G}$ with itself n times.

[2] Or maybe a few bits. But note that since the independence number picks the maximum number of vertices such that no two of which are adjacent, this represents the maximum number of letters such that none of them can be confused.

Definition 4.1.3. *The strong product $\mathcal{G} \boxtimes \mathcal{F}$ of graphs $\mathcal{G}$ and $\mathcal{F}$ is such that*

- $V(\mathcal{G} \boxtimes \mathcal{F}) = V(\mathcal{G}) \times V(\mathcal{F})$,
- $\{(u,u'),(v,v')\} \in E(\mathcal{G} \boxtimes \mathcal{F}) \Leftrightarrow \{u,v\} \in E(\mathcal{G})$ *and* $\{u',v'\} \in E(\mathcal{F})$.

In terms of a channel $\mathcal{C}$, Definition 4.1.3 captures the idea that two 2-letter words are confusable if they are confusable in the first and in the second letter.

So we have that

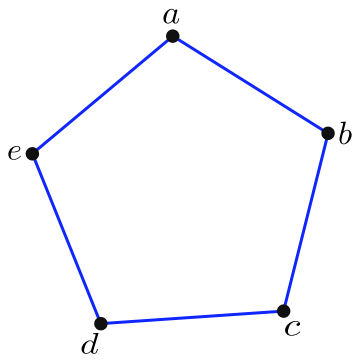
$$C_0 = \sup_n \frac{1}{n} \log \alpha(\mathcal{G}^n) := \log \Theta(\mathcal{G}), \tag{4.7}$$

where

$$\Theta(\mathcal{G}) = \sup_n \sqrt[n]{\alpha(\mathcal{G}^n)}. \tag{4.8}$$

From now on we refer to $\Theta(\mathcal{G})$ as the **Shannon capacity** of graph[3] $\mathcal{G}$.

As an example let us consider the channel with confusability graph given by the pentagon C_5:



The maximum number of 1-letter messages we could send through this channel without confusion is 2, and we have $\alpha(C_5) = 2$. We could for example send letter a or c. Now, considering 2-letter messages, we could obviously make the four non-confusable words: aa, ac, ca, and cc. However one can check that the following five words of size two: aa, bc, ce, db, ed, are such that no two

[3]The supremum in Eq. (4.5) can actually be replaced by a limit, since the strong product satisfies

$$\alpha(\mathcal{G}^2) \geq \alpha(\mathcal{G})^2, \tag{4.9}$$

which can be proved by noting that given an independent set A of graph $\mathcal{G}$, one can generate an independent set for $\mathcal{G}^2$ by taking (i,j) s.t. $i,j \in A$.

of them can be confused, and actually $\alpha(C_5{}^2) = 5$. Therefore, we conclude that $\Theta(C_5) \geq \sqrt{5}$.

In contrast to the ordinary channel capacity where a vanishing probability of error is allowed [Sha48] and the capacity can be efficiently calculate, it is not know whether the zero-error capacity is computable. By the definition given in Eq. (4.8), we have a supremum over n and at the moment there is no algorithm to decide the value of Θ in a finite number of steps for an arbitrary graph.

In 1979 Lovász [Lov79] introduced an efficiently computable upper bound to the Shannon capacity Θ (and therefore also for the independence number α). The Lovász number ϑ is a graph invariant defined as follows:

Definition 4.1.4 (Lovász Number)**.** *Consider an n-vertex graph $\mathcal{G}$. Let the set of vectors $(|v_1\rangle, \ldots, |v_n\rangle)$ be an orthonormal representation of $\bar{\mathcal{G}}$ and $|\psi\rangle$ be a unit vector. The Lovász number is given by*

$$\vartheta(\mathcal{G}) = \max_{\{|v_i\rangle\},|\psi\rangle} \sum_{i=1}^{n} \left(\langle\psi|v_i\rangle\right)^2. \tag{4.10}$$

An orthonormal representation of the complementary graph $\bar{\mathcal{G}}$ is a set of real vectors $(|v_1\rangle, \ldots, |v_n\rangle)$ associated to the vertices of graph $\mathcal{G}$ such that $\langle v_i|v_i\rangle = 1 \; \forall \, i$ and $\{i,j\} \in E \Rightarrow \langle v_i|v_j\rangle = 0$.

By calculating $\vartheta(C_5)$, Lovász proved [Lov79] that the previously known lower bound for the Shannon capacity of the pentagon, $\sqrt{5}$, is actually the exact value: $\Theta(C_5) = \sqrt{5}$.

There are many equivalent characterizations of the Lovász number [Lov09, Knu94], here we consider one that will be useful in Chapter 5:

Theorem 4.1.1 ([Lov79])**.** *Given a graph $\mathcal{G}$, consider the family of $n \times n$ symmetric matrices A such that*

$$A_{ij} = 1 \;\; \text{if} \;\; i = j \;\; \text{or} \;\; \{i,j\} \notin E. \tag{4.11}$$

The Lovász number is the minimum of the maximum eigenvalue of such matrices:

$$\vartheta(\mathcal{G}) = \min_{A} \lambda_{\max}(A). \tag{4.12}$$

Theorem 4.1.1 can be formulated as the semidefinite program (P):

$$(P) = \begin{cases} \min & t \\ \text{s.t.} & t\,\mathbb{1} - A \geq 0 \\ & A_{ij} = 1 \;\; \text{if} \;\; i = j \;\; \text{or} \;\; \{i,j\} \notin E \end{cases} \tag{4.13}$$

where $t\,\mathbb{1} - A \geq 0$ imposes that t is greater than or equal to the maximum eigenvalue of a symmetric matrix A satisfying (4.11), and the minimization picks the smallest of the maximum eigenvalues. Characterization (4.13) makes it clear (see Section 2.2) that the Lovász number can be efficiently determined.

4.2 The exclusivity graph

The graph theoretic approach to contextuality and nonlocality, that we call CSW approach, was first introduced in Ref.[CSW10] (and published later in Ref. [CSW14]). The idea is to associate with a given Bell scenario a graph called the **exclusivity graph**. The exclusivity graph has the vertices labeled by the events[4] of the particular Bell scenario $(a, b|x, y)$, and the edges connect vertices which correspond to exclusive events (*e.g.*, Alice measuring x and obtaining $a = 0$ is exclusive with any event where Alice measures the same x and obtains $a = 1$). The idea of the CSW approach is to take into account that the probabilities of exclusive events should sum up to no more than one.

Definition 4.2.1 (Exclusivity graph)**.** *The exclusivity graph associated to a Bell scenario is a graph $\mathcal{G}$ with vertices representing the possible events: $(a, b|x, y)$, and adjacencies defined by*

$$(a, b|x, y) \sim (a', b'|x', y') \Leftrightarrow (x = x' \ \wedge \ a \neq a') \ \vee \ (y = y' \ \wedge \ b \neq b'), \quad (4.14)$$

where $\wedge$ and $\vee$ denotes respectively the logical operations AND and OR.

Given a Bell scenario with boxes $\vec{P}(a, b|x, y)$, we denote a Bell expression by $\mathcal{S} = \left\{s^{a,b}_{x,y}\right\}$ such that its value for a particular box is given by $\mathcal{S}(\vec{P}) = \sum_{a,b,x,y} s^{a,b}_{x,y} P(a, b|x, y)$. Note that every Bell expression can be written with non-negative coefficients only[5], $s^{a,b}_{x,y} \geq 0$.

Now, given a Bell expression with positive coefficients $\mathcal{S}$, we can consider the **weighted exclusivity graph** $\mathcal{G}(\mathcal{S})$, where the weight $s^{a,b}_{x,y}$ is attributed to each vertex $(a, b|x, y)$ of the exclusivity graph $\mathcal{G}$. What is shown in the CSW approach [CSW14] is that the local, quantum and no-signaling values of a Bell expression $\mathcal{S}$, respectively $\mathcal{S}_c$, $\mathcal{S}_q$, and $\mathcal{S}_{NS}$, are related with invariants of the associated weighted exclusivity graph.

Theorem 4.2.1 ([CSW14])**.** *Given a Bell expression $\mathcal{S}$, and the weighted exclusivity graph $\mathcal{G}(\mathcal{S})$, it holds that*

$$\alpha(\mathcal{G}(\mathcal{S})) = \mathcal{S}_c \leq \mathcal{S}_q \leq \vartheta(\mathcal{G}(\mathcal{S})) \leq \mathcal{S}_{NS} = \alpha^*(\mathcal{G}(\mathcal{S})), \quad (4.15)$$

where $\alpha(\mathcal{G}(\mathcal{S}))$, $\vartheta(\mathcal{G}(\mathcal{S}))$, and $\alpha^*(\mathcal{G}(\mathcal{S}))$ are respectively the weighted independence number, the weighted Lovász number, and the weighted fractional packing number.

[4] By event $(a, b|x, y)$ we denote the occurrence of Alice measuring x and obtaining outcome a, and Bob measuring y and obtaining outcome b.

[5] One just has to use the normalization condition of probability distributions, $\sum_{a,b} P(a, b|x, y) = 1 \ \forall x, y$, in order to avoid the negative coefficients.

The graph invariants that appear in Theorem 4.2.1 are defined bellow.

Definition 4.2.2. *The weighted version of the independence number $\alpha(\mathcal{G}(\mathcal{S}))$, the Lovász number $\vartheta(\mathcal{G}(\mathcal{S}))$, and the fractional packing number $\alpha^*(\mathcal{G}(\mathcal{S}))$ of the weighted graph $\mathcal{G}(\mathcal{S})$ are defined by the following optimization problems:*

$$\alpha(\mathcal{G}(\mathcal{S})) = \begin{cases} \max & \sum_{i\in V} s_i\omega_i \\ s.t. & \omega_i + \omega_j \leq 1 \text{ if } \{i,j\} \in E \\ & \omega_i \in \{0,1\} \ \forall i \in V. \end{cases} \tag{4.16}$$

$$\vartheta(\mathcal{G}(\mathcal{S})) = \begin{cases} \max & \sum_{i\in V} s_i \left(\langle\psi|v_i\rangle\right)^2 \\ s.t. & \langle v_i|v_j\rangle = 0 \text{ if } \{i,j\} \in E \\ & \langle v_i|v_i\rangle = 1 \ \forall i \in V \\ & \langle\psi|\psi\rangle = 1. \end{cases} \tag{4.17}$$

$$\alpha^*(\mathcal{G}(\mathcal{S})) = \begin{cases} \max & \sum_{i\in V} s_i\omega_i \\ s.t. & \omega_i \geq 0 \ \forall i \in V \\ & \sum_{i\in K} \omega_i \leq 1 \ \ \forall \text{ clique } K \text{ of } \mathcal{G}(\mathcal{S}). \end{cases} \tag{4.18}$$

In order to understand Theorem 4.2.1, note that the weighted independence number (4.16) captures the idea that a deterministic probability ω_i is associated to vertex i, and therefore $\alpha(\mathcal{G}(\mathcal{S}))$ gives the classical value of a Bell inequality $\mathcal{S}$. Concerning the Lovász number (4.17), the term $\langle\psi|v_i\rangle^2$ can be interpreted as the probability resultant of a projective measurement (determined by the vector $|v_i\rangle$) in the quantum state $|\psi\rangle$. However note that no tensor product structure was imposed for these measurements and state, which justifies the upper bound $\mathcal{S}_q \leq \vartheta(\mathcal{G}(\mathcal{S}))$. For the fractional packing number (4.18), the constraint that $\sum_{i\in K}\omega_i \leq 1$ for all clique[6] K captures the no-signaling conditions (1.7) and normalization of the probabilities ($\sum_{a,b} P(a,b|x,y) = 1 \forall (x,y)$), and therefore it justifies $\mathcal{S}_{NS} = \alpha^*(\mathcal{G}(\mathcal{S}))$.

The weighted Lovász number (4.17) was introduced and studied in Ref. [Knu94], and it also admits an SDP characterization. The weighted independence number (4.16) is a $\{0,1\}$-integer program which is in general NP-complete, and the weighted fractional packing number[7] (4.18) is defined by an LP.

[6] A clique in the graph $\mathcal{G}$ is a subset of vertices $K \subseteq V$ such that every two vertices in K are adjacent.

[7] The fractional packing number is easy to determine once the cliques of the graph are known, however if this is not the case, the problem of finding the cliques of a graph is also NP-complete.

The CSW approach had great impact in the field of nonlocality and contextuality, allowing us to use techniques of combinatorics to derive many results in these fields (see for example [ATC14, CMSS14] and references therein). The CSW approach was further refined in Ref. [AFLS15] where the authors consider hypergraphs from which it is possible to extract information about the complete nonlocality/contextuality scenario, and not only about the Bell inequalities.

For contextuality it holds that given an exclusivity graph $\mathcal{G}$ there always exists a contextuality scenario and an inequality whose quantum value is equal to the Lovász number of the graph $\mathcal{G}$. This can be seen by the definition (4.10), where one can interpret the vectors $|v_i\rangle$ as projective measurements being performed on the quantum state $|\psi\rangle$. However for nonlocality, equality does not hold in general since the tensor product structure is not captured by the Lovász number. In Ref. [RDLT+14] the authors introduce the **exclusivity multigraph** with the aim to capture the structure presented in the nonlocality scenario. In the exclusivity multigraph, exclusive events are connected by colored edges, which make explicit if the exclusivity is due to Alice's measurement or due to Bob's measurement. They defined the **multigraph Lovász number** $\theta(\mathcal{G}(\mathcal{S}))$ which satisfies $\mathcal{S}_q = \theta(\mathcal{G}(\mathcal{S}))$ for some Bell inequality $\mathcal{S}$. Therefore, $\theta(\mathcal{G}(\mathcal{S}))$ is a quantity that may be uncomputable, but an hierarchy of SDPs (based on the NPA hierarchy [NPA08]) can be used to derive upper bounds on $\theta(\mathcal{G}(\mathcal{S}))$.

Part II

Results

Chapter 5

XOR games with no-quantum advantage and the Shannon capacity of graphs

In this chapter we present results of Ref. [RKMH14]:

> *Characterizing the Performance of* XOR *Games and the Shannon Capacity of Graphs*
> R. Ramanathan, A. Kay, **G. Murta** and P. Horodecki
> **Phys. Rev. Lett., 113, 240401, (2014)**.

Our main result is to use insights from the field of nonlocality in order to derive a result in classical information theory. More specifically: We study the performance of quantum players in two-player XOR games, and we derive a set of necessary and sufficient conditions such that quantum players cannot perform any better than classical players. We then consider the exclusivity graph associated to an XOR game and examine its Shannon capacity. This allows us to specify new families of graphs for which the Shannon capacity can be determined.

5.1 Motivation

In Chapter 4 we have seen that, according to the CSW approach [CSW14], we can associate a weighted graph $\mathcal{G}(\mathcal{S})$ to a Bell inequality $\mathcal{S} = \left\{s_{x,y}^{a,b}\right\}$ such that the classical, quantum, and no-signaling values of $\mathcal{S}$ are related to graph invariants.

For an XOR game with m questions per player, uniformly chosen by the referee, $g^{\oplus}(f, \frac{1}{m^2})$, we can associate the non-weighted graph $\mathcal{G}$ which only contains

the vertices representing events satisfying the winning condition ($(a, b|x, y)$ s.t. $a \oplus b = f(x, y)$), and we have the relation

$$m^2\omega_c(g^{\oplus}) = \alpha(\mathcal{G}) \leq m^2\omega_q(g^{\oplus}) \leq \vartheta(\mathcal{G}). \tag{5.1}$$

At the same time we have seen that the confusability graph $\mathcal{G}$ associated to a classical channel $\mathcal{C}$ satisfies

$$\alpha(\mathcal{G}) \leq \Theta(\mathcal{G}) \leq \vartheta(\mathcal{G}). \tag{5.2}$$

In what concerns the Shannon capacity of a graph $\mathcal{G}$, very few classes of graphs are known for which $\Theta(\mathcal{G})$ has been established analytically. Among these classes are:

- perfect graphs[1]: have $\alpha(\mathcal{G}) = \alpha^*(\mathcal{G})$ (see [CDLTP13]).
- Kneser graphs[2] $KG_{n,k}$: satisfy $\alpha(KG_{n,k}) = \vartheta(KG_{n,k})$ [Lov79].
- vertex-transitive self-complementary graphs: satisfy $\Theta(\mathcal{G}) = \vartheta(\mathcal{G})$ [Lov79].
- König-Egerváry graphs[3]: satisfy $\alpha(\mathcal{G}) = \alpha^*(\mathcal{G})$ [Lar13].

In Section 5.4 we are going to discuss a bit more about some properties of these families of graphs. However we are not going to give any detailed presentation, but rather state only the properties that will be useful for our discussion. For the reader interested in learning more about graphs we refer to Ref. [Die10].

Note that, except for the vertex-transitive self-complementary graphs, all the classes satisfy $\alpha(\mathcal{G}) = \vartheta(\mathcal{G})$. And actually this constitutes a simple way to determine the Shannon capacity of a graph: to prove that $\alpha(\mathcal{G}) = \vartheta(\mathcal{G})$. From Eq. (5.1), we see that for an XOR-game exclusivity graph $\mathcal{G}$ this is only possible if $\omega_c(g^{\oplus}) = \omega_q(g^{\oplus})$. Our goal in this chapter is to characterize XOR games with no-quantum advantage, $\omega_c(g^{\oplus}) = \omega_q(g^{\oplus})$, and, with their corresponding graphs in hand, to study the value of $\vartheta(\mathcal{G})$.

[1] A graph is perfect if the chromatic number of every induced subgraph equals the size of the largest clique of that subgraph.

[2] Kneser graphs $KG_{n,k}$ are graphs whose vertices correspond to k-element subsets of a set of n elements ($S_i \subset \{1, \ldots, n\}$, $|S_i| = k\ \forall i$), and vertices i and j are adjacent $i \sim j \Leftrightarrow S_i \cap S_j = \emptyset$.

[3] A graph $\mathcal{G}$ is a König-Egerváry graph if it satisfies $\alpha(\mathcal{G}) + \nu(\mathcal{G}) = |V|$, where $\nu(\mathcal{G})$ is the maximum size of a matching (for the definition of a matching, see footnote 7).

5.2 XOR games and their graphs

Let us consider an XOR game $g^{\oplus}$ where each player receives one among m possible questions, $|Q_A| = |Q_B| = m$, chosen by the referee with probability $p(x,y)$. The associated game matrix (3.10) is given by

$$\Phi = \sum_{x,y\in[m]} (-1)^{f(x,y)} p(x,y) \, |x\rangle\langle y| \,, \tag{5.3}$$

where $a \oplus b = f(x,y)$ is the winning condition of the game, and $[m]$ denotes the set $\{1,\dots,m\}$.

If the referee choses questions with uniform distribution, $p(x,y) = \frac{1}{m^2}$, we can simply consider the non-normalized game matrix:

$$\tilde{\Phi} = \sum_{x,y\in[m]} \Phi_{xy} \, |x\rangle\langle y| \,, \tag{5.4}$$

where $\Phi_{xy} := (-1)^{f(x,y)}$.

Following the CSW approach [CSW14], every XOR game has an associated graph $\mathcal{G}$ [CMSS14, CSW14, AFLS15], where the vertices are the events $(a,b|x,y)$ that satisfy the winning condition[4] of the game (*i.e.* such that $a \oplus b = f(x,y)$), and the edges are determined by

$$(a,b|x,y) \sim (a',b'|x',y') \Leftrightarrow \big(x = x' \wedge a \neq a'\big) \vee \big(y = y' \wedge b \neq b'\big) \,. \tag{5.5}$$

Now, by making use of the winning relation $(-1)^{a\oplus b} = \Phi_{xy}$, we can parameterize the vertices of an XOR-game graph with only three parameters (x,y,a).

Definition 5.2.1. *The graph $\mathcal{G}(\Phi)$ associated to the XOR game with game matrix Φ consists of $2m^2$ vertices, which can be labeled as (x,y,a) where $x,y \in \{1,\dots,m\}$ and $a \in \{0,1\}$. Two vertices $(x,y,a),(x',y',a') \in V$ form an edge of the graph iff*

$$(x = x' \wedge a \neq a') \;\vee\; (y = y' \wedge (-1)^{a\oplus a'} \neq \Phi_{xy}\Phi_{x'y'}). \tag{5.6}$$

Some properties of the XOR-game graphs are given in the following proposition.

Proposition 5.2.1. *An XOR game-graph $\mathcal{G}(\Phi)$ has the following properties:*

- *$\mathcal{G}(\Phi)$ is $(2m-1)$-regular*[5].

[4] Note that we could include in the graph all the events $(a,b|x,y)$ and just give a weight zero to the ones that do not satisfy $a \oplus b = f(x,y)$.

[5] A graph $\mathcal{G}$ is said to be **k-regular** if every vertex has degree k, *i.e.* every vertex is connected to k other vertices.

- $\mathcal{G}(\Phi)$ *is triangle-free*[6].
- $\mathcal{G}(\Phi)$ *has perfect matching*[7].

Moreover, the adjacency matrix of $\mathcal{G}(\Phi)$ *can be expressed as*

$$\begin{aligned}\mathcal{A}(\mathcal{G}(\Phi)) =& \mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) \otimes \sigma_X + \tfrac{1}{2}|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m \otimes (\mathbb{1}_2 + \sigma_X) \\ & - \tfrac{1}{2}[D(|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m)D] \otimes (\mathbb{1}_2 - \sigma_X)\end{aligned} \tag{5.7}$$

where σ_X *is the Pauli-X matrix,* $|\mathbf{1}\rangle$ *is the all-ones vector* $|\mathbf{1}\rangle = \sum_{x\in[m]} |x\rangle$*, and the matrix* D *is defined as*

$$D = \sum_{x,y\in[m]} \Phi_{xy}|x,y\rangle\langle x,y|. \tag{5.8}$$

In order to see that an XOR-game graph $\mathcal{G}(\Phi)$ is $(2m-1)$-regular note that every vertex has m neighbors due to exclusivity with respect to Alice's measurement, and m neighbors due to exclusivity with respect to Bob's measurement, where one of these neighbors is exclusive due to both. Therefore, each vertex has $2m-1$ neighbors.

By taking two adjacent vertices $(x,y,a) \sim (x',y',a')$, a straightforward analysis shows that if there exists a third vertex (x'',y'',a'') which is adjacent to (x,y,a) and to (x',y',a') that would lead to a contradiction, hence there can be no triangle in $\mathcal{G}(\Phi)$.

A perfect matching for $\mathcal{G}(\Phi)$ is obtained by taking the edges corresponding to the same inputs for both parties $\{(x,y,0),(x,y,1)\}\ \forall x,y$.

Concerning the adjacency matrix (5.7), the first term, $\mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) \otimes \sigma_X$, accounts for the edges representing exclusivity only due to Alice's measurement since it corresponds to

$$\sum_{x,y,y',a} \left|xya\right\rangle\left\langle xy'(a\oplus 1)\right| - \sum_{x,y,a} \left|xya\right\rangle\left\langle xy(a\oplus 1)\right|. \tag{5.9}$$

The remaining terms, $\frac{1}{2}|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m \otimes (\mathbb{1}_2 + \sigma_X) - \frac{1}{2}[D(|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m)D] \otimes (\mathbb{1}_2 - \sigma_X)$, accounts for exclusivity due to Bob and due to both, and corresponds to:

$$\sum_{x,x',y,a,a'} \frac{1}{2}\left(1 - (-1)^{a\oplus a'}\Phi_{xy}\Phi_{x'y}\right)\left|xya\right\rangle\left\langle x'ya'\right|. \tag{5.10}$$

Finally we present the spectrum of the adjacency matrix, which will be very important in the proof of the main result of this chapter.

[6] A triangle is a set of three vertices such that all of them are connected. A graph is triangle-free if it has no subset of vertices forming a triangle.

[7] A **matching** in $\mathcal{G}$ is a set of edges such that no two of them have a vertex in common. A perfect matching is a matching that covers all the vertices of the graph.

Theorem 5.2.1. *The adjacency matrix of an* XOR*-game graph* $\mathcal{G}(\Phi)$*,* $\mathcal{A}(\mathcal{G}(\Phi))$*, has the following spectrum and corresponding degeneracies:*

$$spec(\mathcal{A}(\mathcal{G}(\Phi))) = \begin{cases} 2m-1 & \times 1 \\ m-1 & \times 2m-2 \\ -1 & \times (m-1)^2 \\ 1-m \pm \lambda_z & \times 1 \\ 1 & \times m(m-2) \end{cases} . \tag{5.11}$$

where λ_z *denotes the* m *singular values of* $\tilde{\Phi}$*.*

The proof of Theorem 5.2.1 is presented in Appendix E.

5.3 No-quantum advantage

We have seen in Chapter 1 that quantum mechanics can lead to the violation of Bell inequalities, contradicting the hypothesis of local realism (Definition 1.1.1). This fact opens the possibility to explore quantum systems in many tasks, going beyond what can be achieved with classical systems. In the framework of nonlocal games, quantum theory can make the players to succeed with higher probability. However, it is not only the tasks in which quantum theory brings advantage that are of interest. The tasks in which quantum systems can perform no better than classical systems also tell us something about nature. Most of the proposed principles to explain the set of quantum correlations were based on tasks where quantum theory brings no advantage, as for example the principle of **Information Causality** [PPK+09] and the principle of **Local Orthogonality** [FSA+13] (which was based on the guess your neighbor's input (GYNI) multiplayer game [ABB+10]). Another task which brings no quantum advantage, and also constitutes a class of XOR games, is the **Nonlocal Computation** (NLC) task investigated in Ref. [LPSW07].

Definition 5.3.1 (Nonlocal computation)**.** *Consider that the referee picks a string of* n *bits* $\vec{z} = (z_1, \ldots, z_n)$ *with an arbitrary probability distribution* $p(\vec{z})$*, and for each bit* z_i *he chooses randomly* x_i *and* y_i *such that* $z_i = x_i \oplus y_i$*. Then the referee gives the input bit string* $\vec{x} = (x_1, \ldots, x_n)$ *for Alice and* $\vec{y} = (y_1, \ldots, y_n)$ *for Bob. Upon receiving their inputs, Alice and Bob give respective binary outputs* a *and* b*. Their goal is to satisfy the winning condition*

$$a \oplus b = f(\vec{z}) = f(x_1 \oplus y_1, \ldots, x_n \oplus y_n) \tag{5.12}$$

for an arbitrary function $f(\vec{z})$*.*

The constraint that the function f depends only on the bits z_i, which are distributed between Alice and Bob by the relation $x_i \oplus y_i = z_i$, gives to this game the interpretation of a distributed computation of function f (nonlocal computation). Moreover, given a string $\vec{z}$, the referee chooses with uniform distribution, among the x_i's and y_i's that satisfy $z_i = x_i \oplus y_i$, *i.e.*

$$p(\vec{x}, \vec{y}) = \frac{1}{2^n} p(\vec{z}). \tag{5.13}$$

Therefore, even upon receiving their respective inputs Alice and Bob get no information about the string $\vec{z}$.

In Ref. [LPSW07], the authors have shown that no matter with which probability distribution the referee chooses among strings $\vec{z}$, the players sharing quantum resources cannot perform any better in the computation of function $f(\vec{z})$ than players with only classical resources. Interestingly enough, as this is an XOR game, there always exist a no-signaling strategy which can compute $f(\vec{z})$ perfectly. Given the lack of advantage even with the freedom of the referee's choice, and by the fact that more general probabilistic theories can perform this task perfectly, the **no-advantage for nonlocal computation** was also considered one of the principles to distinguish the quantum set of correlations.

It was known that the nonlocal computation inequalities, for 2-bit and 3-bit input strings, do not constitute facets of the local polytope [ABB+10], and recently it was proved that this is also the case for any number of inputs [RQS+17][8]. Therefore, all the non-local computation inequalities are faces of lower dimension. A facet defining Bell inequality with no-quantum advantage would also be a facet of the set of quantum correlations. It is an open problem whether there exist such facets in the set of bipartite quantum correlations (for multipartite scenarios the GYNI game constitutes facets of $\mathcal{Q}$ [ABB+10]).

5.4 Results

We now present the main results derived in Ref. [RKMH14].

XOR games with no quantum advantage

We are interested in characterizing XOR games which have the property of no quantum advantage. In the following we present a necessary and sufficient

[8] This result was derived before the conclusion of this Thesis, but the full work was completed and published only a few months later. However I am allowing myself to violate causality and include the journal reference here.

condition for $\omega_c = \omega_q$, and a very simple sufficient condition to guarantee no-quantum advantage.

Theorem 5.4.1. *Consider a two-party* XOR *game with game matrix* Φ *(with no all-zero row or column) for which* $S_c = |s^A\rangle\langle s^B|$ *represents the optimal classical strategy matrix. Let* $\Sigma = Diag(\{\langle i|\Phi|s^B\rangle\langle s^A|i\rangle\}_{i=1}^m)$ *and* $\Lambda = Diag(\{\langle i|s^B\rangle\langle s^A|\Phi|i\rangle\}_{i=1}^m)$. *There is no quantum advantage for* Φ *if and only if* $\Sigma, \Lambda > 0$ *and*

$$\rho(\Lambda^{-1}\Phi^T\Sigma^{-1}\Phi) = 1, \tag{5.14}$$

where $\rho(.)$ *denotes the spectral radius*[9].

Proof. We have seen in Chapter 3 that the quantum bias ϵ_q of an XOR game can be calculated by the semidefinite program $(\mathcal{P})$ (3.13):

$$\epsilon_q = \begin{cases} \max & \mathrm{Tr}\,\Phi_s\mathcal{X} \\ \text{s.t.} & \mathrm{diag}(\mathcal{X}) = |\mathbf{1}\rangle \oplus |\mathbf{1}\rangle, \\ & \mathcal{X} \geq 0. \end{cases} \tag{5.15}$$

where $\mathrm{diag}(\mathcal{X})$ is a vector whose entries are the diagonal elements of matrix $\mathcal{X}$, $\Phi_s = \begin{pmatrix} 0 & \frac{1}{2}\Phi \\ \frac{1}{2}\Phi^T & 0 \end{pmatrix}$ and $\mathcal{X} = \begin{pmatrix} A & S \\ S^T & B \end{pmatrix}$. S is the strategy matrix, $S_{x,y} = \langle u_x|v_y\rangle$, and A, B are local terms, $A_{x,x'} = \langle u_x|u_{x'}\rangle$ and $B_{y,y'} = \langle v_y|v_{y'}\rangle$.

By the Lagrange duality theory, the bias can be bounded from above by a feasible solution of the Lagrange dual problem $(\mathcal{D})$. The application of Lagrange duality, presented in Section 2.3, leads us to:

$$(\mathcal{D}) \begin{cases} \min & \sum_{i=1}^{2m} y_i \\ \text{s.t.} & \mathrm{Diag}(y) \geq \Phi_s. \end{cases} \tag{5.16}$$

where the y_i are $2m$ variables and $\mathrm{Diag}(y)$ denotes the diagonal matrix with entries y_i.

Problem $(\mathcal{P})$ satisfies strong duality (Theorem 2.3.2) since $\mathcal{X} = \mathbb{1}$ is a strictly feasible point and, therefore, Slater's conditions (2.22) are satisfied. As such, we need to derive the conditions under which the solution of $(\mathcal{D})$ (5.16) achieves the classical value $\langle s^B|\Phi|s^A\rangle$, which may also be written as $\langle s^s|\Phi_s|s^s\rangle$, for $|s^s\rangle = |s^A\rangle \oplus |s^B\rangle$ being the direct sum of vectors $|s^A\rangle$ and $|s^B\rangle$. So we require that

$$\mathrm{Tr}\left((\mathrm{Diag}(y) - \Phi_s)|s^s\rangle\langle s^s|\right) = 0. \tag{5.17}$$

[9]The spectral radius is the maximum eigenvalue in modulus of a matrix.

By the semi-definite condition $\mathrm{Diag}(y) - \Phi_s \geq 0$, this means that $|s^s\rangle$ is an eigenvector, with zero eigenvalue, of $\mathrm{Diag}(y) - \Phi_s$:

$$\mathrm{Diag}(y)\,|s^s\rangle = \Phi_s\,|s^s\rangle\,. \tag{5.18}$$

Now, since $|s^s\rangle$ is a vector of ± 1 entries (as it corresponds to a classical deterministic strategy), we have that

$$\langle i|\,\mathrm{Diag}(y)\,|s^s\rangle\,\langle s^s|i\rangle = y_i([s^s]_i)^2 = y_i. \tag{5.19}$$

Therefore, an element by element comparison in Eq. (5.18) gives us

$$\langle i|\,\mathrm{Diag}(y)\,|s^s\rangle\,\langle s^s|i\rangle = \langle i|\,\Phi_s\,|s^s\rangle\,\langle s^s|i\rangle\,, \tag{5.20}$$

from which we can derive that whenever a classical strategy achieves the optimal quantum value, we have:

$$\mathrm{Diag}(y) = \begin{pmatrix} \frac{1}{2}\Sigma & 0 \\ 0 & \frac{1}{2}\Lambda \end{pmatrix}. \tag{5.21}$$

The constraint $\mathrm{Diag}(y) \geq \Phi_s$ can be rewritten as $\left(\begin{smallmatrix} \Sigma & -\Phi \\ -\Phi^T & \Lambda \end{smallmatrix}\right) \geq 0$. And since Φ has no all-zero row or column, this condition is satisfied only if $\Sigma, \Lambda > 0$ (see observation 7.1.10 in Ref. [HJ12]). Theorem 7.7.9 in Ref. [HJ12] states that in these conditions

$$\begin{pmatrix} \Sigma & -\Phi \\ -\Phi^T & \Lambda \end{pmatrix} \geq 0 \Leftrightarrow \rho(\Phi^T\Sigma^{-1}\Phi\Lambda^{-1}) \leq 1. \tag{5.22}$$

Finally, when the optimal solution of the dual problem is given by the classical strategy, the inequality on the LHS of Eq. (5.22) is saturated. Therefore, condition $\rho(\Phi^T\Sigma^{-1}\Phi\Lambda^{-1}) \leq 1$ can be replaced by equality. □

When $S_c = S_c^T$ and $\Phi = \Phi^T$, the condition of Theorem 5.4.1 reduces to $\Sigma > 0$ and $\rho(\Sigma^{-1}\Phi) = 1$.

Corollary 5.4.1. *If the (non-normalized) singular vectors corresponding to the maximum singular value of Φ can be written with entries ± 1, then there is no quantum advantage for players of the game Φ.*

Proof. Let the (unnormalised) maximum singular vectors with ± 1 elements be $|\lambda^A\rangle$ and $|\lambda^B\rangle$ such that $\langle\lambda^A|\,\Phi\,|\lambda^B\rangle = \lambda m$, where λ is the maximum singular value of Φ and m is the square of the norm of $|\lambda^A\rangle$. In this case, $S_c = |\lambda^A\rangle\langle\lambda^B|$. Then $\Phi S_c^T = \lambda|\lambda^A\rangle\langle\lambda^A|$ such that $\Sigma = \Lambda = \lambda\mathbb{1}$. Evidently, these are positive and

$$\rho(\Phi^T\Sigma^{-1}\Phi\Lambda^{-1}) = \frac{1}{\lambda^2}\rho(\Phi^T\Phi) = 1. \tag{5.23}$$

□

This is only a sufficient condition and not a necessary one. For example, the maximum eigenvector of

$$\Phi_{ex} = \frac{1}{16}\begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{5.24}$$

does not consist of ± 1 elements, and yet it can be verified that $\omega_q(\Phi_{ex}) = \omega_c(\Phi_{ex}) = \frac{7}{8}$.

Examples of no-quantum advantage

Corollary 5.4.1 gives us a simple way to construct games with no quantum advantage. In the uniform probability case, it suffices to construct any symmetric matrix $\Phi \in \{\pm 1\}^{m\times m}$ for which the total of every row is the same, and at least $\frac{1}{2}m$, which ensures that the all 1's vector $|\mathbf{1}\rangle$ is a maximum eigenvector.

The NLC game (Definition 5.3.1) is a trivial example of Corollary 5.4.1 because the associated game matrix Φ_{NLC} is diagonal in the Hadamard basis for any number of input bits [LPSW07]. So now we address the question posed in Ref. [LPSW07]: *'Finding families of* XOR *games that differ from NLC, but with no quantum advantage'*. Let us consider an anti-circulant matrix[10] Φ, then for any m, $|\mathbf{1}\rangle$ is an eigenvector, and if m is even, so is the alternating signs vector. All we have to do is to restrict the matrix elements to guarantee that one of these two eigenvectors yields the eigenvalue of maximum modulus. For $m = 4$, let $(\gamma_0, \gamma_1, \gamma_2, \gamma_3)$, subject to $\sum_i |\gamma_i| = \frac{1}{4}$, specifies the first row of Φ. If

$$\max\left(\left(\sum_{i=0}^{3}\gamma_i\right)^2, \left(\sum_{i=0}^{3}\gamma_i(-1)^i\right)^2\right) \geq (\gamma_0-\gamma_2)^2 + (\gamma_1-\gamma_3)^2, \tag{5.25}$$

we have a game for which there is no quantum advantage. A sufficient condition for this to happen is that

$$\gamma_0\gamma_2 + \gamma_1\gamma_3 \geq 0. \tag{5.26}$$

Many different patterns for the probability distribution satisfy condition (5.26), as for example

$$\Phi = \begin{pmatrix} p & q & q & -p \\ q & q & -p & p \\ q & -p & p & q \\ -p & p & q & q \end{pmatrix}, \tag{5.27}$$

[10] An anti-circulant matrix is a matrix where each row has the same elements, but shifted one position to the left, with respect to the previous row.

where $|p| + |q| = 1/8$ and $p, q \in \mathbb{R}$. Which leads to matrices that (except for the uniformly distributed case) are not diagonal in the Hadamard basis.

In order to construct a new families of games with no quantum advantage, we can base on the following observation:

($*$) If Φ^1 and Φ^2 are two game matrices satisfying Corollary 5.4.1, then it follows that $\Phi^1 \otimes \Phi^2$ also satisfies Corollary 5.4.1.

This observation allows us to extend any examples for small input size to examples with an arbitrarily large number of inputs.

Actually observations ($*$) can be extended for any two games satisfying Theorem 5.4.1 by the additivity property of the quantum value of these games. In Ref. [CSUU08], it was shown that the quantum value of XOR games satisfy additivity: Consider two XOR games $g_1^{\oplus}(f_1, p_1)$ and $g_2^{\oplus}(f_2, p_2)$, the sum of these games is the XOR game

$$g_{1+2}^{\oplus}(f_1 \oplus f_2, p_1 p_2), \tag{5.28}$$

where the referee picks questions $((x_1, x_2), (y_1, y_2)) \in (Q_{A_1} \times Q_{A_2}) \times (Q_{B_1} \times Q_{B_2})$ with probability $p_1(x_1, y_1)p_2(x_2, y_2)$ and the winning condition of the game is defined by

$$a \oplus b = f_1(x_1, y_1) \oplus f_2(x_2, y_2). \tag{5.29}$$

The game is said to be additive if the optimal strategy is achieved when the players play each game individually and Alice outputs bit $a = a_1 \oplus a_2$ and Bob outputs bit $b = b_1 \oplus b_2$. The classical value does not satisfy additivity in general, however the quantum value does [CSUU08]. And the game matrix of game $g_{1+2}^{\oplus}(f_1 \oplus f_2, p_1 p_2)$ is the tensor product of the individual game matrices $\Phi(g_1^{\oplus}) \otimes \Phi(g_2^{\oplus})$.

Shannon capacity of game graphs

Game graphs for which $\omega_c = \omega_q$ are good candidates to have a Shannon capacity $\Theta(\mathcal{G}) = \alpha(\mathcal{G})$. We now prove that it is the case for games $g^{\oplus}(f, \frac{1}{m^2})$ satisfying the hypothesis of Corollary 5.4.1.

Theorem 5.4.2. *Every two-party* XOR *game with m uniformly chosen inputs for each party and satisfying the hypothesis of Corollary 5.4.1 has a game graph for which $\Theta(\mathcal{G}) = \alpha(\mathcal{G})$.*

Proof. To establish the Shannon capacity, our strategy is to find both $\alpha(\mathcal{G})$ and $\vartheta(\mathcal{G})$, and to show that they are equal. $\alpha(\mathcal{G})$ is straightforward, it coincides with the optimal strategy, and by Corollary 5.4.1 it is specified by the maximum singular value[11] of $\tilde{\Phi}$:

$$\alpha(\mathcal{G}) = m^2\omega_c = \tfrac{1}{2}m(m + \|\tilde{\Phi}\|). \tag{5.30}$$

In order to compute $\vartheta(\mathcal{G})$, we use the characterization of the Lovász number given by Theorem 4.1.1 [Lov79], in which $\vartheta(\mathcal{G})$ is upper bounded by the largest eigenvalue of any symmetric matrix $(A_{i,j})_{i,j=1}^{N}$ such that

$$A_{ij} = 1 \;\text{ if }\; i = j \;\text{ or }\; \{i,j\} \notin E. \tag{5.31}$$

Our goal is to find a symmetric matrix A whose maximum eigenvalue matches $\alpha(\mathcal{G})$ and since $\alpha(\mathcal{G}) \leq \Theta(\mathcal{G}) \leq \vartheta(\mathcal{G})$ we would finish the proof.

Consider the matrix

$$A := |\mathbf{1}\rangle\langle\mathbf{1}| \otimes |\mathbf{1}\rangle\langle\mathbf{1}| \otimes (\mathbb{1} + \sigma_X) + a\mathcal{A}(\mathcal{G}) + b\mathbb{1} \otimes \mathbb{1} \otimes \sigma_X. \tag{5.32}$$

The matrix A satisfies the conditions (5.31), and moreover, all of the three terms in A commute with each other. Therefore, the diagonalization is the same as for the adjacency matrix $\mathcal{A}(\mathcal{G})$, and the eigenvalues can be readily obtained: (see proof of Theorem 5.2.1 in Appendix E):

$$\operatorname{spec}(\mathcal{A}(\mathcal{G}(\Phi))) = \begin{cases} 2m^2 + a(2m-1) + b & \times 1 \\ 2m + a(m-1) + b & \times 2m-2 \\ -a + b & \times (m-1)^2 \\ a(1 - m \pm \lambda_z) - b & \times 1 \\ a - b & \times m(m-2) \end{cases}. \tag{5.33}$$

It is now our task to select a, b such that the largest eigenvalue is $\alpha(\mathcal{G})$. If we set $a = -m$ and $b = \alpha(\mathcal{G}) - m$, this yields a maximum eigenvalue equal to $\alpha(\mathcal{G})$. We conclude then that $\alpha(\mathcal{G}) = \vartheta(\mathcal{G})$, and therefore $\Theta(\mathcal{G}) = \alpha(\mathcal{G})$. □

This proof automatically covers all NLC games, but also includes many other XOR games (Eq. (5.27), for example). A further consequence that follows from the proof of Theorem 5.4.2 is that whenever $\omega_q = \frac{1}{2}(1 + \frac{1}{m}\|\Phi\|)$, we know that $m^2\omega_q = \vartheta(\mathcal{G})$. The CHSH game [CHSH69] is an example of this.

[11] In terms of the normalized game matrix Φ we have $\omega_c = \frac{1}{2}(1 + m\|\Phi\|)$. Note, however, that we are using the unnormalized game matrix $\tilde{\Phi}$.

Previously known families of graphs with $\Theta(\mathcal{G}) = \alpha(\mathcal{G})$

We now come back to the previously known families of graphs for which the Shannon capacity is equal to the independence number, and we compare it with the graphs specified by Theorem 5.4.2:

- For **Perfect graphs**, it was shown in Ref. [CDLTP13] that the classical value coincides with the no-signalling value of any Bell expression associated to a perfect graph, this implies $\omega_c = 1$ for XOR games associated to perfect graphs.
- For **Kneser graphs** on n vertices it holds that [Lov79]

$$\vartheta(\mathcal{G}) = \frac{-n\lambda_{\min}}{\lambda_{\max} - \lambda_{\min}} \tag{5.34}$$

  where $\lambda_{\max\,/\,\min}$ are the corresponding maximum and minimum eigenvalues of the adjacency matrix. From Eq. (5.11), we have that

$$\lambda_{\min} = 1 - m - \|\tilde{\Phi}\| \quad \text{and} \quad \lambda_{\max} = 2m - 1, \tag{5.35}$$

  and from the hypothesis of Corollary 5.4.1 $\vartheta(\mathcal{G}) = \frac{1}{2}m\left(m + \|\tilde{\Phi}\|\right)$. So we have that in this case $\|\tilde{\Phi}\| = m$, which again implies $\omega_c = 1$.
- **König-Egerváry (KE) family** satisfies $\alpha(\mathcal{G}) + \nu(\mathcal{G}) = |V|$. Since the XOR game graphs have a perfect matching, $\nu(\mathcal{G}) = m^2$, they can only belong to the KE family in the case of $\alpha(\mathcal{G}) = m^2 \Rightarrow \omega_c = 1$.

So we see that the previously known families of graphs for which $\alpha(\mathcal{G}) = \vartheta(\mathcal{G})$ could only correspond to an XOR game in the trivial case where $\omega_c = 1$. Therefore the non-trivial XOR games satisfying Corollary 5.4.1 define new families of graphs for which $\alpha(\mathcal{G}) = \vartheta(\mathcal{G})$, the NLC class [LPSW07] being a remarkable example.

5.5 Discussion and open problems

We have presented a necessary and sufficient condition for a bipartite XOR game to have no quantum advantage. And with this characterization we could single out new families of games with no quantum advantage, even when the referee has some freedom in the probability of choosing the inputs. However, the generated examples (based on condition (5.26) and observation $(*)$) rely on ensuring that the optimal classical strategy coincides with the vectors of the

maximum singular value of the game matrix. It would be interesting to know whether there exists any such classes which do not require this condition.

We have also shown that for games satisfying the condition of Corollary 5.4.1, the associated graphs have $\Theta(\mathcal{G}) = \alpha(\mathcal{G})$. This is an entirely classical result derived as a consequence of insights provided from the study of quantum nonlocality. The proof of this result required Corollary 5.4.1 to hold. However, we believe that this restriction can be dropped, and that a necessary and sufficient condition for a game graph to have $\alpha(\mathcal{G}) = \vartheta(\mathcal{G})$ is given by Theorem 5.4.1. So far, the proof of this statement remains an open point.

A more challenging goal would be to prove similar results concerning no quantum advantage and the Shannon capacity of the corresponding graphs for games with more outputs and more players. However, the difficulty in extending the techniques used here relies mainly on the fact that there is no equivalent of Tsirelson's Theorem 3.2.1 for these more general scenarios. In Ref. [RAM16] we were able to find a generalization of the principle of no-advantage for nonlocal computation for a class of functions with d possible values. This result will be presented in the next Chapter.

Finally, we want to remark that relations (5.1) and (5.2) show that the quantum value of a Bell inequality and the Shannon capacity of the corresponding exclusivity graph are both bounded by the same graph parameters (α and ϑ). Moreover, as we have discussed previously, both quantities fall into the class of problems not known to be computable. We point out as an interesting question whether there is a fundamental relation between the quantum value of a Bell inequality and the Shannon capacity of the corresponding graph. In the affirmative case, the physical interpretation of this relation can shed light on foundational aspects of quantum theory.

Chapter 6

Linear games and the task of nonlocal computation

In this chapter we present results of Ref. [RAM16]:

> *Generalized* XOR *games with d outcomes and the task of nonlocal computation*
> R. Ramanathan, R. Augusiak, and **G. Murta**
> **Phys. Rev. A, 92, 022333 (2016)**.

We now focus on bipartite linear games, $g^{\ell}(G, f, p)$. Our main result is to prove an efficiently computable upper bound to the quantum value of a linear game. We then use the bound to derive, in a straightforward way, an upper bound to the quantum value of the CHSH-d game. We also show that boxes that would lead to trivialization of communication complexity are not realized in quantum theory. As the main application of the bound, we prove a larger alphabet generalization of the principle of no-advantage for nonlocal computation discussed in Section 5.3.

6.1 Motivation

As we have discussed in Chapters 2 and 3, it is not known, in general, whether the quantum value of a Bell inequality is computable or not (since there is a priori no restriction on the dimension of the Hilbert space for the quantum states and measurements). Only in some instances it is possible to compute the value efficiently, as it is the case for 2-player XOR games. Apart from this, typically the NPA hierarchy [NPA08] is used to get upper bounds to the quantum value. However, the quality of the approximation achieved by these bounds is

not known in general, and the size of these programs increases exponentially with the level of the hierarchy.

In Ref. [KRT10] it was shown that the quantum value of unique games can be efficiently approximated. Formally, the authors present an efficient algorithm such that, given a unique game with quantum value $\omega_q(g) = 1 - \epsilon$, it outputs a specific quantum strategy that achieves a value $\omega'(g) \geq 1 - 6\epsilon$. This remarkable result was very useful to prove parallel repetition for the quantum value of this class of games [KRT10]. However, this approximation is only good when the quantum value of the game is close to unity, which is not the case for simple examples like the CHSH-d game that we are going to discuss here.

Recently, there has been an increasing interest in developing applications of higher-dimensional entanglement (see, for example, [BPT00, MVWZ01, GJV+06, WLAR06, HP13, ECG+13]) for which Bell inequalities with more than two outcomes are naturally suited. Moreover, in Ref. [KC16] it was shown that, in general, d-chotomic measurements cannot be explained as a classical selection of intrinsically dichotomic measurements. Therefore, both for fundamental reasons as well as for these applications, the study of Bell inequalities with more outcomes is crucial.

6.2 An efficiently computable bound to the quantum value of linear games

Let us recall that a linear game $g^{\ell}(G, f, p)$ is defined by Alice and Bob answering with elements of an Abelian group $(G, +)$, $a, b \in G$, and the winning condition depending only on the group operation $+$ of their outputs (Definition 3.3.1). In order to obtain the main result of this Chapter, which is an upper bound to the quantum value of a linear game, we are going to make use of the Fourier transform on finite Abelian groups [Ter99] and introduce the **generalized correlators**.

Definition 6.2.1 (Generalized correlators)**.** *Let $a, b \in G$ be elements of a finite Abelian group $(G, +)$, where $+$ is the associated group operation. The generalized correlators $\langle A_x^i B_y^j \rangle$ are defined via the Fourier transform of the probabilities $P(a, b|x, y)$ as*

$$\langle A_x^i B_y^j \rangle = \sum_{a,b \in G} \bar{\chi}_i(a) \bar{\chi}_j(b) P(a, b|x, y), \tag{6.1}$$

where χ_i are the characters of the Abelian group $(G, +)$ and $\bar{\chi}_i$ is the conjugate character.

The characters of an Abelian group are complex numbers which satisfy the following relations (see Appendix C):

$$\begin{cases} \text{Homomorphism:} & \chi_i(a+b) = \chi_i(a)\chi_i(b) \ \ \forall a,b \in G \\ \text{Reflexivity:} & \bar{\chi}_i(a) = \chi_i(-a) \\ \text{Orthogonality:} & \sum_{a\in G} \chi_i(a)\bar{\chi}_j(a) = |G|\,\delta_{i,j} \end{cases} . \tag{6.2}$$

More details on groups and the Fourier transform on Abelian groups are presented in Appendix C (see also Ref. [Ter99]).

Given Definition 6.2.1, the probabilities are recovered by the inverse Fourier transform:

$$P(a,b|x,y) = \frac{1}{|G|^2} \sum_{i,j\in G} \chi_i(a)\chi_j(b)\langle A_x^i B_y^j\rangle. \tag{6.3}$$

And in terms of the correlators, normalization is expressed as

$$\langle A_x^e B_y^e\rangle = 1 \ \ \forall\ (x,y) \in Q_A \times Q_B. \tag{6.4}$$

The one-party correlators $\langle A_x^i\rangle$ are defined as

$$\langle A_x^i\rangle := \langle A_x^i B_y^e\rangle = \sum_{a,b\in G} \bar{\chi}_i(a)\bar{\chi}_e(b)P(a,b|x,y) = \sum_{a\in G} \bar{\chi}_i(a)P(a|x), \tag{6.5}$$

where e denotes the identity element of the group with χ_e being the trivial character ($\chi_e(b) = 1 \ \forall b \in G$) and we have used the no-signaling condition $\sum_{b\in G} P(a,b|x,y) = P(a|x)$. An analogous expression holds for $\langle B_y^j\rangle$.

In order to determine the success probability in a linear game, we are only interested in terms of the form $P(a+b = f(x,y)|x,y)$. Consequently, we can use the characters' properties in order to get a very simplified expression.

Lemma 6.2.1. *The average probability of success for a particular box $\vec{P}(a,b|x,y)$, in a linear game $g^\ell(G,f,p)$, can be written as*

$$\omega(g^\ell) = \sum_{x,y} p(x,y)\frac{1}{|G|}\left(1 + \sum_{k\in G\setminus\{e\}} \chi_k(f(x,y))\langle A_x^k B_y^k\rangle\right). \tag{6.6}$$

Proof. In order to prove the lemma we start by evaluating the probability:

$$\begin{aligned} P(a+b=f(x,y)|x,y) &= \sum_a P(a, f(x,y)-a|x,y) \\ &= \sum_a \frac{1}{|G|^2} \sum_{i,j\in G} \chi_i(a)\chi_j(f(x,y)-a)\langle A_x^i B_y^j\rangle \\ &= \frac{1}{|G|^2} \sum_{i,j\in G} \chi_j(f(x,y)) \left(\sum_a \chi_i(a)\chi_j(-a)\right) \langle A_x^i B_y^j\rangle \\ &= \frac{1}{|G|} \sum_{j\in G} \chi_j(f(x,y))\langle A_x^j B_y^j\rangle \end{aligned} \tag{6.7}$$

where we have used the characters' properties (6.2).

Finally, taking the average sum over the inputs x and y, and using normalization ($\langle A_x^e B_y^e\rangle = 1$), we have the desired result. □

Lemma 6.2.1 inspire us to define a set of $|G|-1$ game matrices associated to the linear game $g^\ell(G,f,p)$ which carry information about the probability distribution of the inputs and the winning condition of the game. These matrices are the analogue of the XOR game matrices, Eq. (3.10), to the case of linear games.

Definition 6.2.2 (Linear game matrices)**.** *Given a linear game $g^\ell(G,f,p)$, the associated game matrices are*

$$\Phi_k = \sum_{x,y} p(x,y)\chi_k(f(x,y))\,|x\rangle\langle y| \quad \textit{for} \quad k\in G\setminus\{e\}\,, \tag{6.8}$$

where $\{|x\rangle\}$ and $\{|y\rangle\}$ are orthonormal basis in $\mathbb{C}^{|Q_A|}$ and $\mathbb{C}^{|Q_B|}$ respectively.

Now, let us analyze the meaning of the generalized correlators for a quantum strategy. In a quantum strategy, local projective measurements $\{M_x^a\}$ and $\{M_y^b\}$ are performed by each player in a shared quantum state $|\psi\rangle$. Now if we define the (in general non-Hermitian) 'observables'

$$A_x^i = \sum_{a\in G} \bar{\chi}_i(a) M_x^a \quad \text{and} \quad B_y^j = \sum_{b\in G} \bar{\chi}_j(b) M_y^b, \tag{6.9}$$

we have that the generalized correlators correspond to:

$$\langle A_x^i B_y^j\rangle = \langle\psi|\, A_x^i \otimes B_y^j\,|\psi\rangle\,. \tag{6.10}$$

And therefore, the average success probability of a quantum strategy, specified by $\left\{\{M_x^a\}, \{M_y^b\}, |\psi\rangle\right\}$, is given by

$$\omega(g^\ell) = \frac{1}{|G|}\left(1 + \sum_{x,y} p(x,y) \sum_{k\in G\setminus\{e\}} \chi_k(f(x,y)) \langle\psi| A_x^k \otimes B_y^k |\psi\rangle\right). \tag{6.11}$$

Now we are ready to state the main result of this Chapter.

Theorem 6.2.1. *The quantum value of a linear game $g^\ell(G,f,p)$, with input sets Q_A and Q_B, can be bounded as*

$$\omega_q(g^\ell) \leq \frac{1}{|G|}\left(1 + \sqrt{|Q_A||Q_B|} \sum_{k\in G\setminus\{e\}} \|\Phi_k\|\right), \tag{6.12}$$

where Φ_k are the game matrices, χ_k are the characters of the group $(G,+)$, and $\|\Phi_k\|$ denotes the maximum singular value of matrix Φ_k (the spectral norm).

Proof. In order to derive the upper bound to $\omega_q(g^\ell)$, let us consider a quantum strategy given by the measurements $\{M_x^a\}$ and $\{M_y^b\}$, from which we derive the observables A_x^i and B_y^j, being applied to the pure state $|\psi\rangle$. Now, let us define the unit vectors:

$$\begin{aligned} |\alpha_k\rangle &= \sum_{x\in Q_A} \frac{1}{\sqrt{|Q_A|}} \left(A_x^{k\dagger} \otimes \mathbb{1}_B \otimes \mathbb{1}_x\right) |\psi\rangle \otimes |x\rangle, \\ |\beta_k\rangle &= \sum_{y\in Q_B} \frac{1}{\sqrt{|Q_B|}} \left(\mathbb{1}_A \otimes B_y^k \otimes \mathbb{1}_y\right) |\psi\rangle \otimes |y\rangle. \end{aligned} \tag{6.13}$$

By substituting into Eq. (6.11) we have

$$\begin{aligned} \omega_q(g^\ell) &= \sup_{\{|\alpha_k\rangle\},\{|\beta_k\rangle\}} \frac{1}{|G|}\left(1 + \sqrt{|Q_A||Q_B|} \sum_{k\in G\setminus\{e\}} \langle\alpha_k|\mathbb{1}_{AB} \otimes \Phi_k|\beta_k\rangle\right) \\ &\leq \frac{1}{|G|}\left(1 + \sqrt{|Q_A||Q_B|} \sum_{k\in G\setminus\{e\}} \|\mathbb{1}_{AB} \otimes \Phi_k\|\right) \\ &= \frac{1}{|G|}\left(1 + \sqrt{|Q_A||Q_B|} \sum_{k\in G\setminus\{e\}} \|\Phi_k\|\right), \end{aligned} \tag{6.14}$$

where the supremum in the first equation is taken over all vectors $\{|\alpha_k\rangle\}$ and $\{|\beta_k\rangle\}$ that can be expressed as in Eq. (6.13). □

The particular case of linear games corresponding to the cyclic group $\mathbb{Z}_d$ (the set $[d] = \{0, \ldots, d-1\}$ with the operation of sum modulo d) we denote by **generalized** XOR **games**, or simply XOR-d games. The characters of the cyclic group $\mathbb{Z}_d$ correspond to the d-th roots of unity $\chi_j(a) = \zeta^{ja}$, where $\zeta = \exp(2\pi \mathrm{i}/d)$. For an XOR-$d$, the Eq. (6.12) reduces to

$$\omega_q(g^{\oplus_d}) \leq \frac{1}{d}\left(1 + \sqrt{|Q_A||Q_B|}\sum_{k=1}^{d-1}\|\Phi_k\|\right), \tag{6.15}$$

with

$$\Phi_k = \sum_{x,y} p(x,y)\zeta^{kf(x,y)}\,|x\rangle\langle y|\,. \tag{6.16}$$

The computational complexity of our bound

Theorem 6.2.1 states an upper bound to the quantum value of linear games based on the spectral norm of the game matrices. Although we still do not know how good the bound is in general, it satisfies one of the requirements of a good relaxation: the bound is easy to compute.

The spectral norm of a matrix A, $\|A\|$, is equal to its maximum singular value. The singular value decomposition (SVD) of an $m \times n$ matrix A is the decomposition of A into the form

$$A = U\Sigma V^\dagger, \tag{6.17}$$

where

- U: is an $m \times m$ matrix whose columns are composed by a set of orthonormal vectors which are called the **left singular vectors** of A.
- V: is an $n \times n$ matrix whose columns are composed by a set of orthonormal vectors which are called the **right singular vectors** of A.
- Σ: is an $m \times n$ matrix with nonnegative elements in the principal diagonal, the **singular values of** A, and zero elsewhere.

Many algorithms are known for the singular value decomposition (see Ref. [GVL96]). The best known SVD algorithms have polynomial complexity in terms of the size of the matrices. If one is interested in determining only the singular values of an $n \times n$ matrix, there exists an algorithm with time complexity $T(n) = \mathcal{O}(n^3)$ [GVL96]. In a linear game $g^\ell(G, f, p)$ with d possible outcomes and m questions per player, we have $(d-1)$ $m \times m$ game matrices. Therefore the time complexity of computing our bound is $T(d, m) = \mathcal{O}(dm^3)$, which increases polynomially in the number of inputs and outputs.

6.3 Applications of the bound

The CHSH-d game

As a direct application of Theorem 6.2.1, we consider a d-output generalization, for d prime or power of a prime, of the CHSH game. The CHSH-d game is defined with the operations of sum and multiplication over the finite field $\mathbb{F}_d$ (For more details on finite fields see Appendix C.4).

Definition 6.3.1. *The CHSH-d game is a linear game with d inputs and d outputs per player, defined for d prime or power of a prime. In the CHSH-d game, Alice and Bob receive questions x and y and output answers a and b respectively, $a, b, x, y \in \mathbb{F}_d$, with the goal to satisfy*

$$a + b = x \cdot y \tag{6.18}$$

where $+$ and $\cdot$ are operations defined over the field $\mathbb{F}_d$.

Definition 6.3.1 is the generalization of the CHSH game for more outputs considered in Ref. [BS15]. Similar definitions were previously considered in Refs. [BM05, JLL+08, LLD09]. It is interesting to note that these games have recently found application in the security analysis of a relativistic bit commitment protocol [KTHW13].

In Ref. [BS15], an intensive study of this game was performed. The authors present results on the asymptotic classical and quantum values of the game. They also prove, for the first time, an upper bound on the quantum value of the CHSH-d game. Their proof is based on reducing these games to other information theoretic principles like no-advantage for nonlocal computation [LPSW07] and information causality [PPK+09]. We now apply Theorem 6.2.1 to re-derive in a different way the upper bound for the quantum value of the CHSH-d game obtained in Ref. [BS15].

Theorem 6.3.1 (see also [BS15])**.** *The quantum value of the CHSH-d game, for d prime or power of a prime, is upper bounded by*

$$\omega_q(\text{CHSH-}d) \leq \frac{1}{d} + \frac{d-1}{d\sqrt{d}}. \tag{6.19}$$

Proof. The proof follows from the explicit analysis of the game matrices for the CHSH-d game. For the CHSH-d game, the inputs are uniformly distributed and the winning condition is defined by $f(x, y) = x \cdot y$. Therefore the game matrices are:

$$\Phi_k = \sum_{x,y=0}^{d-1} \frac{1}{d^2} \chi_k(x \cdot y) \, |x\rangle\langle y| \tag{6.20}$$

where χ_k is the character of the additive group formed by the elements of the field $\mathbb{F}_d$.

Now we evaluate $\Phi_k^\dagger \Phi_k$ using the characters relations (6.2):

$$\begin{aligned}
\Phi_k^\dagger \Phi_k &= \frac{1}{d^4} \sum_{x,y=0}^{d-1} \sum_{x',y'=0}^{d-1} \bar{\chi}_k(x \cdot y) \chi_k(x' \cdot y') \, |y\rangle \langle x|x'\rangle \langle y'| \\
&= \frac{1}{d^4} \sum_{x,y=0}^{d-1} \sum_{y'=0}^{d-1} \chi_k(-x \cdot y) \chi_k(x \cdot y') \, |y\rangle\langle y'| \\
&= \frac{1}{d^4} \sum_{y,y'=0}^{d-1} \underbrace{\left(\sum_{x=0}^{d-1} \chi_k(x \cdot (y' - y)) \right)}_{d\delta_{y,y'}} |y\rangle\langle y'| \\
&= \frac{1}{d^3} \sum_{y=0}^{d-1} |y\rangle\langle y| \, .
\end{aligned} \tag{6.21}$$

Therefore $\Phi_k^\dagger \Phi_k = \mathbb{1}/d^3$, so that $\|\Phi_k\| = 1/d\sqrt{d}, \;\; \forall k \in \{1, \ldots, d-1\}$. Substitution into Eq. (6.15), with $|Q_A| = |Q_B| = d$, yields the desired result. □

Comparison with the numerical results of Ref. [LLD09] (see Table III in Ref. [LLD09]) indicates that the bound (6.19) is not tight in general[1] but might correspond to the value obtained for the first level of the NPA hierarchy. Note that in Ref. [LLD09] the authors only present the value attained at the first level of the hierarchy up to $d = 7$. This is probably due to the fact that the NPA hierarchy becomes impractical for dealing with Bell inequalities with high number of inputs and outputs, which shows that our simple bound can be very powerful for these cases.

No trivialization of communication complexity

We now address the question of whether there exist linear games that can be won perfectly with a quantum strategy, *i.e.* if there exist games $g^\ell(G, f, p)$ for which $\omega_q(g^\ell) = 1$. The interest in this question comes from communication complexity. In Ref. [vD13] it was shown that if Alice and Bob had unlimited access to PR-boxes (1.19), they could compute any distributed Boolean function with only one bit of communication. This result was later generalized [Wan11] to functions with d possible values. In Ref. [Wan11] it was shown that the called

[1] For $d = 3$, results of Ref. [LLD09] show that the optimal value is smaller than the bound (6.19). And moreover it is attained with the maximally entangled state of dimension 3.

functional boxes, which are no-signaling boxes that win perfectly some XOR-d games, would lead to a trivialization of communication complexity, where a distributed function could be computed with a single $d$it of communication (See Appendix D for more details).

The XOR-d games for which a perfect no-signaling strategy can trivialize communication complexity are the uniformly distributed total function games with the winning condition given by a non-additively-separable function. A total function game is one for which all inputs have a probability strictly greater than zero to be chosen by the referee, $p(x,y) > 0 \ \forall x,y$. And a function $f(x,y)$ is additively separable if it can be decomposed into the form $f(x,y) = f_1(x) + f_2(y)$.

We now make use of Theorem 6.2.1 to show that, for XOR-d games with uniformly chosen inputs, there is a quantum strategy that wins the game with probability one if and only if this game is trivial, *i.e.* when $\omega_c(g^{\oplus_d}) = 1$.

Theorem 6.3.2. *For XOR-d games $g^{\oplus_d}$ with m questions per player and uniformly distributed inputs, $p(x,y) = 1/m^2$, $\omega_q(g^{\oplus_d}) = 1$ iff $\omega_c(g^{\oplus_d}) = 1$.*

Proof. The constraint of uniformly distributed questions, $p(x,y) = 1/m^2$ for all (x,y), is equivalent to $\|\Phi_k\| \leq 1/m$ since both the maximum absolute value column sum and row sum of the matrix are equal to $1/m$. Hence, from our bound, Eq. (6.15), we have that

$$\omega_q(g^{\oplus_d}) = 1 \Rightarrow \|\Phi_k\| = \frac{1}{m} \ \forall k \in \{1,\ldots,d-1\}. \tag{6.22}$$

Now, let us consider the matrix $\Phi_1^\dagger \Phi_1$:

$$\left[\Phi_1^\dagger \Phi_1\right]_{y,y'} = \sum_{x=0}^{m-1} \frac{1}{m^4} \zeta^{-f(x,y)+f(x,y')}, \tag{6.23}$$

where $\zeta = \exp(2\pi \mathrm{i}/d)$. Let $|\lambda\rangle = (\lambda_0,\ldots,\lambda_{m-1})$ be an eigenvector corresponding to the maximum eigenvalue $1/m^2$ of $\Phi_1^\dagger \Phi_1$, with complex entries $\lambda_j = |\lambda_j| \zeta^{\theta_j}$. Assume, without loss of generality, that the entries of the eigenvector are ordered by absolute value, $|\lambda_0| \geq \cdots \geq |\lambda_{m-1}|$. From the eigenvalue equation corresponding to the first entry of $|\lambda\rangle$ we have

$$\sum_{x,y=0}^{m-1} |\lambda_y| \zeta^{-f(x,0)+f(x,y)+\theta_y} = m^2 |\lambda_0| \zeta^{\theta_0}. \tag{6.24}$$

Since $|\lambda_0| \geq |\lambda_j| \ \forall j$, the above equation can only be satisfied when

$$|\lambda_j| = |\lambda_0| \ \ \forall j \tag{6.25a}$$

$$f(x,y) - f(x,0) + \theta_y = f(x',y') - f(x',0) + \theta_{y'} \ \ \forall x,y,x',y' \tag{6.25b}$$

in particular choosing $x = x'$ we get

$$f(x,y) - f(x,y') = \theta_{y'} - \theta_y \ \forall x,y,y', \tag{6.26}$$

where all the operations are modulo d. With all $|\lambda_j|$ equal, the rest of the eigenvalue equations (for $j \neq 0$) lead to similar consistent constraint equations. We then deduce that $\omega_q(g^{\oplus_d}) = 1$ only when the columns of the game matrix Φ_1 are proportional to each other, the proportionality factor between columns y, y' being $\zeta^{f(x,y)-f(x,y')} = \zeta^{\theta_{y'}-\theta_y}$, and therefore the game matrix has rank$(\Phi_1) = 1$. Now consider a_0 and b_0 satisfying $a_0 + b_0 = f(0,0)$, by setting

$$a_x = f(x,0) - b_0 \tag{6.27}$$
$$b_x = b_0 + (\theta_0 - \theta_y) \tag{6.28}$$

we have a classical strategy that wins the game with probability 1. □

A more general result was recently proved in Ref. [RTHH16], showing that all the extremal points of the no-signaling polytope, in any Bell scenario, cannot be realized within quantum theory. Here, by a direct application of the norm bound (Theorem 6.2.1) we are able to exclude the quantum realization of those boxes corresponding to XOR-d games that would lead to trivialization of communication complexity.

6.4 XOR-d games and the task of nonlocal computation

In Section 5.3 we have introduced the principle of no-advantage for nonlocal computation proposed in Ref. [LPSW07], which corresponds to a class of XOR games for which $\omega_q(g^{\oplus}) = \omega_c(g^{\oplus})$. The question of the generalization of this class to a larger alphabet size was also left posed as an open question in Ref. [LPSW07]. Here we use Theorem 6.2.1 in order to characterize a class of XOR-d games, that resembles NLC, for which there is no quantum advantage.

Consider the following generalization of the non-local computation task to the computation of a particular function $f(z_1, \ldots, z_n)$ on n *dits*, $z_i \in \mathbb{F}_d$ for d prime.

Definition 6.4.1 (NLC_d)**.** *The generalized nonlocal computation of a d-nary function, NLC_d, for d prime, is the task where Alice and Bob each receives a n-dit string from a referee, $\vec{x}_n = (x_1, \ldots, x_n)$ and $\vec{y}_n = (y_1, \ldots, y_n)$, $\vec{x}_n, \vec{y}_n \in \mathbb{F}_d^n$, which obey $x_i + y_i = z_i$. They output respectively dits $a, b \in \mathbb{F}_d$ with the goal to satisfy*

$$a + b = h(\vec{x}_{n-1} + \vec{y}_{n-1}) \cdot (x_n + y_n), \tag{6.29}$$

for a previously agreed function $h : \mathbb{F}_d^{n-1} \times \mathbb{F}_d^{n-1} \longrightarrow \mathbb{F}_d$, *where* $+, \cdot$ *are sum and multiplication modulo* d. *Moreover, the input strings are chosen by the referee according to the distribution*

$$p(\vec{x}_n, \vec{y}_n) = \frac{1}{d^{n+1}} \tilde{p}(\vec{x}_{n-1} + \vec{y}_{n-1}) \tag{6.30}$$

for $\tilde{p}(\vec{z}_{n-1})$ *being an arbitrary probability distribution.*

We now prove that the games NLC_d, as defined above, exhibit no quantum advantage. The idea behind the proof is to show that the matrices $\Phi_k^\dagger \Phi_k$ for these games are diagonal in a basis composed of tensor products of the Fourier vectors of dimension d. We then present a classical strategy which achieves the quantum value, which is essentially given by the maximum singular vectors of Φ_1.

Theorem 6.4.1. *The games* NLC_d *for arbitrary prime* d *and input distribution satisfying* (6.30) *have no quantum advantage, i.e.,* $\omega_c(NLC_d) = \omega_q(NLC_d)$.

Proof. We first consider the case of uniformly chosen inputs. The games NLC_d consider functions of the following form

$$a + b = h(x_1 + y_1, \ldots, x_{n-1} + y_{n-1}) \cdot (x_n + y_n), \tag{6.31}$$

where $+$ and $\cdot$ are sum and multiplication modulo d, and h is an arbitrary function. Given the winning condition (6.31), the game matrices of NLC_d are composed of "building-block games" $g(t)$:

$$g(t) := \{a + b = t \cdot (x + y)\}, \tag{6.32}$$

with $t \in \{0, \ldots, d-1\}$, i.e., $f(x, y) = t \cdot (x + y)$.

There are d different games $g(t)$, each with a single $d$it input for each party (which we will take to be x_n and y_n). Every game $g(t)$ has the classical value $\omega_c(g(t)) = 1$. Explicitly, the classical strategy

$$a = t \cdot x \quad \text{and} \quad b = t \cdot y \tag{6.33}$$

wins the game $g(t)$ with probability one. The corresponding (non-normalized) game matrices $\tilde{\Phi}_k^{(1)}(t)$ for game $g(t)$ are given by

$$\tilde{\Phi}_k^{(1)}(t) := \sum_{x,y \in [d]} \zeta^{kt(x+y)} |x\rangle\langle y|, \tag{6.34}$$

with $\zeta = \exp(2\pi \mathrm{i}/d)$. Here the superscript (1) denotes that these matrices correspond to the NLC_d game matrices for $n = 1$.

Let us state some properties of the matrices $\tilde{\Phi}_k^{(1)}(t)$:

(i) $\tilde{\Phi}_k^{(1)}(t)^\dagger \tilde{\Phi}_k^{(1)}(t)$ for any k, t is diagonal in the Fourier basis defined by the Fourier vectors $|v_j\rangle$ with

$$|v_j\rangle = \left(1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(d-1)j}\right) \tag{6.35}$$

with $j \in \{0, \ldots, d-1\}$.

(ii) Each $\tilde{\Phi}_k^{(1)}(t)^\dagger \tilde{\Phi}_k^{(1)}(t)$ has only one eigenvalue (=d^2) different from zero and this corresponds to the eigenvector $|v_{d-k\cdot t}\rangle$.

Properties (i) and (ii) imply the orthogonality

$$\tilde{\Phi}_k^{(1)}(t)^\dagger \tilde{\Phi}_{k'}^{(1)}(t') = 0 \quad \text{for} \quad k \cdot t \neq k' \cdot t'. \tag{6.36}$$

Since, we will be concerned with finding the maximum singular vectors corresponding to a fixed k, we can encapsulate the above properties by the equation

$$\left(\tilde{\Phi}_k^{(1)}(t)^\dagger \tilde{\Phi}_k^{(1)}(t')\right) |v_j\rangle = d^2 \delta_{t,t'} \delta_{j,d-k.t} \, |v_j\rangle \, . \tag{6.37}$$

Now we use the properties of $\tilde{\Phi}_k^{(1)}(t)$ in order to analyze the game matrices $\tilde{\Phi}_k^{(n)}$ for the general NLC_d games with n-$d$its strings of input. Due to the structure of the function in Eq. (6.29), namely the fact that the winning condition depends only on the $d$it-wise sum of the n dits, and moreover the dependence on the last $d$its, x_n, y_n, is given by the games $g(n)$, we see that $\tilde{\Phi}_k^{(n)\dagger} \tilde{\Phi}_k^{(n)}$ acquires a block circulant structure (for $1 \leq i \leq n$ the corresponding matrices $\tilde{\Phi}_k^{(i)\dagger} \tilde{\Phi}_k^{(i)}$ for each k are block-wise circulant matrices). For example, if for $n = 2, d = 3$ an unnormalized game matrix $\tilde{\Phi}^{(2)}$ has the form

$$\tilde{\Phi}^{(2)} := \begin{array}{|c|c|c|} \hline \tilde{\Phi}^{(1)}(0) & \tilde{\Phi}^{(1)}(1) & \tilde{\Phi}^{(1)}(2) \\ \hline \tilde{\Phi}^{(1)}(1) & \tilde{\Phi}^{(1)}(2) & \tilde{\Phi}^{(1)}(0) \\ \hline \tilde{\Phi}^{(1)}(2) & \tilde{\Phi}^{(1)}(0) & \tilde{\Phi}^{(1)}(1) \\ \hline \end{array} \tag{6.38}$$

with $\tilde{\Phi}^{(1)}(t)$ defined as in Eq. (6.34), we would have $\tilde{\Phi}^{(2)\dagger} \tilde{\Phi}^{(2)}$ equals to

$$\tilde{\Phi}^{(2)\dagger} \tilde{\Phi}^{(2)} = \begin{array}{|c|c|c|} \hline \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i) & \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i+1) & \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i+2) \\ \hline \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i+2) & \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i) & \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i+1) \\ \hline \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i+1) & \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i+2) & \sum_i \tilde{\Phi}^{(1)}(i)^\dagger \tilde{\Phi}^{(1)}(i) \\ \hline \end{array} \tag{6.39}$$

which is a block-wise circulant matrix. In general, the entries of $\tilde{\Phi}_k^{(n)\dagger}\tilde{\Phi}_k^{(n)}$ are explicitly given by

$$\left[\tilde{\Phi}_k^{(n)\dagger}\tilde{\Phi}_k^{(n)}\right]_{\vec{x}_{n-1},\vec{y}_{n-1}} = \sum_{u_1,\ldots,u_{n-1}=0}^{d-1} \tilde{\Phi}_k^{(1)}(h(\vec{x}_{n-1}+\vec{u}_{n-1}))^{\dagger}\tilde{\Phi}_k^{(1)}(h(\vec{u}_{n-1}+\vec{y}_{n-1})). \tag{6.40}$$

Due to this block circulant structure, we have that $\tilde{\Phi}_k^{(n)\dagger}\tilde{\Phi}_k^{(n)}$ for any n and k is diagonal in the basis formed by the tensor products of the Fourier vectors $\{|v_{i_1}\rangle \otimes \ldots \otimes |v_{i_n}\rangle\}$ with $i_1, \ldots, i_n \in \{0, \ldots, d-1\}$.

We now proceed to find the eigenvector corresponding to the maximum eigenvalue of $\tilde{\Phi}_k^{(n)\dagger}\tilde{\Phi}_k^{(n)}$ among the basis formed by $\{|v_{i_1}\rangle \otimes \ldots \otimes |v_{i_n}\rangle\}$. Using the properties of the game matrices $\tilde{\Phi}_k^{(1)}(t)$ encapsulated by Eq. (6.37), one can see that for any fixed i_n, the eigenvalue corresponding to $|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle$ cannot be smaller than that corresponding to any other $|v_{i_1}\rangle \otimes \ldots \otimes |v_{i_n}\rangle$. Therefore we can concentrate only on the vectors $|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle$.

Let us compute the eigenvalues corresponding to $|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle$ for $i_n \in \{0, \ldots, d-1\}$. To do this, let us fix an input string $\vec{x}_{n-1}$ (say $(0, \ldots, 0)$) and vary over $\vec{y}_{n-1}$, in other words we consider the first row block of $\tilde{\Phi}_k^{(n)}$ corresponding to the game blocks $\tilde{\Phi}_k^{(1)}(t)$, with $t = h(\vec{0}_{n-1} + \vec{y}_{n-1})$. Denote by $\lambda^{\vec{x}_{n-1}}(i_n, k)$ the number of times the game $g(d - k^{-1} \cdot i_n)$ appears for this choice of $\vec{x}_{n-1}$ in the matrix $\tilde{\Phi}_k^{(n)}$. Due to the symmetry of the winning condition, $\lambda^{\vec{x}_{n-1}}(i_n, k)$ is independent of the choice of row $\vec{x}_{n-1}$ so we may drop the superscript. Moreover, since $\tilde{\Phi}_k^{(n)}$ is a symmetric matrix, we also have $\lambda^{\vec{x}_{n-1}}(i_n, k) = \lambda^{\vec{y}_{n-1}}(i_n, k)$ for an analogously defined $\lambda^{\vec{y}_{n-1}}(i_n, k)$.

Let us define $\Lambda(k) := \max_{i_n} \lambda(i_n, k)$ and let $\mu := d - k^{-1} \cdot i_n$ for the value of i_n for which the maximum of $\lambda(i_n, k)$ is achieved. Using Eq. (6.37), we have that

$$\left(\tilde{\Phi}_k^{(n)\dagger}\tilde{\Phi}_k^{(n)}\right)|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle = d^2\lambda^2(i_n, k)|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle, \tag{6.41}$$

from which we obtain that $\|\tilde{\Phi}_k^{(n)}\| = d\Lambda(k)$.

For prime d, multiplication (mod d) by $k \neq 0$ maps each game $g(t)$ into a game $g(t' = k \cdot t)$ such that if $t_1 \neq t_2$ then $t_1' \neq t_2'$. Therefore the maximum number of elementary games of the same type composing matrix $\Phi_k^{(n)}$ is the same for all k, $\Lambda(k) = \Lambda$. Hence we obtain the following bound on the quantum value of NLC_d for the uniformly distributed inputs case

$$\omega_q(NLC_d) \leq \frac{1}{d}\left(1 + \frac{(d-1)\Lambda}{d^{n-1}}\right). \tag{6.42}$$

We now consider the classical deterministic strategy where Alice outputs $a = \mu \cdot x_n$ independently of her inputs $\vec{x}_{n-1}$ and Bob outputs $b = \mu \cdot y_n$ independently of his input $\vec{y}_{n-1}$. Note that for the $d \times d$ blocks described by the game $g(\mu)$ all the d^2 constraints will be satisfied. On the other hand, for the blocks described by $g(t)$ for $t \neq \mu$, only d constraints are satisfied (when $x_n + y_n = 0$). Therefore the score achieved by this strategy is given by

$$\omega_c(NLC_d) = \frac{d^{n-1}}{d^{2n}} \left[\Lambda d^2 + (d^{n-1} - \Lambda)d\right], \tag{6.43}$$

which equals the upper bound on the quantum value in Eq. (6.42). This completes the proof for uniformly chosen inputs.

Now we consider the case of input probability distributions

$$p(\vec{x}_n, \vec{y}_n) = \frac{1}{d^{n+1}} \tilde{p}(\vec{x}_{n-1} + \vec{y}_{n-1}). \tag{6.44}$$

For this input distribution, the matrix $\Phi_k^{(n)}$ is still composed of the elementary games $\Phi_k^{(1)}(t)$ that can be classically saturated. The difference is that a weight $\tilde{p}(\vec{x}_{n-1} + \vec{y}_{n-1})/d^{n+1}$ is now attributed to each $d \times d$ block

$$\left[\Phi_k^{(n)}\right]_{\vec{x}_{n-1},\vec{y}_{n-1}} = \frac{1}{d^{n+1}} \tilde{p}(\vec{x}_{n-1} + \vec{y}_{n-1}) \Phi_k^{(1)}(h(\vec{x}_{n-1} + \vec{y}_{n-1})). \tag{6.45}$$

This preserves the block-wise circulant structure of ${\Phi_k^{(n)}}^\dagger \Phi_k^{(n)}$ ensuring that these matrices are still diagonal in the basis formed by the tensor product of Fourier vectors. As in the case of uniformly distributed inputs, the properties of $\Phi_k^{(1)}(t)$ in Eq. (6.37) imply that the maximum eigenvalue corresponds to one of the vectors $|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle$.

To compute the eigenvalues corresponding to $|v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle$, we now have to take into account the number of times a game $g(d - k^{-1} \cdot i_n)$ appears in a given row block as well as the respective weights. Let us denote by $\tilde{\lambda}(i_n, k)$ the weighted sum of the times the game $g(d - k^{-1} \cdot i_n)$ appears in a row block, i.e.,

$$\tilde{\lambda}(i_n, k) = \sum_{\substack{\vec{y}_{n-1} \text{ s.t.} \\ h(\vec{0}_{n-1} + \vec{y}_{n-1}) = d - k^{-1} \cdot i_n}} \frac{1}{d^{n+1}} \tilde{p}(\vec{0}_{n-1} + \vec{y}_{n-1}). \tag{6.46}$$

As before, let us define $\tilde{\Lambda}(k) := \max_{i_n} \tilde{\lambda}(i_n, k)$ and let $\mu = d - k^{-1} \cdot i_n$ for the i_n which achieves the maximum. For the game matrix $\Phi_k^{(n)}$ we have

$$\left({\Phi_k^{(n)}}^\dagger \Phi_k^{(n)}\right) |v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle = d^2 \tilde{\lambda}(i_n, k)^2 |v_0\rangle^{\otimes n-1} \otimes |v_{i_n}\rangle. \tag{6.47}$$

We therefore obtain that $\|\Phi_k^{(n)}\| = d\tilde{\Lambda}(k)$.

Again, for prime d, the maximum of $\tilde{\Lambda}(k)$ is independent of k. Therefore, we obtain the following upper bound on the quantum value of a general NLC_d game

$$\omega_q(NLC_d) \leq \frac{1}{d}\left[1 + d^{n+1}(d-1)\tilde{\Lambda}\right]. \tag{6.48}$$

Consider the classical deterministic strategy where Alice outputs $a = \mu x_n$ independently of $\vec{x}_{n-1}$ and Bob outputs $b = \mu y_n$ independently of $\vec{y}_{n-1}$. Analogously to the uniformly distributed inputs case, the score achieved by this strategy is

$$\omega_c(NLC_d) = d^{n-1}\left[\tilde{\Lambda}d^2 + \left(\frac{1}{d^{n+1}} - \tilde{\Lambda}\right)d\right], \tag{6.49}$$

which again equals the upper bound on the quantum value in Eq.(6.48). This completes the proof that quantum strategies cannot outperform classical strategies in the NLC_d game. □

Note that our proof relies on the assumption that the winning constraint function has the form $h(\vec{x}_{n-1} + \vec{y}_{n-1}) \cdot (x_n + y_n)$, which seems more restrictive than stated for the binary NLC [LPSW07]. Now, let us consider the 3-input and 3-output game g^{eg}, *i.e.* $d = 3$ and $n = 1$, whose winning condition is specified by

$$f(x,y) = \begin{cases} 0, & \text{if } x+y = 0 \text{ or } x+y = 1 \\ 1, & \text{if } x+y = 2 \end{cases} \tag{6.50}$$

and the associated game matrices are $\Phi_1^{eg} = \frac{1}{9}\begin{pmatrix} 1 & 1 & \zeta \\ 1 & \zeta & 1 \\ \zeta & 1 & 1 \end{pmatrix}$ and $\Phi_2^{eg} = \Phi_1^{eg*}$. An SDP optimization over measurements for the maximally entangled state in dimension 3 shows that the quantum value overcomes the classical value of the game (6.50). Therefore Theorem 6.4.1 cannot be extended to an arbitrary function $f(\vec{x}_n + \vec{y}_n)$.

6.5 Discussion and open problems

In this chapter, we have presented an upper bound to the quantum value of linear games. The bound is not tight in general but it is very simple and, as we have shown by examples, it allowed us to derive several results: We have used the bound to rule out from the quantum set a class of no-signaling boxes that would result in trivialization of communication complexity; Also, we have shown that the recently discovered bound on the quantum value of

the CHSH-d game, obtained in Ref. [BS15], can be derived in a simple manner using our bound; And finally, we have extended the principle of no-advantage for nonlocal computation to a class of functions with prime d possible values.

Moreover the derived bound is efficiently computable since, for a linear game with d outcomes, it requires the spectral norm of d game matrices, where the size of these matrices grows polynomially with the number of questions in the game (a game with m question per player has game matrices of size $m \times m$).

As a future direction, it would be particularly interesting to investigate if one can extend the result of Theorem 5.4.2 to the graphs associated to NLC_d. As a more challenging next step, we point to the generalization of the technique of norm bounds to classes of Bell inequalities beyond linear games. Due to its simplicity, it could lead to general results of fundamental and practical interest.

Chapter 7

Multiplayer linear games and device-independent witness of genuine tripartite entanglement

In this chapter we present results of Ref. [MRMT16]

> *Quantum bounds on multiplayer linear games and device-independent witness of genuine tripartite entanglement*
> **G. Murta**, R. Ramanathan, N. Móller, and M. Terra Cunha
> **Phys. Rev. A, 93, 022305, (2016)**.

Now we consider the case of linear games with n players. We generalize the bound obtained in the previous Chapter [RAM16] to the quantum value of an n-player game. We extend the examples of the 2-player case, deriving an upper bound to the quantum value of a generalization of the CHSH-d game for n players, and also we exclude the possibility of quantum realization of multipartite functional boxes that would lead to trivialization of communication complexity in a multipartite scenario. As our main result for the multipartite scenario, we use the bounds to design devide-independent witnesses of genuine multipartite entanglement for tripartite systems.

7.1 Motivation

Multipartite scenarios bring fundamental and practical new features. From the fundamental point of view, the possibility of having more parties interacting with each other brings the novelty of different classes of correlations (now all the parties can share nonlocal correlations or, else, only a subgroup of the parties can be non-classically correlated), and therefore we can have a much richer

nonlocality structure. Moreover, as shown in Ref. [GWAN11], no bipartite principle is sufficient to single out the set of quantum correlations for an arbitrary number of parties, and hence the study of the intrinsically multipartite features is necessary. From the practical point of view, multipartite scenarios allow for the realization of many cryptographic tasks whose unconditional security cannot be guaranteed in a bipartite scenario [BOGKW88]. A remarkable example is the task of bit commitment for which no-go theorems [May97, LC97] state the impossibility of having an unconditionally secure bipartite protocol. This impossibility was circumvented by Kent [Ken11, Ken12] who proposed the idea of adding multiple space-like separated agents for each party (what is called a "relativistic protocol"), allowing unconditional security as long as the agents remain separated. In Ref. [KTHW13] a relativistic protocol was proposed, where the commitment can be made arbitrarily long by the introduction of a rounding procedure. Interestingly, the security against classical adversaries is guaranteed by a mapping to the problem of estimating the performance of the players in a multiplayer game.

Besides its undeniable importance, very few results are known for multipartite Bell scenarios. We now extend the techniques presented in Chapter 6 [RAM16] and provide an upper bound to the quantum value of multiplayer linear games based on game matrices.

7.2 An efficiently computable bound to the quantum value of multiplayer linear games

Our goal in this Section is to bound the performance of players sharing quantum resources in an n-player linear game $g_n^\ell(G, f, p)$ (Definition 3.4.2).

A generalization of Lemma 6.2.1 also holds for multiplayer games, and the average probability of success on the game, $\omega(g_n^\ell)$, can be written in terms of the generalized correlators. The **multipartite generalized correlators** $\langle A_{1\,x_1}^{1\,i} \dots A_{n\,x_n}^{n\,j} \rangle$ are defined as the Fourier transform of the probabilities

$$\langle A_{1\,x_1}^{1\,i} \dots A_{n\,x_n}^{n\,j} \rangle = \sum_{a_1,\dots,a_n \in G} \bar{\chi}_i(a_1) \dots \bar{\chi}_j(a_n) P(a_1, \dots, a_n | x_1, \dots, x_n), \tag{7.1}$$

and the inverse Fourier transform gives us

$$P(a_1, \dots, a_n | x_1, \dots, x_n) = \frac{1}{|G|^n} \sum_{a_1,\dots,a_n \in G} \chi_i(a_1) \dots \chi_j(a_n) \langle A_{1\,x_1}^{1\,i} \dots A_{n\,x_n}^{n\,j} \rangle. \tag{7.2}$$

Lemma 7.2.1. *Given a particular strategy $\vec{P}(a_1,\ldots,a_n|x_1,\ldots,x_n)$, the average probability of success in an n-player linear game $g_n^\ell(G,f,p)$ can be written as*

$$\omega(g_n^\ell)=\frac{1}{|G|}\left(1+\sum_{x_1,\ldots,x_n}\sum_{k\in G\setminus\{e\}}p(x_1,\ldots,x_n)\chi_k(f(x_1,\ldots,x_n))\langle A_{1x_1}^k\ldots A_{nx_n}^k\rangle\right). \tag{7.3}$$

For the particular case of a 3-player linear game $g_3^\ell(G,f,p)$, Lemma 7.2.1 gives us

$$\omega(g_3^\ell)=\frac{1}{|G|}\left(1+\sum_{x,y,z}\sum_{k\in G\setminus\{e\}}p(x,y,z)\chi_k(f(x,y,z))\langle A_x^kB_y^kC_z^k\rangle\right). \tag{7.4}$$

Proof of Lemma 7.2.1. We present the proof for the case of 3 players. The case of n players follows in an analogous way.

Given the probabilities in terms of the generalized correlators:

$$P(a,b,c|x,y,z)=\frac{1}{|G|^3}\sum_{i,j,k\in G}\chi_i(a)\chi_j(b)\chi_k(c)\langle A_x^iB_y^jC_z^k\rangle, \tag{7.5}$$

we can proceed to calculate $P(a+b+c=f(x,y,z)|x,y,z)$:

$$\begin{aligned}
P(a+b+c=f(x,y,z)|x,y,z)=&\\
&=\sum_{a,b}P(a,b,f(x,y,z)-a-b|x,y,z)\\
&=\sum_{a,b}\frac{1}{|G|^3}\sum_{i,j,k\in G}\chi_i(a)\chi_j(b)\chi_k(f(x,y)-a-b)\langle A_x^iB_y^jC_z^k\rangle\\
&=\frac{1}{|G|^3}\sum_{i,j,k\in G}\chi_k(f(x,y))\left(\sum_a\chi_i(a)\chi_j(-a)\right)\\
&\qquad\times\left(\sum_b\chi_j(b)\chi_k(-b)\right)\langle A_x^iB_y^jC_z^k\rangle\\
&=\frac{1}{|G|}\sum_{k\in G}\chi_k(f(x,y))\langle A_x^kB_y^kC_z^k\rangle
\end{aligned} \tag{7.6}$$

where we have used the characters' properties (6.2).

The weighted sum over the inputs, gives us the desired result. □

Considering a particular quantum strategy given by the set of projective measurements $\{M_x^a\}$, $\{M_y^b\}$, $\{M_z^c\}$ performed on the tripartite quantum state $|\psi\rangle$, the tripartite correlators correspond to

$$\langle A_x^i B_y^j C_z^k \rangle = \langle \psi | \, A_x^i \otimes B_y^j \otimes C_z^k \, | \psi \rangle \,, \tag{7.7}$$

where, as defined in the previous Chapter:

$$A_x^i = \sum_a \bar{\chi}_i(a) M_x^a, \tag{7.8}$$

and analogously for B_y^j and C_z^k.

Motivated by Lemma 7.2.1, for tripartite linear games we can also associate a set of $|G| - 1$ (rectangular) matrices which carry information about the probability distribution with which the referee picks questions and also the winning condition of the game.

Definition 7.2.1 (Multiplayer linear game matrices)**.** *Given a linear game $g_3^\ell(G, f, p)$ the associated $|G| - 1$ game matrices are defined as*

$$\Phi_k = \sum_{(x,y,z)\in Q} p(x,y,z)\chi_k(f(x,y,z)) \, |x\rangle\langle yz| \quad \text{for} \quad k \in G \setminus \{e\} \tag{7.9}$$

where $\{|x\rangle\}$, $\{|y\rangle\}$ and $\{|z\rangle\}$ form orthonormal basis in $\mathbb{C}^{|Q_1|}$, $\mathbb{C}^{|Q_2|}$ and $\mathbb{C}^{|Q_3|}$ respectively, and $Q = Q_1 \times Q_2 \times Q_3$.

Note that in Definition 7.2.1 we have chosen to write the game matrices in terms of the partition $x|yz$ of the inputs. However, we could equally chose any other partition $y|xz$ or $z|xy$ and define the respective game matrices in an analogous way. If the winning condition of the game $f(x, y, z)$ is not invariant over the permutation of parties, each partition would give rise to different matrices.

Given all these definitions we are ready to state the main result of this Chapter which generalizes the norm bound presented in Chapter 6 for multiplayer linear games. We start with a 3-player game.

Theorem 7.2.1. *The quantum value of a tripartite linear game, $g_3^\ell(G, f, p)$, where players A, B, and C receive respectively questions $x \in Q_1, y \in Q_2, z \in Q_3$ and answer with elements of an Abelian group $(G, +)$, is upper bounded by*

$$\omega_q(g_3^\ell) \leq \frac{1}{|G|}\left(1 + \sqrt{|Q_1||Q_2||Q_3|} \sum_{k\in G\setminus\{e\}} \|\Phi_k\|\right), \tag{7.10}$$

where $\|\cdot\|$ denotes the maximum singular value of the matrix, e is the identity element of the group G, and Φ_k are the game matrices.

Proof. The proof follows analogously to the 2-player case. Consider a quantum strategy where measurements $\{M_x^a\}$, $\{M_y^b\}$, $\{M_z^c\}$ are performed on the tripartite quantum state $|\psi\rangle$, hence we have

$$\omega(g_3^\ell) = \frac{1}{|G|}\left(1 + \sum_{x,y,z}\sum_{k\in G\setminus\{e\}} p(x,y,z)\chi_k(f(x,y,z))\,\langle\psi|\, A_x^k \otimes B_y^k \otimes C_z^k\,|\psi\rangle\right). \tag{7.11}$$

And we can define the normalized vectors

$$\begin{aligned}\left|\alpha^k\right\rangle &= \frac{1}{\sqrt{|Q_1|}}\sum_{x\in Q_1} A_x^{k\dagger}\otimes \mathbb{1}_{BC}\otimes\mathbb{1}_{Q_1}\,|\psi\rangle\,|x\rangle \\ \left|\beta^k\right\rangle &= \frac{1}{\sqrt{|Q_2||Q_3|}}\sum_{x,y\in Q_2\times Q_3} \mathbb{1}_A\otimes B_y^k\otimes C_z^k\otimes\mathbb{1}_{Q_2,Q_3}\,|\psi\rangle\,|y,z\rangle\,.\end{aligned} \tag{7.12}$$

Now by making use of the game matrices Φ_k (7.9) we have the desired result:

$$\begin{aligned}\omega(g_3^\ell) &= \frac{1}{|G|}\left(1 + \sqrt{|Q_1||Q_2||Q_3|}\sum_{k\in G\setminus\{e\}}\left\langle\alpha^k\right|\mathbb{1}_{ABC}\otimes\Phi_k\left|\beta^k\right\rangle\right) \\ &\leq \frac{1}{|G|}\left(1 + \sqrt{|Q_1||Q_2||Q_3|}\sum_{k\in G\setminus\{e\}}\|\mathbb{1}_{ABC}\otimes\Phi_k\|\right) \\ &= \frac{1}{|G|}\left(1 + \sqrt{|Q_1||Q_2||Q_3|}\sum_{k\in G\setminus\{e\}}\|\Phi_k\|\right).\end{aligned} \tag{7.13}$$

□

The generalization for n-player games is given by the following Theorem.

Theorem 7.2.2. *Consider an n-player linear game, $g_n^\ell(G,f,p)$. Let S be a proper subset of the parties, $S\subset\{1,\ldots,n\}$. The quantum value of an n-player linear game, $g_n^\ell(G,f,p)$, is upper bounded by*

$$\omega_q(g_n^\ell) \leq \min_S \frac{1}{|G|}\left(1 + \sqrt{|Q_1|\ldots|Q_n|}\sum_{k\in G\setminus\{e\}}\|\Phi_k^S\|\right), \tag{7.14}$$

where $\|\Phi_k^S\|$ denotes the maximum singular value of matrix Φ_k^S and the game matrices for partition S are defined as

$$\Phi_k^S = \sum_{\vec{x}\in Q_S,\vec{y}\in Q_{S^c}} p(\vec{x},\vec{y})\chi_k(f(\vec{x},\vec{y}))\,|\vec{x}\rangle\langle\vec{y}|\,. \tag{7.15}$$

$\vec{x} \in Q_S$ denotes the vector of inputs of the players that belong to set S, and S^c is the complement of S.

Proof. Let S be a proper subset of the parties $S \subset \{1, \ldots, n\}$, and the associated game matrices be defined as

$$\Phi_k^S = \sum_{\vec{x}\in Q_S, \vec{y}\in Q_{S^c}} p(\vec{x},\vec{y})\chi_k(f(\vec{x},\vec{y})) \left|\vec{x}\right\rangle\left\langle\vec{y}\right| . \tag{7.16}$$

Now by defining the normalized vectors

$$\begin{aligned} \left|\alpha^k\right\rangle =& \frac{1}{\sqrt{|Q_S|}} \sum_{\vec{x}\in Q_S} \left(\bigotimes_{i\in S} {A_i^k}_{x_i}^\dagger\right) \otimes \mathbb{1}_{S^c} \otimes \mathbb{1}_{Q_S} \left|\psi\right\rangle \left|\vec{x}\right\rangle \\ \left|\beta^k\right\rangle =& \frac{1}{\sqrt{|Q_{S^c}|}} \sum_{\vec{y}\in Q_{S^c}} \mathbb{1}_S \otimes \left(\bigotimes_{i\in S^c} A_{i x_i}^k\right) \otimes \mathbb{1}_{Q_{S^c}} \left|\psi\right\rangle \left|\vec{y}\right\rangle , \end{aligned} \tag{7.17}$$

where $|Q_S| = \prod_{i\in S} |Q_i|$, and $Q_S = Q_{i_1} \times \ldots \times Q_{i_k}$ for $i_k \in S$, we have that

$$\begin{aligned} \omega(g_n^\ell) &= \frac{1}{|G|}\left(1 + \sqrt{|Q_1|\ldots|Q_n|} \sum_{k\in G\setminus\{e\}} \left\langle\alpha^k\right| \mathbb{1}_{A_1\ldots A_n} \otimes \Phi_k^S \left|\beta^k\right\rangle\right) \\ &\leq \frac{1}{|G|}\left(1 + \sqrt{|Q_1|\ldots|Q_n|} \sum_{k\in G\setminus\{e\}} \|\mathbb{1}_{A_1\ldots A_n} \otimes \Phi_k^S\|\right) \\ &= \frac{1}{|G|}\left(1 + \sqrt{|Q_1|\ldots|Q_n|} \sum_{k\in G\setminus\{e\}} \|\Phi_k^S\|\right) . \end{aligned} \tag{7.18}$$

By the construction of the proof we see that for all subset S we have a valid upper bound to the quantum value. □

In Theorem 7.2.2 each partition S of the set of parties provides an upper bound to the quantum value, the minimum in Eq. (7.14) selects the most restrictive one. In Definition 7.2.1 we have chosen $S = \{1\}$ for the 3-player game, but writing the game matrices with $S = \{2\}$ or $S = \{3\}$ can lead to tighter bounds than the one derived from Eq. (7.9).

The computational complexity of our bound

Theorem 7.2.2 states an upper bound to the quantum value of n-player linear games in terms of the spectral norm of the game matrices Φ_k^S, whose dimension depends on the number of players and the number of questions per

player. Given an n-player linear game $g_n^\ell(G, f, p)$ with m questions per player and d possible outcomes, the game matrices have dimension m^n (where the number of rows and columns depends on the subset S chosen to construct the matrix). The singular value decomposition of these matrices has time complexity at most[1] $T(n, m) = \mathcal{O}(m^{\frac{3}{2}n})$ [GVL96]. Therefore, for a particular subset S, an upper bound to the quantum value of game $g_n^\ell(G, f, p)$ can be obtained with time complexity $T(n, m, d) = \mathcal{O}(dm^{\frac{3}{2}n})$. So we see that the complexity increases exponentially with the number of players. Moreover if we want to obtain the smallest of the upper bounds we would have to run the algorithm an exponential number of times, since there are 2^{n-1} possible subsets[2] S. Nevertheless, for particular problems (as for example the n-player CHSH-d game that we are going to discuss in the next Section) the bound may be easily calculated analytically by using the symmetries of the game matrix, without the need to perform an explicit numerical calculation.

7.3 n-player CHSH-d game

In Section 6.3 we considered a d-output generalization of the CHSH game, for d prime or power of a prime. Here we generalize this game for n players following an expression first introduced by Svetlichny [Sve87] in the context of detecting genuine multipartite nonlocality.

Definition 7.3.1. *The d-input and d-output per player, n-player CHSH game, the CHSH$_n$-d game, for d prime or a power of prime, is a linear game with the winning condition given by*

$$a_1 + \ldots + a_n = \sum_{i<j} x_i \cdot x_j \tag{7.19}$$

where addition and multiplication are operations defined over the finite field $\mathbb{F}_d$.

In order to exemplify, let us consider the CHSH$_3$-3 game, where the inputs and outputs are elements of $\mathbb{Z}_3$, $a, b, c, x, y, z \in \{0, 1, 2\}$, and $+, \cdot$ are sum and multiplication modulo 3. The winning condition (7.19) reduces to

$$a + b + c = x \cdot y + x \cdot z + y \cdot z. \tag{7.20}$$

[1] In Ref. [GVL96], an algorithm for finding the singular values of an $k \times l$ matrix, $l \leq k$, in time $T(k, l) = \mathcal{O}(2kl^2 + 2l^3)$ is presented. Therefore, for the worst case of S containing $n/2$ elements, Φ_k^S is an $m^{n/2} \times m^{n/2}$ matrix, and $T(n, m, d) = \mathcal{O}(dm^{\frac{3}{2}n})$.

[2] Note that $\Phi_k^S = (\Phi_k^{S^c})^T$ which therefore leads to the same bound.

The game matrix Φ_1 for the CHSH$_3$-3 is then given by

$$\Phi_1 = \sum_{x,y,z=0}^{2} \frac{1}{27} \zeta^{x\cdot y + x\cdot z + y\cdot z} \left|x\right\rangle\left\langle yz\right|, \tag{7.21}$$

which is explicitly written as

$$\Phi_1 = \frac{1}{27}\begin{bmatrix} 1 & 1 & 1 & 1 & \zeta & \zeta^2 & 1 & \zeta^2 & \zeta \\ 1 & \zeta & \zeta^2 & \zeta & 1 & \zeta^2 & \zeta^2 & \zeta^2 & \zeta^2 \\ 1 & \zeta^2 & \zeta & \zeta^2 & \zeta^2 & \zeta^2 & \zeta & \zeta^2 & 1 \end{bmatrix}. \tag{7.22}$$

where $\zeta = e^{2\pi \mathrm{i}/3}$ is a 3rd root of unity.

Now we use Theorem 7.2.2 to prove an upper bound on the performance of quantum players in the CHSH$_n$-d game.

Theorem 7.3.1. *The quantum value of the CHSH$_n$-d game, for d prime or a power of a prime, obeys*

$$\omega_q(CHSH_n\text{-}d) \leq \frac{1}{d} + \frac{d-1}{d\sqrt{d}}. \tag{7.23}$$

Proof. The proof follows from a direct calculation of $\Phi_k^S \Phi_k^{S\dagger}$ with the partition $S = \{1\}$. The game matrices associated to partition $S = \{1\}$ are the following:

$$\Phi_k^{A_1} = \sum_{x_1,\ldots,x_n} \frac{1}{d^n} \chi_k\Big(\sum_{j>i} x_i \cdot x_j\Big) \left|x_1\right\rangle\left\langle x_2 \ldots x_n\right|. \tag{7.24}$$

By making use of the characters relations, Eq. (6.2), we have

$$\begin{aligned} \Phi_k^{A_1}{\Phi_k^{A_1}}^\dagger &= \frac{1}{d^{2n}} \sum_{x_1,\ldots,x_n} \sum_{x_1',\ldots,x_n'} \chi_k\Big(\sum_{j>i} x_i \cdot x_j\Big) \\ &\qquad \times \bar{\chi}_k\Big(\sum_{j>i} x_i' \cdot x_j'\Big) \left|x_1\right\rangle \left\langle x_2 \ldots x_n \middle| x_2' \ldots x_n'\right\rangle \left\langle x_1'\right| \\ &= \frac{1}{d^{2n}} \sum_{x_1,\ldots,x_n} \sum_{x_1'} \prod_{j>1} \chi_k(x_1 \cdot x_j) \bar{\chi}_k(x_1' \cdot x_j) \left|x_1\right\rangle\left\langle x_1'\right| \\ &= \sum_{x_1} \frac{1}{d^{n+1}} \left|x_1\right\rangle\left\langle x_1\right| \\ &= \frac{1}{d^{n+1}} \mathbb{1}_d, \end{aligned} \tag{7.25}$$

where in the second step we have used the fact that $\chi_k(x_i \cdot x_j)\bar{\chi}_k(x_i \cdot x_j) = 1$. Therefore, $\|\Phi_k^{A_1}\| = \frac{1}{\sqrt{d^{n+1}}}$ for all k. Finally, by applying Theorem 7.2.2 we obtain

$$\omega_q(\text{CHSH}_n\text{-}d) \leq \frac{1}{d} + \frac{d-1}{d\sqrt{d}}. \tag{7.26}$$

□

Interestingly these bounds are independent of the number of parties showing that by increasing the number of players the performance is still limited. Note that in order to derive Theorem 7.3.1 we have used $S = \{1\}$. For the 3-player case all the other possible partitions of the players would lead to the same result since the winning condition of the game, Eq. (7.19), is invariant under the permutation of parties. However for games with $n > 3$ players it is possible that exploring partitions with more players $S = \{1, \ldots, r\}$ can lead to a better bound.

7.4 No quantum realization of non-trivial multiparty functional boxes

In Ref. [vD13] it was shown that the possibility of existence of strong correlations known as PR-boxes [PR94] would lead to the trivialization of communication complexity. As Alice and Bob would be able to compute any distributed Boolean function with only one bit of communication, by sharing a sufficient number of PR-boxes. Therefore, the belief that communication complexity is not trivial (*i.e.* , some distributed functions require more than one bit of communication in order to be computed) is viewed as a principle that should be respected by nature.

As we discussed in Section 6.3, this result was later generalized [Wan11] to the so-called functional boxes, *i.e.* a d-output generalization of PR-boxes for $a + b = f(x, y)$ in $\mathbb{Z}_d$ arithmetic, with d prime and f any non-additively separable function (*i.e.* $f(x, y) \neq f_1(x) + f_2(y)$). Any functional box which cannot be simulated classically would also lead to trivialization of communication complexity [Wan11]. Furthermore, a generalization to multiparty communication complexity scenarios for binary outcome was considered in Ref. [BP05]. In the multipartite problem, n parties are each given an input x_i and must compute a function $f(\vec{x})$ of their joint inputs with as little communication as possible. If the parties share a sufficient number of boxes with input-output relation satisfying $\bigoplus_i a_i = \prod_i x_i$, then any n-party communication complexity problem can

be solved with only $n-1$ bits of communication (from $n-1$ parties to the first party who then computes the function) [BP05].

In Appendix D, we analyze the task of computing a multipartite function with d possible values, and show that multipartite functional boxes associated to non-trivial XOR-d games with uniformly distributed inputs, for d prime, lead to a trivialization of communication complexity in this scenario. Here we use Theorem 7.2.2 to show that an n-party functional box which maximally saturates these games cannot be realized in quantum theory.

Theorem 7.4.1. *For an n-player XOR-d game $g_n^{\oplus_d}$, with m questions per player and uniform input distribution $p(\vec{x}) = 1/m^n$, $\omega_q(g_n^{\oplus_d}) = 1$ iff $\omega_c(g_n^{\oplus_d}) = 1$.*

Proof. We start by proving the result for 3 players. We first chose the partition $S = \{1\}$ to write the game matrices.

The constraint that the input distribution is $p(x,y,z) = 1/m^3$ for all x,y,z implies $\|\Phi_k^A\| \leq 1/\sqrt{m^3}$ since $\Phi_k^A \Phi_k^{A\dagger}$ is an $m \times m$ matrix with the absolute value of all elements $\leq 1/m^4$ (and then $\|\Phi_k^A \Phi_k^{A\dagger}\| \leq 1/m^3$). For the particular case of 3-player XOR-d games, the bound (7.10) is given by

$$\omega_q(g_n^{\oplus_d}) \leq \frac{1}{d}\left[1 + \sqrt{m^3}\sum_{k=1}^{d-1}\|\Phi_k^A\|\right], \tag{7.27}$$

where

$$\Phi_1^A = \sum_{x,y,z}\frac{1}{m^3}\zeta^{f(x,y,z)}\,|x\rangle\langle yz|\,. \tag{7.28}$$

So we see that

$$\omega_q(g^{\oplus_d}) = 1 \Rightarrow \|\Phi_k^A\| = \frac{1}{\sqrt{m^3}}\ \forall k. \tag{7.29}$$

Let $|\lambda^A\rangle = (\lambda_0^A, \ldots, \lambda_{m-1}^A)$ be the eigenvector corresponding to the maximum eigenvalue $1/m^3$ of $\Phi_1^A \Phi_1^{A\dagger}$. Consider $\lambda_j^A = |\lambda_j^A|\zeta^{\theta_j^A}$ and assume $|\lambda_0^A| \geq |\lambda_1^A| \geq \ldots \geq |\lambda_{m-1}^A|$. Then we have

$$\begin{aligned}\Phi_1^A \Phi_1^{A\dagger} =& \frac{1}{m^6}\sum_{x,y,z}\sum_{x',y',z'}\zeta^{f(x,y,z)-f(x',y',z')}\,|x\rangle\,\langle yz|y'z'\rangle\,\langle x'| \\ =& \frac{1}{m^6}\sum_{x,x',y,z}\zeta^{f(x,y,z)-f(x',y,z)}\,|x\rangle\langle x'|\end{aligned} \tag{7.30}$$

and

$$\begin{aligned}\Phi_1^A\Phi_1^{A\dagger}\left|\lambda^A\right\rangle =& \frac{1}{m^6}\sum_{x,x',y,z,i}\zeta^{f(x,y,z)-f(x',y,z)+\theta_i^A}|\lambda_i^A|\,|x\rangle\,\langle x'|i\rangle \\ =& \frac{1}{m^6}\sum_{x,y,z,i}\zeta^{f(x,y,z)-f(i,y,z)+\theta_i^A}|\lambda_i^A|\,|x\rangle\,.\end{aligned} \tag{7.31}$$

By analyzing the first component of the eigenvalue equation $\Phi_1^A\Phi_1^{A\dagger}\left|\lambda^A\right\rangle = 1/m^3\left|\lambda^A\right\rangle$ we have

$$\left[\Phi_1^A\Phi_1^{A\dagger}\left|\lambda^A\right\rangle\right]_1 = \frac{1}{m^6}\sum_{y,z,i}\zeta^{f(0,y,z)-f(i,y,z)+\theta_i^A}|\lambda_i^A| = \frac{1}{m^3}|\lambda_0^A|\zeta^{\theta_0^A}. \tag{7.32}$$

In order to satisfy this equation we need to have

$$|\lambda_i^A| = |\lambda_0^A| \;\;\forall\;\; i \tag{7.33a}$$

$$\zeta^{f(0,y,z)-f(i,y,z)+\theta_i^A} = \zeta^{\theta_0^A} \;\;\forall\;\; i,y,z. \tag{7.33b}$$

The equations for the other components of the eigenvalue equation imply:

$$f(x,y,z) - f(x',y,z) = \theta_x^A - \theta_{x'}^A \;\forall\; y,z, \tag{7.34a}$$

where the operations are modulo d.

We can do the same argument for the other partitions, $S = \{2\}$ and $S = \{3\}$, and the hypothesis of $\omega_q(g_n^{\oplus_d}) = 1$ implies that $\mathrm{rank}(\Phi_1^S) = 1$ for all S, and

$$f(x,y,z) - f(x,y',z) = \theta_y^B - \theta_{y'}^B \;\forall\; x,z \tag{7.34b}$$

$$f(x,y,z) - f(x,y,z') = \theta_z^C - \theta_{z'}^C \;\forall\; x,y. \tag{7.34c}$$

By the relations (7.34a), (7.34b) and (7.34c) we deduce that

$$\begin{aligned} f(x,y,z) &= (\theta_x^A - \theta_0^A) + f(0,y,z) \\ &= (\theta_x^A - \theta_0^A) + (\theta_y^B - \theta_0^B) + f(0,0,z) \\ &= (\theta_x^A - \theta_0^A) + (\theta_y^B - \theta_0^B) + (\theta_z^C - \theta_0^C) + f(0,0,0). \end{aligned} \tag{7.35}$$

Now, consider a_0, b_0, c_0 such that $a_0 \oplus_d b_0 \oplus_d c_0 = f(0,0,0)$, the classical strategy

$$\begin{aligned} a &= a_0 + (\theta_x^A - \theta_0^A) \\ b &= b_0 + (\theta_y^B - \theta_0^B) \\ c &= c_0 + (\theta_z^C - \theta_0^C) \end{aligned} \tag{7.36}$$

wins the game with probability 1.

The proof for an n-player game follows in the same way. Considering the partition $S = \{A_1\}$. The constraint of equally distributed inputs implies $\Phi_k^S \Phi_k^{S\dagger}$ is an $m \times m$ matrix with the absolute value of all elements equal to $1/m^{n+1}$ (and then $\|\Phi_k^S \Phi_k^{S\dagger}\| \leq 1/m^n$). Now considering the bound

$$\omega_q \leq \frac{1}{d}\left[1 + \sqrt{m^n}\sum_{k=1}^{d-1}\|\Phi_k^S\|\right], \tag{7.37}$$

we see that $\omega_q(g^{\oplus_d}) = 1$ requires $\|\Phi_k^S\| = 1/\sqrt{m^n}$ for all k.

Following the same argument as for the 3-player game, we conclude that in order to satisfy $\|\Phi_k^S\| = 1/\sqrt{m^n}$ all the rows of the game matrix have to be proportional to each other and then

$$f(x_1, x_2, \ldots, x_n) - f(x'_1, x_2, \ldots, x_n) = \theta_{x_1}^{A_1} - \theta_{x'_1}^{A_1} \;\; \forall \;\; x_2, \ldots x_n. \tag{7.38}$$

Running the analysis over the partitions $S = A_i$ for $i = 2, \ldots, n$ we can specify a classical strategy, given by $a_{x_i} = a_{0_i} + (\theta_{x_i}^{A_i} - \theta_{0_i}^{A_i})\ \forall i$, that wins the game with probability 1. □

Note that the no-signaling boxes that win some of these n-player XOR-d games with probability one correspond to nontrivial functional boxes, hence our bound excludes the possibility of quantum realization of functional boxes that trivialize communication complexity in the multiparty scenario.

7.5 Device independent witnesses of genuine tripartite entanglement

We now present a systematic way to derive device-independent witnesses for genuine tripartite entanglement.

The characterization of entanglement is a very challenging task (see Appendix A.2). For bipartite systems, positive maps which are not completely positive constitute a powerful tool for generating simple operational criteria for detecting entanglement in mixed states [HHH96]. The most celebrated example is the Peres-Horodecki criterion [Per96b] (Proposition A.2.2), also known as PPT criterion. The characterization of multipartite entanglement, however, is much more challenging since inequivalent forms of entanglement appear. When we are considering correlations among many parties it can happen that all of the

parties share quantum correlations, in which case we say that we have **genuine multipartite entanglement**, or it can be the case that the state is composed by quantum correlations only between subsets of the parties, in which case the state of the system is said to be biseparable[3]. Formally, a biseparable state of three parties is a state that can be decomposed into the form

$$\rho_{\mathcal{B}} = \sum_i \left(p^i_A \rho^i_A \otimes \rho^i_{BC} + p^i_B \rho^i_B \otimes \rho^i_{AC} + p^i_C \rho^i_C \otimes \rho^i_{AB} \right), \tag{7.39}$$

where $p^i_j \geq 0$, $\sum_i (p^i_A + p^i_B + p^i_C) = 1$. If a tripartite quantum state cannot be written as Eq. (7.39), it is said to be genuinely tripartite entangled.

For the detection of genuine multipartite entanglement there is no known direct criteria like the PPT-criterion. For this reason, the development of device-independent entanglement witnesses (DIEW) for genuine multipartite entanglement brings together with all the advantage of distinguishing the type of entanglement in a multipartite system, the possibility of performing this task in a scenario where we do not have full trust in our devices, which is of extreme importance for cryptographic tasks.

Device independent witnesses of genuine multipartite entanglement were introduced in Ref. [BGLP11]. The idea of a DIEW for genuine multipartite entanglement is to find the maximal value that a biseparable quantum state (Eq. (7.39) for 3 parties) can achieve in a Bell expression (which in general is in between the classical and the quantum value of this expression). Therefore, in a Bell experiment, if a quantum state overtakes the biseparable bound we can assert that this state is genuinely multipartite entangled.

It is important to note that a DIEW is a weaker condition than the Svetilichny inequalities [Sve87]. Svetlichny inequalities were introduced in multipartite Bell scenarios in order to detect the existence of genuine multipartite nonlocality (see Section 1.5). The violation of a Svetlichny inequality guarantees that even if some parties are allowed to perform a joint strategy (which includes a global quantum measurement in their systems) they are not able to simulate the exhibited multipartite correlations. The violation of a DIEW guarantees that the parties share a genuinely multipartite entangled state but not necessarily that they are able to exhibit genuine multipartite nonlocality.

[3]This concept can be refined to many levels which is denoted k-separability. An n-partite state is k-separable (see [GHH10] for more detailed definition) if it can be write as a convex combination of states that are products of k subspaces:

$$\rho_{k-\text{sep}} = \sum_i p_i \left| \psi^i_{k-\text{sep}} \right\rangle \left\langle \psi^i_{k-\text{sep}} \right|$$

where $\left| \psi^i_{k-\text{sep}} \right\rangle = \left| \psi_{i_1} \right\rangle \otimes \left| \psi_{i_2} \right\rangle \otimes \ldots \otimes \left| \psi_{i_k} \right\rangle$. An n-partite state is separable if it is n-separable.

Concerning previous works in the subject of DIEWs of genuine multipartite entanglement: A tripartite 3-input 2-output inequality which is able to detect genuine tripartite entanglement in a noisy three-qubit GHZ state, $\rho(V) = V\,|GHZ\rangle\langle GHZ| + (1-V)\frac{\mathbb{1}}{8}$, for parameter $V > 2/3$, was presented in Ref. [BGLP11]. This result was later [PV11] generalized for multisetting Bell inequalities that in the limit of infinitely many inputs are able to detect genuine tripartite entanglement for $\rho(V)$ with parameter as low as $2/\pi$, which is the limiting value for which there exist a local model for the noisy GHZ state for full-correlation Bell inequalities [PV11, BGLP11]. Other examples of DIEWs with binary outcomes can be found in Ref. [BBB+12].

Let us consider that Alice, Bob, and Charlie are playing a 3-player linear game, $g_3^\ell(G, f, p)$, and they have access to the shared biseparable quantum state:

$$|\psi_{\mathcal{B}}\rangle = |\psi_{AB}\rangle \otimes |\psi_C\rangle\,. \tag{7.40}$$

In that case Alice and Bob can take advantage of a quantum strategy using their shared entangled state $|\psi_{AB}\rangle$. However, the best Charlie can do is to apply a classical (deterministic) strategy, since he shares no resources with Alice and Bob. For this case, their probability of success will be given by

$$\omega(g_3^\ell) \leq \frac{1}{|G|}\left(1 + \sum_{x,y,z}\sum_{k\neq\{e\}} p(x,y,z)\chi_k(f(x,y,z))\bar{\chi}_k(c_z)\,\langle\psi_{AB}|\,A_x^k \otimes B_y^k\,|\psi_{AB}\rangle\right), \tag{7.41}$$

where $\{c_z\}$ represents the deterministic strategy performed by Charlie, where upon receiving input z he outputs c_z.

Now we have essentially a bipartite expression to evaluate, and by making use of the theorem 6.2.1 we can bound the performance of the players sharing a state biseparable with respect to the partition $AB|C$. We denote by $\omega_{\mathcal{B}}^C(g_3^\ell)$ the maximum value the players can achieve in the game $g_3^\ell(G, f, p)$ when they share a state of the form (7.40):

$$\omega_{\mathcal{B}}^C(g_3^\ell) \leq \max_{\{c_z\}} \frac{1}{|G|}\left(1 + \sqrt{|Q_A||Q_B|}\sum_{k\in G\setminus\{e\}} \|\Phi_k^{\mathcal{B}}(c_z)\|\right), \tag{7.42}$$

where

$$\Phi_k^{\mathcal{B}}(c_z) = \sum_{x,y}\left(\sum_z p(x,y,z)\chi_k(f(x,y,z) - c_z)\right)|x\rangle\langle y|\,. \tag{7.43}$$

Let us denote by $\omega_{\mathcal{B}}(g_3^{\ell})$ the maximum probability of success in the game $g_3^{\ell}(G, f, p)$ that can be achieved with a biseparable state. In Eq. (7.42) we have derived an upper bound for $\omega_{\mathcal{B}}^{C}$, which is the performance when the players share a quantum state biseparable with respect to the partition $AB|C$. In the case of Bell expressions which are invariant under the permutation of the parties, it is sufficient to consider Eq. (7.42) in order to bound $\omega_{\mathcal{B}}$. For general Bell inequalities, an upper bound on the biseparable bound, that holds for any state of the form given by Eq. (7.39), can be obtained by taking the maximum over all bipartitions, since

$$\omega_{\mathcal{B}} = \max_{X} \omega_{\mathcal{B}}^{X}, \tag{7.44}$$

where $X \in \{A, B, C\}$.

In general we have

$$\omega_c \leq \omega_{\mathcal{B}} \leq \omega_q \tag{7.45}$$

and then, for games where the strict relation $\omega_{\mathcal{B}} < \omega_q$ holds, by violating the biseparable bound $\omega_{\mathcal{B}}$ we can certify in a device-independent way that Alice, Bob and Charlie share a genuine tripartite entangled quantum state.

By using our norm bounds, Eq. (7.42), we have a simple way to upper bound the biseparable value of a Bell expression. Hence, our techniques of bounding the quantum value of linear games open the possibility of exploring higher dimensional device-independent witnesses of genuine tripartite entanglement.

We now exemplify the method by deriving a DIEW from a 3-input 3-output tripartite Bell expression.

Example:

Inspired by the Mermin's inequality [Mer90] for the GHZ paradox, we consider the following game that we denote g_3^{Mermin}: A referee picks questions $x, y, z \in \{0, 1, 2\}$ with the promise that $x + y + z = 0$. The players are supposed to give answers $a, b, c \in \{0, 1, 2\}$ in order to satisfy

$$g_3^{\text{Mermin}} : a + b + c = x \cdot y \cdot z\,, \quad \text{s.t.} \quad x + y + z = 0 \tag{7.46}$$

where the operations $+, \cdot$ are sum and multiplication modulo 3.

Substituting the winning condition of the game, Eq. (7.46), into Eq. (7.42) (note that the constraints of the game are invariant under the permutation of the parties), allows us to derive

$$\omega_{\mathcal{B}} \leq 0.896, \tag{7.47}$$

with RHS approximated up to the third decimal.

On the other hand, the GHZ_3 state defined as

$$|GHZ_3\rangle = \frac{|000\rangle + |111\rangle + |222\rangle}{\sqrt{3}}, \tag{7.48}$$

can win the game g_3^{Mermin} with probability 1.

Consequently, we have a device-independent witness of genuine tripartite entanglement: $\omega_{\mathcal{B}}(g_3^{\text{Mermin}}) \leq 0.896$.

The explicit measurements that lead the GHZ_3 to reach value one in the g_3^{Mermin} game are presented in Appendix E. However, an important property of these measurements is that they define traceless 'observables' (by the relation $A_x^i = \sum_a \bar{\chi}_i(a) M_x^a$):

$$\text{Tr}\left(A_x^i \otimes B_y^j \otimes C_z^k\right) = 0. \tag{7.49}$$

Therefore, we can easily calculate the success probability one can achieve with a noisy GHZ_3 state

$$\tilde{\rho}(V) = V\,|GHZ_3\rangle\langle GHZ_3| + (1-V)\frac{\mathbb{1}}{27}, \tag{7.50}$$

when these measurements are performed:

$$\begin{aligned}
\omega(\tilde{\rho}(V)) &= \frac{1}{3}\left(1 + \sum_{x,y,z}\sum_{k=1}^{2} p(x,y,z)\zeta^{k\cdot f(x,y,z)}\,\text{Tr}\left(\tilde{\rho}(V)(A_x^k \otimes B_y^k \otimes C_z^k)\right)\right) \\
&= \frac{1}{3} + \frac{V}{3}\sum_{x,y,z}\sum_{k=1}^{2} p(x,y,z)\zeta^{k\cdot f(x,y,z)}\,\text{Tr}\left(|GHZ_3\rangle\langle GHZ_3|\, A_x^k \otimes B_y^k \otimes C_z^k\right) \\
&= \frac{1-V}{3} + V\omega(|GHZ_3\rangle\langle GHZ_3|) \\
&= \frac{1+2V}{3}.
\end{aligned} \tag{7.51}$$

Hence, by using the optimal measurements for the GHZ_3 state we are able to witness genuine multipartite entanglement on noisy GHZ_3 state for parameter $V > 0.85$.

This example also stresses the difference between genuine multipartite entanglement and genuine multipartite nonlocality. Since the Svetlichny bound [Sve87] for this game is 1, it cannot be used as a witness of genuine tripartite nonlocality, despite being a good witness for genuine tripartite entanglement.

The 3-input 2-output witness presented in Ref. [BGLP11] can detect genuine multipartite entanglement in $\tilde{\rho}(V)$ for $V > 0.81$, however the two-outcome DIEW involves the calculation of 18 expected values whereas for the g_3^{Mermin} game, only 9 expected values are involved.

7.6 Discussion and open problems

In this Chapter we have extended the bound presented in Chapter 6 to n-player linear games. As for the bipartite case, the bound derived for multiplayer games is not tight in general, nevertheless we could apply it to derive non-trivial results. It would be interesting to characterize the classes of linear games for which the norm bound is tight. This could lead us to understand a bit more about the structure of the set of quantum correlations. In addition, the characterization of multiplayer games with no quantum advantage is interesting to highlight the limitations of quantum theory in the multipartite scenario. For multipartite Bell scenarios it is known that the quantum set of correlations contains facets [ABB$^+$10], it would be interesting to investigate if a multiplayer linear game can constitute a facet of the quantum set.

By using Theorem 7.2.2, we have proved upper bounds to the quantum value of a multipartite generalization of the CHSH-d game, for any number of players. Also, we have shown that boxes that trivialize communication complexity in the multipartite scenario cannot be realized in quantum theory. An important question for further investigation would be to analyze the relation between the bounds on linear games (bipartite and multipartite) we presented here and the communication complexity of the associated functions.

Finally, we have presented a systematic way to derive device independent witnesses of genuine tripartite entanglement. The method is very general and can be applied to any tripartite linear game in order to derive a DIEW of genuine tripartite entanglement with many inputs and outputs. We exhibited an example were a DIEW involving only 9 expected values is able to detect genuine tripartite entanglement in a noisy GHZ_3 state. It remains an open point whether these DIEWs with d outcomes are optimal in terms of the number of inputs to detect genuine tripartite entanglement of d-dimensional systems. The search for optimal witnesses with few inputs per player can lead to feasible applications and experiments.

It is important to stress that the bound derived in Theorem 7.2.2 involves the norm of matrices, which is an object with an intrinsic bipartite structure. A possible future direction would be to explore the use of tensors, which have a natural multipartite structure, in order to describe the games.

Final remarks

In this Thesis we have studied nonlocality focusing on the quantum value of a Bell expression. In particular, we took the approach of stressing how difficult is the problem of determining the quantum value of a Bell expression by situating it in the framework of computational complexity. In this framework, the main result of this Thesis can be summarized as: *efficiently computable upper bounds to the quantum value of linear games (a particular class of Bell inequalities).*

Those bounds are based on the spectral norm of some matrices associated to the games. The major advantage of our bounds is that they are easy to compute analytically for games with a small number of inputs and they can be implemented numerically by efficient algorithms. The drawback, however, is that the bounds are not tight in general and the quality of approximation is not known. Besides that, we could explore the bounds deriving several non-trivial results.

For the case of XOR games, the SDP characterization of the quantum value, due to Tsirelson's theorem, allowed us to derive necessary and sufficient conditions for a game to have no quantum advantage. This led to the characterization of a new family of graphs for which the Shannon capacity is equal to the independence number.

Concerning linear games with more outputs we could easily re-derive a recently discovered upper bound to the quantum value of the CHSH-d game, and we also extended it to the case of n players, the CHSH$_n$-d game. Also, we have shown that the norm bounds can exclude the existence of some boxes that would lead to trivialization of communication complexity in the bipartite and the multipartite case.

Furthermore, we defined an extension of the no-advantage for nonlocal computation principle, introduced in Ref. [LPSW07], to functions with d prime possible values. And finally, as the main outcome of exploring the norm bounds in the multipartite scenario, we presented a systematic way of deriving device-independent witnesses of genuine multipartite entanglement for tripartite systems.

In conclusion, we had a glance in the intricacy of quantum nonlocality by phrasing the problem of finding the maximal quantum violation of a Bell in-

equality in the framework of computational complexity. At the end of the day, I hope I have convinced the reader that finding simple bounds to this problem is a good game to play, or, at least, I hope the reader enjoyed it!

Appendix

Appendix A

Quantum Mechanics

In this Appendix we give an overview of Quantum theory, introducing the main concepts and properties discussed along the text. For an excellent introduction to the quantum theory formalism with an information theoretic approach the reader is referred to the book of Nielsen and Chuang [NC10].

A.1 A few concepts and definitions

In the study of nonlocality we usually adopt a minimalistic view of quantum theory: We do not exploit particular interactions among systems, or how is the dynamics of the systems and so on, other than that, we only capture the fundamental features and consequences of the mathematical formulation of quantum theory.

A.1.1 Concepts and axioms

Every quantum system has an associated complex Hilbert space $\mathcal{H}$ (*i.e.* a complete vector space with inner product). The system is mathematically described by a **quantum state**, which is an operator acting on $\mathcal{H}$. The quantum state contains all the information necessary to predict the statistics of the results of measurements performed in the system.

Definition A.1.1.a (Quantum state)**.** *A quantum state (also called density operator) is an operator $\rho \in D(\mathcal{H})$ with the following properties:*

(i) $\rho \geq 0$,

(ii) $\operatorname{Tr}\rho = 1$.

We denote the set of positive trace-1 operators acting on $\mathcal{H}$ by $D(\mathcal{H})$.

A very important particular case of quantum states are the **pure states**.

Definition A.1.1.b (Pure state)**.** *A pure state is a quantum state of rank 1, which means that they are one-dimensional projections*[1]*, $\rho = |\psi\rangle\langle\psi|$. A pure state can be represented by a vector $|\psi\rangle \in \mathcal{H}$.*

If a state is not pure we call it a **mixed state**.

Given that we know the quantum state of a physical system, quantum theory tells us how to predict the statistics of results of any experiment performed in the system. An experiment is a question that we are asking about our system and each experiment has its set of expected outcomes (*e.g.* when tossing a coin we have two possible outcomes: head or tail). In the quantum theory formalism, the experiments are described as following:

Definition A.1.2.a (Quantum measurements)**.** *A quantum measurement is described by a 'Positive Operator-Valued Measure' POVM, i.e. a set of m operators acting on $\mathcal{H}$, $\{M_i\}_{i=1}^m$ such that*

(i) $M_i \geq 0 \ \ \forall\, i = \{1, \ldots, m\}$,

(ii) $\sum_{i=1}^m M_i = \mathbb{1}$,

The M_i's are denoted elements of POVM and m is the number of possible outcomes of the measurement.

A particular case of POVM are the **Projective measurements**.

Definition A.1.2.b (Projective measurements)**.** *A projective measurement is the particular case of measurements where the all the POVM elements, $\{\Pi_i\}_{i=1}^m$, are orthogonal projectors i.e.*

1. $\Pi_i \Pi_j = \delta_{i,j} \Pi_i$,
2. $\sum_{i=1}^m \Pi_i = \mathbb{1}$.

The recipe for obtaining the probabilities of outcomes of experiments given these mathematical objects is state by Born's rule, introduced by Max Born in [Bor26].

[1] Note that the two vectors $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ give rise to the same density operator, therefore pure quantum states are defined up to a global phase.

Definition A.1.3 (Born rule). *If an m-outcome measurement, described by the POVM set* $\{M_i\}_{i=1}^m$*, is performed in a system described by a quantum state* ρ*, then the probability of obtaining the outcome k is given by*

$$P(k) = \mathrm{Tr}\left(M_k \rho\right). \tag{A.1a}$$

And for the particular case of projective measurement $\{\Pi_i\}_{i=1}^m$ *in a pure state* $|\psi\rangle$ *the probability of obtaining the outcome k is given by*

$$P(k) = \langle\psi| \Pi_k |\psi\rangle. \tag{A.1b}$$

A.1.2 Composite systems

When dealing with more than one system, or systems with many degrees of freedom, we have to establish a way to describe these systems in the formalism of quantum theory.

Given two single systems, A and B, with respective associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the composite system AB has an associated Hilbert space:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \tag{A.2}$$

Now, a very interesting phenomenon arises from this mathematical structure: the quantum states associated with system AB are still described by Definition A.1.1 and hence every positive operator of trace one acting on $\mathcal{H}_{AB}$ is an allowed quantum state. But **not** all quantum states of AB have the **product** structure:

$$\rho_{AB} = \sigma_A \otimes \sigma_B \quad \text{where} \quad \sigma_A \in D(\mathcal{H}_A) \quad \text{and} \quad \sigma_B \in D(\mathcal{H}_B),$$

and hence we have a rich structure arising from multipartite systems.

A quantum state of a bipartite system AB is a **separable state** if it can be approximated by a state of the form

$$\sigma_{AB} = \sum_i q(i) \sigma_A^i \otimes \sigma_B^i, \tag{A.3}$$

where $q(i)$ is a probability distribution, and $\sigma_A^i \in D(\mathcal{H}_A)$, $\sigma_B^i \in D(\mathcal{H}_B)$ are quantum states of single systems. Formally:

Definition A.1.4 (Separable states). *A quantum state* ρ_{AB} *is separable if for every* $\epsilon > 0$*, there exist* $N(\epsilon) \in \mathbb{N}$ *such that*

$$\left\| \rho_{AB} - \sum_{i=1}^{N} q(i) \sigma_A^i \otimes \sigma_B^i \right\|_1 < \epsilon \tag{A.4}$$

where $\|X\|_1 = \frac{1}{2} \mathrm{Tr}\,|X|$ *is the trace norm.*

Given a system with Hilbert space $\mathcal{H}_{AB}$, the set of all separable states is denoted SEP, and it is a closed convex set. For finite dimensional systems, $\mathcal{H}_{AB} = \mathbb{C}^d \otimes \mathbb{C}^d$, Carathéodory's theorem guarantees that every separable state can be written as a convex combination of at most $d^2 + 1$ pure separable states (*i.e.* states of the form $|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|$), and therefore every finite dimensional separable state has the for of Eq. (A.3).

If a quantum state is not separable, *i.e.* if it cannot be approximated by a separable decomposition (A.4), it is called an **entangled state**. Entanglement is in the core of the novelties brought by quantum theory. It gives rise to totally new phenomena with no classical analogue. As a remarkable example: the existence of entangled states gives rise to the quantum nonlocality.

Reduced state

When in possession of a multipartite system we might be interested in describing only part of it (or only few degrees of freedom). For that task we have the concept of **reduced state**.

Definition A.1.5 (Reduced state)**.** *Given a bipartite system in state ρ_{AB}, the reduced state of system A is given by*

$$\rho_A = \mathrm{Tr}_B \rho_{AB}, \tag{A.5}$$

and analogously for the reduced state of system B. Tr_B denotes partial trace[2] with respect to subsystem B. ρ_A is a positive operator with trace one acting on $\mathcal{H}_A$, and hence is a quantum state of system A.

The reduced state is the best description we can give for a subsystem, in case we ignore completely what is happening with the other subsystems. It is sufficient to describe the statistics of all local measurements (measurements performed only in the subsystem). If we have a composite system AB and we want to perform a POVM $\{M_{Ai}\}_{i=1}^m$ in the system A, this is equivalent to performing the measurement $\{M_{Ai} \otimes \mathbb{1}\}_{i=1}^m$ in the system AB, and the probability of getting an outcome k is given by

$$p(k) = \mathrm{Tr}_{AB}\left[(M_{Ak} \otimes \mathbb{1})\,\rho_{AB}\right] = \mathrm{Tr}_A\left(M_{Ak}\rho_A\right). \tag{A.6}$$

[2]The partial trace is a linear map, $\mathrm{Tr}_B : D(\mathcal{H}_{AB}) \longrightarrow D(\mathcal{H}_A)$, defined by

$$\mathrm{Tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2|\,\mathrm{Tr}(|b_1\rangle\langle b_2|),$$

and extended by linearity.

A very interesting fact is that the complete knowledge of the state of the parties do not allow us to recover the global state of the system, as in general

$$\rho_{AB} \neq \rho_A \otimes \rho_B. \tag{A.7}$$

For a separable state of the form $\rho_{AB} = \sum_i q(i)\sigma_A^i \otimes \sigma_B^i$ we have that

$$\rho_A = \mathrm{Tr}_B\, \rho_A B = \sum_i q(i)\sigma_A^i, \tag{A.8}$$

but the reduced state (A.8) does not uniquely recover the global state $\rho_{AB} = \sum_i q(i)\sigma_A^i \otimes \sigma_B^i$, and it could even correspond to the reduced state of a global entangled state.

A.2 Entanglement theory

We have presented the definition of an entangled state as the one which is not separable. However given a quantum state, checking whether or not it satisfies Eq. (A.4) is not an easy problem. In this section we briefly discuss entanglement detection and quantification.

A.2.1 Entanglement criteria

In general, given a finite dimensional quantum state, it is hard to conclude whether or not it can be written as Eq. (A.3). For pure states, however, the situation is much simpler, and we just have to look at the rank of the reduced state.

Proposition A.2.1. *A pure state* $|\psi\rangle_{AB}$ *is separable iff* $\mathrm{rank}(\rho_A) = 1$.

Proposition A.2.1 follows from the fact that $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$ is a rank one operator, and if it is separable it has to be written as the tensor product of rank one operators in $D(\mathcal{H}_A)$ and $D(\mathcal{H}_B)$.

For mixed states the situation is way harder, since a reduced state with rank greater than one leads us to no conclusion. Nevertheless it is possible to derive simple criteria that gives sufficient conditions for a state to be entangled. One of the most remarkable of these criteria was introduced by Peres in Ref. [Per96b]. Let us consider the **partial transposition** map, which is a linear map

$$\begin{aligned} T \otimes I : D(\mathcal{H}_{AB}) &\longrightarrow D(\mathcal{H}_{AB}) \\ \rho_{AB} &\longmapsto \rho_{AB}^{\Gamma}, \end{aligned} \tag{A.9}$$

where ρ_{AB}^{Γ} denotes the partial transposition of state ρ_{AB}. The action of $T \otimes I$ is to transpose the matrix ρ_{AB} with respect to subsystem A ($T \otimes I(|ab\rangle\langle a'b'|) = |a'b\rangle\langle ab'|$ and extended by linearity).

Let us look at the application of this map to a separable state (A.3):

$$\rho_{AB}^{\Gamma} = \sum_i q(i)(\sigma_A^i)^T \otimes \sigma_B^i, \tag{A.10}$$

where T denotes transposition. Since transposition is a trace preserve positive map we have that $(\sigma_A^i)^T$ are quantum states, hence ρ_{AB}^{Γ} is also a quantum state (*i.e.* it is a positive operator with trace one).

So we have seen that the application of the partial transposition map into a separable state results in a positive operator. But that is not true for every quantum state! Let us consider the maximally entangled 2-qubit state $\Phi = |\Phi\rangle\langle\Phi|$, $|\Phi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. A direct calculation shows that

$$\Phi^{\Gamma} \ngeq 0. \tag{A.11}$$

And we have just demonstrated our first entanglement criteria:

Proposition A.2.2 (The PPT criteria)**.** *If $\rho_{AB}^{\Gamma} \ngeq 0$ then ρ_{AB} is entangled.*

In Ref. [HHH96] the Horodeccy showed that the PPT criteria (also know as Peres-Horodecki criteria) is a necessary and sufficient condition for systems with Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathbb{C}^2 \otimes \mathbb{C}^3$, but only a sufficient condition for higher dimensional systems.

An interesting feature of the transposition is that it is a positive map that is not completely positive[3]. In Ref. [HHH96] it was shown that this is the main property that leads to an entanglement criteria. The same argument as above, applied to a generic map, implies that every separable state should remain positive under the application of a generic positive but not completely positive linear map. Hence each non-completely positive map can give rise to an entanglement criteria (a sufficient condition for a state to be entangled). But the breakthrough of Ref. [HHH96] comes with the proof that actually the formalism of positive but not completely positive maps can fully characterize the set of bipartite entangled states.

Theorem A.2.1 ([HHH96])**.** *A quantum state $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ is separable iff*

$$\Lambda \otimes \mathbb{1}(\rho_{AB}) \geq 0 \tag{A.12}$$

for any positive map $\Lambda : D(\mathcal{H}_A) \longrightarrow D(\mathcal{H}_B)$.

[3] A completely positive map is a positive map Λ such that any trivial extension $\Lambda \otimes \mathbb{1}$ is also a positive map.

A.2.2 Entanglement quantification

Let us start by the two most common operational ways to quantify entanglement: **distillable entanglement**, E_D, and **entanglement cost**, E_C. In the operational paradigm the unit of bipartite entanglement is the maximally entangled two qubit state, $|\psi^-\rangle = \frac{1}{2}(|01\rangle - |10\rangle)$. And the operations that are considered free are the **local operations and classical communication** (LOCC). Hence the E_D and E_C are defined in terms of how many resources, $|\psi^-\rangle$ states, one need or one can obtain out of a state ρ, when only LOCC operations are applied.

The paradigm of LOCC as free operations in entanglement theory is justified by the fact that entanglement cannot be created if only local operations and classical communication are available. LOCC operations can only generate a separable states (A.4). Conversely, any separable state can be created using LOCC.

Let us represent a general protocol (*i.e.* a set of maps/operations that take quantum states into quantum states) by Λ.

Definition A.2.1 (Distillable entanglement)**.** *A distillation protocol is an LOCC map that takes a certain number n of copies of a state ρ and turn it into another number, $r_d n$, of copies of $|\psi^-\rangle$:*

$$\rho^{\otimes n} \xrightarrow{\Lambda_{LOCC}} \Lambda_{LOCC}(\rho^{\otimes n}) \approx |\psi^-\rangle\langle\psi^-|^{\otimes r_d n} \tag{A.13}$$

where $\approx$ means that the states are asymptotically close in trace distance:

$$\|\Lambda_{LOCC}(\rho^{\otimes n}) - |\psi^-\rangle\langle\psi^-|^{\otimes r_d n}\| \xrightarrow{n\longrightarrow\infty} 0. \tag{A.14}$$

The distillable entanglement is defined as the best rate at which one can distil singlets out of the state ρ:

$$E_D = \sup_{\Lambda_{LOCC}} r_d. \tag{A.15}$$

In a similar way we have the cost of entanglement.

Definition A.2.2 (Entanglement cost)**.** *A creation protocol is a map that takes a certain number $r_c n$ of copies of the singlet state $|\psi^-\rangle$ and turn in into n copies of the state ρ:*

$$|\psi^-\rangle\langle\psi^-|^{\otimes r_c n} \xrightarrow{\Lambda_{LOCC}} \Lambda_{LOCC}(|\psi^-\rangle\langle\psi^-|^{\otimes r_c n}) \approx \rho^{\otimes n} \tag{A.16}$$

where $\approx$ means that the states are asymptotically close in trace distance:

$$\|\Lambda_{LOCC}(|\psi^-\rangle\langle\psi^-|^{\otimes r_c n}) - \rho^{\otimes n}\| \xrightarrow{n\longrightarrow\infty} 0. \tag{A.17}$$

The entanglement cost is defined as the best rate at which one can generate the state ρ:

$$E_C = \inf_{\Lambda_{LOCC}} r_c. \tag{A.18}$$

In general $E_D \leq E_C$, with equality carrying a meaning of reversibility. For pure states $E_D = E_C$, but for mixed states the strict relation can hold $E_D < E_C$. The entanglement cost is always strictly positive for an entangled state, however the distillable entanglement can be zero even though the state is entangled. There exist entangled states which cannot be distillable [HHH98], these are called **bound entangled** states. In particular it is known that states which do not violate the PPT criteria (Proposition A.2.2), *i.e.* states which are positive under partial transposition (that we call PPT states), cannot be distilled [HHH98]. Whether these are the only non-distillable states, or if there exists NPT states (states which are not positive under partial transposition) for which $E_D = 0$, is one of the big open problems in quantum information theory.

A.2.3 Multipartite entanglement

Multipartite systems have a much richer structure them the bipartite ones. Already in the tripartite case we have example of two inequivalent maximally entangled states. The states:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \tag{A.19}$$

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{A.20}$$

cannot be taken one into the other by any SLOCC protocol (*i.e.* an LOCC protocol that has a probability of success)[DVC00], whereas in the bipartite case, all the maximally entangled states are equivalent.

The generalization of separability for multipartite systems is straightforward. A finite dimensional[4] n-partite state is **separable** if it can be written as:

$$\rho = \sum_i p_i \rho_{A_1}^{(i)} \otimes \rho_{A_2}^{(i)} \otimes \ldots \otimes \rho_{A_n}^{(i)} \quad \text{s.t.} \quad p_i \geq 0\,, \sum_i p_i = 1. \tag{A.21}$$

But when it concerns entanglement in a multipartite system the situation is not so simple. It can be the case that all the parties share quantum correlations, in which case the state is said to be **genuinely multipartite entangled** (GME), or else, we can have a combination of states where only subsets of the parties share entanglement, which is called a **biseparable state**.

[4]Separability of infinite dimensional systems are defined analogously to Eq. (A.4).

Definition A.2.3 (Biseparable state)**.** *Let $S \subset \{1, \ldots, n\}$. An n-partite state $\rho_{\mathcal{B}}$ is biseparable if it can be decomposed into the form:*

$$\rho_{\mathcal{B}} = \sum_{S \neq \emptyset} \sum_{i_S} p_{i_S} \rho_{A_S}^{(i_S)} \otimes \rho_{A_{S^C}}^{(i_S)}, \tag{A.22}$$

where $\sum_{S \neq \emptyset} \sum_{i_S} p_{i_S} = 1$, $p_{i_S} \geq 0$, and S^C is the complement of S.

A state which is not biseparable is genuinely multipartite entangled. One can also define intermediate classes between biseparable and fully separable states, which are basically characterized by the number of subsystems that share entanglement.

In the tripartite case we have three possible bipartitions of the set of parties: $A|BC$, $B|CA$ and $C|AB$, and a general biseparable state is written as:

$$\rho_{\mathcal{B}} = \sum_{i_A} p_{i_A} \rho_A^{(i_A)} \otimes \rho_{BC}^{(i_A)} + \sum_{i_B} p_{i_B} \rho_B^{(i_B)} \otimes \rho_{CA}^{(i_B)} + \sum_{i_C} p_{i_C} \rho_C^{(i_C)} \otimes \rho_{AB}^{(i_C)}. \tag{A.23}$$

In order to explore a multipartite scenario in its full extent, one is usually interested in having a GME state. Detection of genuine multipartite entanglement is a fruitful area of research, but, for this task, there is no such direct criteria like the PPT-criteria. A connexion between positive maps and witnesses of genuine multipartite entanglement was established in Ref. [HS14]. There, a framework to construct witnesses of genuine multipartite entanglement from positive maps was derived. Other criteria to detect genuine multipartite entanglement were proposed in Refs. [MCC+11, HdV13]. And a device-independent witness of GME, based on Bell inequalities was proposed in [BGLP11]. A systematic method to derive device-independent witnesses of genuine tripartite entanglement was presented in Chapter 7.

Appendix B

State dependent bounds

In this Appendix we briefly describe the main results of Ref. [HM15]:

Bounds on quantum nonlocality via partial transposition
K. Horodecki and **G. Murta**
Phys. Rev. A, 92, 010301, (2015).

The quantitative study of quantum nonlocality has two opposite approaches: One is to ask, for a fixed Bell scenario, what is the highest violation one can obtain optimizing over all possible quantum resources (states and measurements); Another is to fix the quantum state, or a class of states, and ask what is the best one can achieve using this state as a nonlocal resource, *i.e.* optimizing over all Bell scenarios. In this thesis we have focused on the first approach, deriving bounds on the quantum value of a particular classes of Bell inequalities: the linear games. In Ref. [HM15] we have taken the opposite direction and asked *'How much nonlocality one can extract from a particular quantum state?'*.

B.1 Bound on single copy nonlocality

In this section we consider a standard Bell scenario where Alice and Bob share a single copy of a quantum state ρ_{AB} and perform local measurements on it, and we want to bound, for an arbitrary Bell inequality, the violation Alice and Bob can achieve by using ρ_{AB}.

Some previous results in this direction include the seminal work of Werner [Wer89] showing that some entangled quantum states cannot violate any Bell inequality[1]. Another general result shows that typically the violation of correlation Bell inequalities by multipartite qudit states is very small [DO12]. And

[1] The result of Werner [Wer89] concerns only projective measurements. It was extended for POVMs in Ref. [Bar02].

also an hierarchy of semidefinite programs that allows one to bound the violation achievable by a PPT state was developed in Ref. [MBL+13].

Our goal is to derive a state dependent bound for the violation of a particular Bell inequality. In order to achieve this goal, we explore the link between two concepts: the level of violation of a Bell inequality by a quantum state and discrimination between two states by means of a restricted classes of operations. Note that since only entangled quantum states can exhibit nonlocality, Bell inequalities can be viewed as particular cases of entanglement witnesses [HGBL05, Ter00]. Moreover, the test of a Bell inequality can be seen as the application of a separable operator to the quantum state. Therefore, we can say that a Bell inequality is an entanglement witness which only involves a restricted class of operations, the separable ones.

Definition B.1.1. *A separable operation is a quantum operation that can be written in the form:*

$$\Lambda_{sep}(\rho) = \sum_i K_i \rho K_i^\dagger \;\; s.t. \;\; K_i = K_{Ai} \otimes K_{Bi}. \tag{B.1}$$

The class of separable operations includes the LOCC operations, and they are a subset of a larger class called *PPT* operations.

Definition B.1.2. *A PPT operation is a quantum operation that can be written in the form:*

$$\Lambda_{PPT}(\rho) = \sum_i K_i \rho K_i^\dagger \;\; s.t. \;\; (K_i^\dagger K_i)^\Gamma \geq 0. \tag{B.2}$$

It is easier to impose the constraint that an operator is PPT compared to imposing separability. For this reason, PPT operations are used many times to upper bound results concerning separable and LOCC operations[YDY14].

The first surprising result concerning distinguishability of quantum states by a restricted class of operations was obtained in Ref. [BDF+99], where the authors showed the existence of a set of separable orthogonal states which cannot be perfectly distinguishable by any sequence of LOCC operations. Later, it was shown that there exist pairs of states which are hardly distinguishable from each other by means of LOCC, although being almost orthogonal. This gave rise to the **quantum data hiding**, which is the task of hiding classical bits in a quantum state [TDL01, DLT02, EW02]. In Ref. [Hor08] it is shown that there exist even entangled states containing a bit of private key, which are almost indistinguishable by LOCC operations from some separable (insecure) states. This fact has been shown recently to rule them out as a potential resource for swapping of a private key, in the so called quantum key repeaters [BCHW15].

Given a Bell expression $\mathcal{S}$, we denote by $\mathcal{S}_c$, $\mathcal{S}_q$ and $\mathcal{S}_{NS}$ respectively the classical, quantum and no-signaling value of this expression. For a particular bipartite state ρ_{AB} and local POVMs $\{M_x^a\}$ and $\{M_y^b\}$, we represent the corresponding box by $\vec{P}(a,b|x,y) \equiv \left\{\mathrm{Tr}(M_x^a \otimes M_y^b \rho_{AB})\right\}$. The value of the Bell expression $\mathcal{S}$ for these particular POVMs and state is denoted

$$\mathbf{S}(\rho_{AB}) = \mathrm{Tr}\, \mathbf{S}\rho_{AB}, \tag{B.3}$$

where

$$\mathbf{S} = \sum_{a,b,x,y} s_{x,y}^{a,b} M_x^a \otimes M_y^b \tag{B.4}$$

is the Bell operator for POVMs $\{M_x^a\}$ and $\{M_y^b\}$. Note that the Bell operator $\mathbf{S}$ is a separable operator (Definition B.1.1), so, intuitively, we expect that if a given state is hardly distinguishable from some separable one by means of separable operations, it cannot exhibit large violation in any Bell scenario, or else, one could use the procedure of checking the violation of a Bell inequality to discriminate between these two states. We now make this idea quantitative and state our first result, relating the value of a Bell expression on two bipartite states to the their distinguishability by means of *PPT* operations.

Lemma B.1.1. *Given two states $\rho, \sigma \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$, a Bell expression $\mathcal{S} = \left\{s_{x,y}^{a,b}\right\}$ and a set of POVMs $\{M_x^a\}, \{M_y^b\}$, it holds that:*

$$|\mathbf{S}(\rho) - \mathbf{S}(\sigma)| \leq \|\mathbf{S}^\Gamma\|_\infty \|\rho^\Gamma - \sigma^\Gamma\|_1. \tag{B.5}$$

where $\|\cdot\|_1$ denotes the trace norm, $\|X\|_\infty$ is the largest eigenvalue in modulus of operator X (which is equivalent to the spectral norm), and Γ denotes partial transposition.

Note that $\mathbf{S}^\Gamma$ is also a Bell operator, since partial transposition maps the POVMs $\{M_x^a \otimes M_y^b\}$ into another set of allowed measurements $\{M_x^a \otimes (M_y^b)^T\}$, and $\|\mathbf{S}^\Gamma\|_\infty$ is nothing but the largest quantum value of the Bell expression $\mathbf{S}$ given the particular measurements $\{M_x^a \otimes (M_y^b)^T\}$. The second term on the RHS represents the distinguishability of these two states by means of PPT operations. Calculating distinguishability by separable operations is a hard problem since there is no simple description for the set of separable operations. A relaxation of this problem is to consider the set of PPT operations which is much simpler to characterize [Rai01]. A weaker form of Lemma B.1.1, concerning distinguishability under general measurements, was similarly derived in Ref. [BV12].

Proof.

$$\begin{aligned}
|\mathbf{S}(\rho) - \mathbf{S}(\sigma)| =& |\sum_{a,b,x,y} \operatorname{Tr} s^{a,b}_{x,y} M^a_x \otimes M^b_y (\rho - \sigma)| \\
=& |\sum_{a,b,x,y} \operatorname{Tr} s^{a,b}_{x,y} M^a_x \otimes (M^b_y)^T (\rho - \sigma)^\Gamma| \\
=& |\operatorname{Tr}\ \mathbf{S}^\Gamma (\rho^\Gamma - \sigma^\Gamma)| \\
\leq& \operatorname{Tr}\ |\mathbf{S}^\Gamma (\rho^\Gamma - \sigma^\Gamma)| \\
\leq& \|\mathbf{S}^\Gamma\|_\infty \|\rho^\Gamma - \sigma^\Gamma\|_1.
\end{aligned} \tag{B.6}$$

In the first and second equality we used the linearity of the trace, then the identity $\operatorname{Tr} XY = \operatorname{Tr} X^\Gamma Y^\Gamma$. In the fourth step we used the triangle inequality, and the last step follows from Hölder's inequality for $p-$norms, which states that $\|XY\|_1 \leq \|X\|_\infty \|Y\|_1$. □

As we have discussed in Chapter 1, separable states can only generate local boxes. Therefore, we have that

$$\mathbf{S}(\sigma_{AB}) \leq \mathcal{S}_c \ \ \forall\ \sigma_{AB} \in SEP. \tag{B.7}$$

Given this observation, we can derive the main result of this Section.

Theorem B.1.1. *For any bipartite Bell expression $\mathcal{S}$, and state ρ, it holds that:*

$$\mathcal{S}(\rho) \leq \mathcal{S}_c + \mathcal{S}_q \inf_{\sigma \in SEP} \|\rho^\Gamma - \sigma\|_1. \tag{B.8}$$

where

$$\mathcal{S}(\rho) := \sup_{\{M^a_x\},\{M^b_y\}} \sum_{a,b,x,y} s^{a,b}_{x,y} \operatorname{Tr}(M^a_x \otimes M^b_y \rho), \tag{B.9}$$

with supremum taken over all POVMs $\{M^a_x\}$ and $\{M^b_y\}$.

Proof. By substituting any separable state σ in Lemma B.1.1, and using the fact that $\mathbf{S}(\sigma_{AB}) \leq \mathcal{S}_c \ \ \forall\ \sigma_{AB} \in SEP$ we have:

$$\mathbf{S}(\rho) \leq \mathcal{S}_c + \|\mathbf{S}^\Gamma\|_\infty \|\rho^\Gamma - \sigma^\Gamma\|_1. \tag{B.10}$$

Now taking supremum over POVMs $\{M^a_x\}$, $\{M^b_y\}$ on both sides, and infimum over all separable states σ, we have the desired result . Note that $\mathcal{S}_q = \sup_\rho \mathcal{S}(\rho)$, and that $\|\mathbf{S}^\Gamma\|_\infty$ is upper bounded by $\mathcal{S}_q$. □

Theorem B.1.1 shows that, given a Bell inequality $\mathcal{S}$, the best violation one can achieve with a particular quantum state ρ cannot outperform the classical bound by the quantum value of the Bell inequality shrunk by a factor reporting the distinguishability of state ρ from the set of separable states by means of PPT operations. Since the bound (B.8) only depends on the distance to the set of separable states, every state which is distinguishable from a separable state by the same content ϵ will exhibit the same limitations in a Bell scenario. Hence we can define the sets

$$D(\epsilon) := \{\rho : \exists_{\sigma \in SEP} \ \|\rho^{\Gamma} - \sigma\| \leq \epsilon\}. \tag{B.11}$$

Observe that $D(\epsilon)$ is a convex set, which includes the set of separable states SEP for any $\epsilon > 0$. Due to Theorem B.1.1, we have the following dependence (see Fig. B.1):

$$\sup_{\rho \in D(\epsilon)} \mathcal{S}(\rho) \leq \mathcal{S}_c + \epsilon \mathcal{S}_q. \tag{B.12}$$

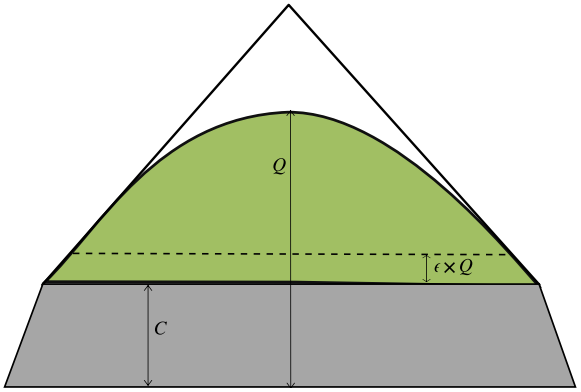


Figure B.1: For states in $D(\epsilon)$, Eq. (B.11), the violation of a Bell inequality $\mathcal{S}$ is limited by its quantum value $\mathcal{S}_q$ shrunk by ϵ (dashed line).

B.2 Bound on the asymptotic scenario

In the previous section we have considered the standard Bell scenario, where a single copy of a bipartite state is shared between Alice and Bob. However, if the state ρ_{AB} is distillable, as it was noted by Peres [Per96a], a pre-processing of many copies of a state by LOCC, before the Bell test, could lead to the violation of a Bell inequality, even for states that have local model in the standard

scenario. Here we quantify the asymptotic nonlocality by defining the asymptotic relative entropy of nonlocality and applying methods of Ref. [BCHW15] to bound it. In the first step, we will bound this quantity by a function of the relative entropy distance under restrictive measurements introduced by Piani in Ref. [Pia09].

In Ref. [vDGG05] a nonlocality quantifier, based on the relative entropy, was introduced. The relative entropy between two probability distributions, P and Q, is defined as $D(P||Q) \equiv \sum_i P(i) \log \frac{P(i)}{Q(i)}$. The **statistical strength of nonlocality** defined in Ref. [vDGG05] captures quantitatively how "similar" a given probability distribution is to a local one: Given a box $\vec{P}(ab|xy)$, where for fixed x, y we have distribution $P_{xy}(ab|xy)$, its nonlocality is quantified by

$$\mathcal{N}(\vec{P}) = \sup_{\{p(x,y)\}} \inf_{P_L \in \mathcal{L}} \sum_{x,y} p(x,y) D(P_{xy}(ab|xy)||P_L(ab|x,y)), \tag{B.13}$$

where infimum in the above is taken over all local boxes, $\vec{P}(ab|xy) \in \mathcal{L}$, for the particular scenario and $D(P||Q)$ is the relative entropy.

Now, we are interested in quantifying how much nonlocality $\mathcal{N}$ one can obtain from n copies of a given state ρ_{AB}, per number of copies, in the asymptotic limit, after processing it by LOCC. For that we introduce the **asymptotic relative entropy of nonlocality**.

Definition B.2.1. *For a bipartite state ρ_{AB} its asymptotic relative entropy of nonlocality, $R(\rho_{AB})$, is given by:*

$$R(\rho_{AB}) \equiv \overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda \in LOCC} \sup_{\{M_{xy}\}} \mathcal{N}(\{\mathrm{Tr}\, M_{xy} \Lambda(\rho_{AB}^{\otimes n})\}), \tag{B.14}$$

where $\overline{\lim}$ is the supremum limit, and $\{M_{xy}\}$ denote local POVMs $M_{xy} = M_x^a \otimes M_y^b$.

The asymptotic relative entropy of nonlocality captures the idea of an optimization over all Bell scenarios after a pre-processing of many copies of a quantum state ρ_{AB} by LOCC operations.

We want to set bounds for the nonlocality attainable in the asymptotic scenario. In order to state the bound, we will need a well known entanglement measure called **relative entropy of entanglement** [VPRK97]:

$$E_r(\rho) = \inf_{\sigma \in SEP} S(\rho||\sigma), \tag{B.15}$$

where $S(\rho||\sigma) = \mathrm{Tr}\, \rho \log \rho - \mathrm{Tr}\, \rho \log \sigma$ is the quantum relative entropy.

Now we are ready to state the main result of this Section.

Theorem B.2.1. *For any bipartite state it holds that*

$$R(\rho_{AB}) \leq E_r(\rho_{AB}). \tag{B.16}$$

For ρ_{AB} a PPT state, it holds that

$$R(\rho_{AB}) \leq \min\left\{E_r(\rho_{AB}), E_r(\rho_{AB}^{\Gamma})\right\}. \tag{B.17}$$

The upper bound $R(\rho_{AB}) \leq E_r(\rho_{AB})$ gives meaningful results only when the state is close to separable states under global operations. More important is the second bound, which can give meaningful results even for some states which are highly distinguishable from separable states by global operations, but cannot be distinguished if only PPT operations are allowed. We refer the reader to Ref. [HM15] for the proof of Theorem B.2.1.

We can also extend Theorem B.2.1 to asymptotic scenarios where the parties can perform a 'filtering' operation (a non-trace-preserving map) before the Bell test: the so called hidden nonlocality scenario, introduced by Popescu in Ref. [Pop95]. Popescu showed that by performing a 'filtering' operation it is possible to obtain a much larger violation of a Bell inequality on the resulting state. However, we note that, in order to quantify nonlocality in this scenario, it is important to take into account the probability of obtaining the 'filtered' result. For this reason, we propose to consider the **asymptotic relative entropy of hidden-nonlocality**, $R_H(\rho_{AB})$, defined as follows:

$$R_H(\rho_{AB}) \equiv \overline{\lim_{n\to\infty}} \frac{1}{n} \sup_{\Lambda\in LOCC} \sup_{\{M_{xy}\}} \sup_{F_0} p^{F_0}\mathcal{N}(\{\mathrm{Tr}\, M_{xy}F_0(\Lambda(\rho_{AB}^{\otimes n}))\}). \tag{B.18}$$

Where we can see a filtering process F_0 as an operation that takes the state $\Lambda(\rho_{AB}^{\otimes n})$ to a flag form

$$F(\rho) = \sum_i |i\rangle\langle i| \otimes F_i \rho F_i^{\dagger}, \tag{B.19}$$

and later erasures all other results except the "good" one, that leads to the highest violation of the Bell inequality. The probability that the filter results in the desired outcome is given by

$$p^{F_0} = \mathrm{Tr}\, F_0 \Lambda(\rho_{AB}^{\otimes n}) F_0^{\dagger}. \tag{B.20}$$

We can have the same bound for R_H, as for R.

Theorem B.2.2. *For any bipartite state ρ_{AB} it holds that*

$$R_H(\rho_{AB}) \leq E_r(\rho_{AB}). \tag{B.21}$$

For a bipartite PPT state ρ_{AB} it holds that

$$R_H(\rho_{AB}) \leq \min\left\{E_r(\rho_{AB}), E_r(\rho_{AB}^{\Gamma})\right\}. \tag{B.22}$$

B.3 Examples

In Ref. [HHHO05], it was shown that the general form of a quantum state from which it is possible to extract one bit of classical private key, a **private bit**, is given by

$$\gamma_X = \frac{1}{2}[|00\rangle\langle 00| \otimes \sqrt{XX^\dagger} + |00\rangle\langle 11| \otimes X + |11\rangle\langle 00| \otimes X^\dagger + |11\rangle\langle 11| \otimes \sqrt{X^\dagger X}],$$

where X is an arbitrary operator with trace norm 1 acting on $\mathbb{C}^{d_s} \otimes \mathbb{C}^{d_s}$. .

Consider a private state defined by $X = \frac{1}{d^2}\sum_{i,j=0}^{d-1} |ij\rangle\langle ji|$ being the (normalized) swap operator. Then for the CHSH inequality we have the following bound [Hor08]:

$$Q_{CHSH}(\gamma_X) \leq 2 + \frac{\sqrt{2}+1}{2\sqrt{2}d}. \tag{B.23}$$

In [ACPA10] it was shown that all perfect private states violate the CHSH inequality. With our techniques we can bound this violation and also analyze PPT approximate private states.

Consider the following PPT approximate private state:

$$\rho_p = (1-p)\gamma_X + \frac{p}{2}[|01\rangle\langle 01| \otimes \sqrt{YY^\dagger} + |10\rangle\langle 10| \otimes \sqrt{Y^\dagger Y}] \tag{B.24}$$

with $X = \frac{1}{d_s\sqrt{d_s}}\sum_{i,j=0}^{d_s-1} u_{ij}|ij\rangle\langle ji|$ and $Y = \sqrt{d_s}X^\Gamma$, $|u_{ij}| = \frac{1}{d_s}$, and $p = \frac{1}{\sqrt{d_s}+1}$. By Theorem B.1.1, we have

$$Q_{\mathcal{S}}(\rho_p) \leq \mathcal{S}_c + \mathcal{S}_q\frac{1}{\sqrt{d_s}}. \tag{B.25}$$

In Ref. [HHHO05], it was shown that there exists a family of states invariant under partial transposition for which the distillable key can be made arbitrarily close to one, $K_D \to 1$. By applying Theorem B.1.1 to this family of states we obtain the following proposition.

Proposition B.3.1. *There exist bipartite states* $\rho \in B(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes (\mathbb{C}^{d^k} \otimes \mathbb{C}^{d^k})^{\otimes m})$ *with* $d = m^2$, $k = m$ *satisfying* $K_D(\rho^\Gamma \otimes \rho) \to 1$ *with increasing* m, *such that:*

$$Q_{\mathcal{S}}(\rho \otimes \rho^\Gamma) \leq \mathcal{S}_c + \frac{\mathcal{S}_q}{2^{m-1}}. \tag{B.26}$$

Proposition B.3.1 shows that for the class of states in consideration, although the rate of distillable key can be made arbitrarily close to one by increasing the dimension of the systems, the possibility of violating any Bell inequality is bounded by an amount vanishing with the dimension of the system. For a bipartite Bell inequality with n inputs and k outputs it holds that $\mathcal{S}_q \leq \mathcal{S}_c \times \min\{n, k\}$, up to some universal constant independent of the parameters of the scenario [JP11]. Therefore, Theorem B.1.1 ensures that for any fixed Bell scenario, as we wish to increase the key rate obtained from the exhibited family of states, the possibility of observing a violation of a Bell inequality vanishes.

An application of Theorems B.2.1 and B.2.2 follows from the fact that the relative entropy of entanglement, E_r, is asymptotically continuous[2][SRH06]. Generally, for $\rho_\epsilon \in D(\epsilon)$, and $\epsilon < \frac{1}{2}$, we have:

$$R_{(H)}(\rho_\epsilon) \leq 4\epsilon \log d + 2h(\epsilon)$$

Hence, if ϵ decreases with d faster than $\frac{1}{\log d}$, the asymptotic relative entropy of nonlocality vanishes with increasing dimension The family of states shown in Eq. (B.24) have this property.

B.4 Discussion and open problems

We have presented bounds on the quantum nonlocality of a bipartite state, both, in the single copy case, as well as in the asymptotic scenarios. Although we use partial transposition techniques for obtaining nontrivial results, our method is based on the concept of state discrimination via a restricted classes of operations: the separable ones.

As future directions exploring the bounds: For the single copy scenario, instead of discrimination from separable states, a refinement would be to consider

[2] A function $f : D(\mathbb{C}^d) \longrightarrow \mathbb{R}$ is asymptotically continuous if

$$|f(\rho_1) - f(\rho_2)| \leq K\|\rho_1 - \rho_2\|_1 \log d + g(\|\rho_1 - \rho_2\|_1) \tag{B.27}$$

where K is a constant and $g(\epsilon) \xrightarrow{\epsilon \longrightarrow 0} 0$.

the distance from states admitting a local hidden-variable model, which could possibly lead to tighter bounds; For the asymptotic scenarios, it would be interesting to find nontrivial upper bounds on the asymptotic relative entropy of (hidden) nonlocality of NPT states. Note that, for these states, we only have $E_R(\rho)$ as an upper bound, which is small only for the cases where the state is almost indistinguishable from a separable state under global operations.

In Refs. [HHH+08, HLLO06] it was shown that one can launch quantum key distribution (QKD) protocols based on shared private bits. However, if we are interested in device-independent quantum key distribution (DI QKD) protocols we need to have a violate of some Bell inequality. A DI QKD protocol is based on some Bell inequality $\mathcal{S}$, and admits some level of violation, say ϵ_v, below which it aborts. Now, due to Eqs. (B.25) and (B.26) there are (approximate) private bits, which exhibit violation of inequality $\mathcal{S}$ only up to $\epsilon' < \epsilon_v$, and hence will be aborted. This rules out such states from usage in this particular DI QKD protocol. Moreover, every realization of a DI QKD has inevitable errors. In such a case, the level of violation ϵ' can be even below the precision of the experiment. An interesting question for further investigation is the difference in terms of key rates between QKD and DI QKD protocols.

It is worth noting, that our results are strongly related to the so called *Peres conjecture* [Per99], recently disproved in [VB14]. Namely, we have asked a quantitative rephrasing of the original question posed by Asher Peres: how much one can violate a Bell inequality with PPT states? We have shown that, for *certain* PPT states, the level of violation, both for single copy as well as in terms of the relative entropy of (hidden) nonlocality in the asymptotic cases, can be negligible. Notably, as we showed in the examples, even some states containing privacy admit such limited nonlocality content.

Appendix C

A group of facts about groups

In Chapters 6 and 7 we have discussed a class of games associated to finite Abelian groups. Here we state some results and properties of finite Abelian groups. For more details the reader in referred to the book [Ter99].

C.1 Some definitions

Definition C.1 (Group). *A group $(G, \circ)$ is a set of elements $a \in G$ with the associated operation $\circ$ satisfying*

(i) $a \circ b \in G, \forall a, b \in G,$

(ii) $\exists\, e$ *s.t.* $a \circ e = a, \forall a \in G,$

(iii) $\forall\, a, \exists\, a^{-1}$ *s.t.* $a \circ a^{-1} = a^{-1} \circ a = e,$

(iv) Associativity holds: $\forall a, b, c \in G$

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Definition C.2 (Abelian group). *An Abelian group $(G, +)$ is a group with associated operation denoted by $+$ that, additionally to properties (i)-(iv), also satisfies commutativity:*

$$a + b = b + a \quad \forall a, b \in G. \tag{C.1}$$

Definition C.3 (Cyclic group). *A group is called cyclic if it can be generated by a single element $g \in G$, called the* ***generator*** *of the group.*

A finite cyclic group is a group with the property that all the elements can be obtained by starting with the generator g and applying the group operation to it many times, *i.e.* $G = \{g, (g \circ g), ((g \circ g) \circ g), \ldots\}$. This makes it clear that all finite cyclic groups are Abelian groups.

Definition C.4 (Homomorphism)**.** *An homomorphism of a group $(G, \circ)$ into a group $(H, \circ)$ is a function $f : G \longrightarrow H$ such that*

$$f(a \circ b) = f(a) \circ f(b) \quad \forall\, a, b \in G \tag{C.2}$$

A remarkable example of these concepts is given by the cyclic group $\mathbb{Z}_d$, for which:

- $G = \{0, \ldots, d-1\}$.
- The associated operation $+$ is the sum modulo d.
- The identity element is $e = 0$.
- The inverse element of a is $a^{-1} = -a = d - a$.
- $g = 1$ is a generator[1] for all d.
- An homomorphism from $\mathbb{Z}_d$ to the group $\mathbb{T}$ of unitary complex numbers with the product operation is given by

$$a \longmapsto e^{\frac{2\pi i a}{d}} \quad \forall\, a \in \{0, \ldots, d-1\}\,. \tag{C.3}$$

C.2 The characters of an Abelian group

Definition C.5. *A character χ_j of a finite Abelian group $(G, +)$ is a group homomorphism from $(G, +)$ to the group $\mathbb{T}$ of unitary complex numbers with the product operation:*

$$\chi_j : a \mapsto \chi_j(a). \tag{C.4}$$

By Definition C.5 we have that the characters of an Abelian group are complex numbers satisfying the properties:

$$\begin{cases} \text{Homomorphism:} & \chi_j(a+b) = \chi_j(a)\chi_j(b) \quad \forall a, b \in G, \\ \text{Reflexivity:} & \bar{\chi}_j(a) = \chi_j(-a), \\ \text{Orthogonality:} & \sum_{a \in G} \chi_i(a)\bar{\chi}_j(a) = |G|\, \delta_{i,j}. \end{cases} \tag{C.5}$$

[1] A cyclic group can have more than one generator. For example, for prime d, every element of $\mathbb{Z}_d$ is a generator.

For the cyclic group $\mathbb{Z}_d$, the characters are the d roots of unit

$$\chi_j(a) = \zeta^{ja} \quad \text{for} \quad j \in \{0, \ldots, d-1\}, \tag{C.6}$$

where $\zeta = e^{2\pi \mathrm{i}/d}$.

A very interesting result is the called **fundamental theorem of finite Abelian groups** (see Ref. [Ter99]), which states that any finite Abelian group $(G, +)$ can be seen as a direct product of cyclic groups

$$(G, +) \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}, \tag{C.7}$$

where every element $x \in G$ is as a r-tuple $(x_1, \ldots, x_r)$ with $x_i \in \mathbb{Z}_{d_i}$ and the operation in $(G, +)$ is given by

$$(x_1, \ldots, x_r) + (y_1, \ldots, y_r) = (x_1 + y_1, \ldots, x_r + y_r). \tag{C.8}$$

With this characterization, the characters χ_j of the Abelian group $(G, +)$, can be written as the product of the characters of the cyclic groups that compose $(G, +)$:

$$\chi_k(a) = \prod_{j=1}^{r} \chi_{k_j}(a_j), \tag{C.9}$$

where $\chi_{k_j}(a_j) = e^{\frac{2\pi \mathrm{i} k_j a_j}{d_j}}$ is a d_j-th root of unity, and $a_j \in \mathbb{Z}_{d_j}$.

C.3 The Fourier transform over finite Abelian groups

A Fourier transform can be seen as a change of basis, where we pass from a description of a function f in terms of a set of variables to a description in terms of different variables, but keeping all the information about f. When we have a function of the elements of a finite Abelian group, the Fourier transform can be expressed in terms of the characters of the group.

Let f be a complex valued function on the finite Abelian group $(G, +)$

$$f : (G, +) \longrightarrow \mathbb{C}.$$

The Fourier transform of f is defined as :

$$\hat{f}(\chi_i) = \sum_{a \in G} \bar{\chi}_i(a) f(a), \tag{C.10}$$

with the inverse given by

$$f(a) = \frac{1}{|G|} \sum_{j \in G} \chi_i(a) \hat{f}(\chi_i). \tag{C.11}$$

For non-Abelian groups the characters are more subtle, and the Fourier transform uses the irreducible representations of the group. For the reader interested in a further reading about Fourier transform on groups we refer to Ref. [Ter99].

C.4 Finite Fields

Fields are sets which have more structure than an Abelian group. While for an Abelian group $(G, +)$ we only have the associated sum operation $+$, a field $\mathbb{F}_d$ has two associated operations $+$ and $\cdot$ satisfying the properties specified bellow.

Definition C.6 (Finite Field). *A finite field $\mathbb{F}_d$ is a set of d elements with the operations sum $+$ and multiplication $\cdot$ such that*

(i) $a + b, a \cdot b \in \mathbb{F}_d, \forall a, b \in \mathbb{F}_d$,

(ii) $\exists\ 0\ s.t.\ a + 0 = a, \forall a \in \mathbb{F}_d$,

(iii) $\exists\ 1\ s.t.\ a \cdot 1 = a, \forall a \in \mathbb{F}_d$,

(iv) $\forall\ a, \exists\ -a\ s.t.\ a + (-a) = 0$,

(v) $\forall\ b \neq 0, \exists\ b^{-1}\ s.t.\ b \cdot b^{-1} = 1$,

(vi) Associativity: $\forall a, b, c\ \in \mathbb{F}_d$

$$a + (b + c) = (a + b) + c$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(vii) Commutativity: $\forall a, b\ \in \mathbb{F}_d$

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

(viii) Distributivity: $\forall a, b, c\ \in \mathbb{F}_d$

$$a \cdot (b + c) = a \cdot b + a \cdot c. \tag{C.12}$$

Finite fields can only be defined for a set of d prime or a power of prime elements. For d prime all the conditions (i)-$(viii)$ can be satisfied by arithmetic modulo d. For $d = p^r$ the arithmetic operations[2] can be defined by addition

[2] See https://en.wikipedia.org/wiki/Finite_field_arithmetic.

and multiplication of polynomials of degree $< r$ over $\mathbb{Z}_p$, $\mathbb{Z}_p[X]$. In order to construct a field $\mathbb{F}_{p^r}$ one can start by choosing an irreducible polynomial of degree r over $\mathbb{Z}_p$, this polynomial will define the zero of the field by the so called quotient.

As an example for the field $\mathbb{F}_d$ with $d = 2^3$ we can pick the polynomial $X^3 + X + 1 \in \mathbb{Z}_2[X]$ from which we can obtain the relation

$$X^3 + X + 1 = 0 \Rightarrow X^3 = X + 1. \tag{C.13}$$

Now the elements of the field can be represented by strings (a, b, c), with $a, b, c \in \{0, 1\}$, and we can associate each string with the polynomial $aX^2 + bX + c$. Given that, addition and multiplication will be taken as addition and multiplication of polynomials reduced by the relation (C.13).

Appendix D

Functional boxes and multipartite communication complexity

Here we discuss functional boxes and the communication complexity task in the multipartite scenario. These results were also presented in Ref. [MRMT16].

We start by defining the PR_n-d boxes, a generalization of PR boxes [PR94] for n parties and prime d outputs.

Definition D.1.

$$PR_n\text{-}d(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{d^{n-1}}, \text{ if } a_1 + \ldots + a_n = x_1 \cdot \ldots \cdot x_n \\ 0, \text{ otherwise} \end{cases} \tag{D.1}$$

where d is prime and sum $+$ and multiplication $\cdot$ are operations modulo d.

A multipartite communication complexity scenario consists of n parties, denoted $A_1, \ldots, A_n$, where each party A_i receives an input x_i, and their goal is to exchange the least number of classical messages in order to compute the value of a global function of their inputs $f(x_1, \ldots, x_n)$.

In what follows we prove that if the n parties have access to a sufficient large amount of PR_n-d boxes, they can compute any function $f(x_1, \ldots, x_n)$ with only $n-1$ dits of communication: where each player $A_{i\neq 1}$ communicate one dit to player A_1 which them computes the function.

Theorem D.1. *If n parties are allowed to share an arbitrary number of PR_n-d boxes, any n-partite communication complexity problem can be solved with only $n-1$ dits of communication.*

Proof. Our proof is a straightforward generalization of Ref. [Wan11]. We prove for the case $n = 3$. The proof for general n follows directly.

Let us consider that Alice receives input string $\vec{x} \in \mathbb{Z}_d^{m_1}$, Bob receives $\vec{y} \in \mathbb{Z}_d^{m_2}$ and Charlie receives $\vec{z} \in \mathbb{Z}_d^{m_3}$. We start by observing that any function $f(\vec{x},\vec{y},\vec{z})$, $f : \mathbb{Z}_d^{m_1} \times \mathbb{Z}_d^{m_2} \times \mathbb{Z}_d^{m_3} \to \mathbb{Z}_d$, can be written as a multivariate polynomial with degree at most $d-1$ in each variable x_i, y_j and z_k

$$f(\vec{x},\vec{y},\vec{z}) = \sum_{\vec{\alpha},\vec{\beta},\vec{\gamma}} \mu_{\vec{\alpha},\vec{\beta},\vec{\gamma}}\, \vec{x}^{\vec{\alpha}}\, \vec{y}^{\vec{\beta}}\, \vec{z}^{\vec{\gamma}}, \tag{D.2}$$

where $\vec{x}^{\vec{\alpha}} = \prod_{i=1}^{m_1} x_i^{\alpha_i}$, $\vec{y}^{\vec{\beta}} = \prod_{j=1}^{m_2} y_j^{\beta_j}$, $\vec{z}^{\vec{\gamma}} = \prod_{k=1}^{m_3} z_k^{\gamma_k}$, $\mu_{\vec{\alpha},\vec{\beta},\vec{\gamma}} \in \mathbb{Z}_d$, and $\vec{\alpha} = (\alpha_1,\ldots,\alpha_{m_1}) \in \mathbb{Z}_d^{m_1}$. And analogously for $\vec{\beta}$ and $\vec{\gamma}$. Now if the players have access to $r = d^{m_1 m_2 m_3}$ PR_3-d boxes they can execute the following protocol in order to compute $f(\vec{x},\vec{y},\vec{z})$:

1. For each $(\vec{\alpha},\vec{\beta},\vec{\gamma})$ the players picks one PR_3-d,
2. Alice inputs $\vec{x}^{\vec{\alpha}} = \prod_{i=1}^{m_1} x_i^{\alpha_i}$. Bob inputs $\vec{y}^{\vec{\beta}} = \prod_{j=1}^{m_2} y_j^{\beta_j}$. Charlie inputs $\vec{z}^{\vec{\gamma}} = \prod_{k=1}^{m_3} z_k^{\gamma_k}$. And they get respectively the outputs $a_{\vec{\alpha}}$, $b_{\vec{\beta}}$ and $c_{\vec{\gamma}}$.
3. Bob sets $b = \sum_{\vec{\alpha}} \sum_{\vec{\beta}} \sum_{\vec{\gamma}} \mu_{\vec{\alpha},\vec{\beta},\vec{\gamma}} b_{\vec{\beta}}$ and send b to Alice. Charlie sets $c = \sum_{\vec{\alpha}} \sum_{\vec{\beta}} \sum_{\vec{\gamma}} \mu_{\vec{\alpha},\vec{\beta},\vec{\gamma}} c_{\vec{\gamma}}$ and send c to Alice.
4. Alice sets $a = \sum_{\vec{\alpha}} \sum_{\vec{\beta}} \sum_{\vec{\gamma}} \mu_{\vec{\alpha},\vec{\beta},\vec{\gamma}} a_{\vec{\alpha}}$ and she computes $f(\vec{x},\vec{y},\vec{z}) = a + b + c$.

where only 2 dits were communicated in order to compute the function.

The generalization for n-party function follows in analogous way, where any function $f : \mathbb{Z}_d^{m_1} \times \ldots \times \mathbb{Z}_d^{m_n} \to \mathbb{Z}_d$ will be written as a multivariate polynomial with degree at most $d-1$ in each variable and using an analogous protocol, with $n-1$ parties communicating only one dit to the first party, the computation of function f will be performed. □

Now we consider a natural generalization of bipartite functional boxes, introduced in Ref. [Wan11], to the multipartite case:

Definition D.2. *For any function $f : \mathbb{Z}_d \times \ldots \times \mathbb{Z}_d \to \mathbb{Z}_d$, the multipartite functional box corresponding to f is defined as*

$$P_n^f(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{d^{n-1}}, \text{ if } a_1 + \ldots + a_n = f(x_1,\ldots,x_n) \\ 0, \text{ otherwise} \end{cases} \tag{D.3}$$

Now we argue that all n-partite functional box with f non-additively separable (f is additively separable if $f(x_1,\ldots,x_n) = f_1(x_1) + f_2(x_2) + \ldots + f_n(x_n)$) would lead to some kind of trivialization of communication complexity.

Theorem D.2. *All P_3^f with $f(x,y,z)$ such that there exists a partial derivative of some order equals to $\lambda \cdot x \cdot y \cdot z + g(x) + h(y) + s(z)$ can be used to simulate a PR_3-d, and then can be used to solve any 3-partite communication complexity problem with only 2 dits of communication.*

Proof. First let us consider

$$f(x,y,z) = \lambda \cdot x \cdot y \cdot z + g(x) + h(y) + s(z). \tag{D.4}$$

So by using box P_3^f Alice, Bob and Charlie can input x, y and z respectively and get outputs a, b and c. Now following Ref. [Wan11] Alice sets $a' = \lambda^{-1}(a - g(x))$, Bob sets $b' = \lambda^{-1}(b - h(y))$ and Charlie sets $c' = \lambda^{-1}(c - s(z))$, so that we have

$$a' + b' + c' = x \cdot y \cdot z\,. \tag{D.5}$$

In order to randomize the results they can randomly chose $k \in \mathbb{Z}_d$ and output $a_f = a' + k$, $b_f = b' + k$ and $c_f = c' - 2k$, so that they perfectly simulate a PR_3-d box.

Now for other functions f we can use the method of Ref. [Wan11] of applying partial derivatives to the function. The partial derivative of f with respect to x is defined as

$$f_x(x,y,z) \equiv f(x+1,y,z) - f(x,y,z) \tag{D.6}$$

and it generates a polynomial with the degree in x reduced by 1, while the degree in y and z remains the same or is smaller. And note that with two boxes P_3^f we can simulate the box $f_x(x,y,z)$.

Then if by partial derivatives we can reduce function f to the form (D.4) we have a protocol using a finite number of boxes P_3^f to simulate PR_3-d. By the result of Theorem D.1, with an arbitrary finite number of P_3^f, we can solve any 3-partite communication complexity problem with only 2 dits of communication. □

If a function $f(x,y,z)$ is not additively separable it will contain at least one term involving product of two variables, for example $x^r y^s$ and this box can be reduced, by derivatives, into a box of the form $\lambda \cdot x \cdot y + g(x) + h(y) + s(z)$. Now using the results for the bipartite case [Wan11], if Charlie always inputs $z = 1$, with only 2 dits of communication they can compute any function of two variables $f(x,y)$.

Appendix E

Proofs of some results

E.1 Some proofs on XOR games

In this Section we prove some of the results stated in Chapters 3 and 5.

Theorem E.1. *Given a bipartite* XOR*-game, with m inputs for Alice, m inputs for Bob, and an associated game matrix* Φ*, the quantum value is upper bounded by*

$$\omega_q^{\oplus} \leq \frac{1}{2}\left(1 + m||\Phi||\right). \tag{E.1}$$

Proof. We now prove this result using Lagrange duality. Let us consider the SDP characterization given by Theorem 3.2.2:

$$\epsilon_q = \begin{cases} \max & \operatorname{Tr}\Phi_s\mathcal{X} \\ \text{s.t.} & \operatorname{diag}(\mathcal{X}) = |\mathbf{1}\rangle, \\ & \mathcal{X} \geq 0. \end{cases} \tag{E.2}$$

By weak duality (Theorem 2.3.1), every feasible solution to the dual Lagrange problem provides an upper bound to the quantum bias ϵ_q. So let us consider the dual problem of (E.2):

$$(\mathcal{D}) \begin{cases} \min & \sum_{i=1}^{2m} y_i \\ \text{s.t.} & \operatorname{Diag}(y) \geq \Phi_s. \end{cases} \tag{E.3}$$

Note that $y_i' = \|\Phi\|$ for all i is a feasible solution to problem $(\mathcal{D})$, since $\|\Phi_s\| = \|\Phi\|/2$ and then

$$\operatorname{Diag}(y') = \frac{\|\Phi\|}{2}\mathbb{1}_{2m} \geq \Phi_s. \tag{E.4}$$

Therefore we have that

$$\epsilon_q = \sum_{i=1}^{2m} y_i' = m\|\Phi\| \tag{E.5}$$

Now

$$\omega_q \leq \frac{1}{2}(1+\epsilon_q) = \frac{1}{2}\left(1+m\|\Phi\|\right), \tag{E.6}$$

which ends the proof. □

For the case where $|Q_A| = m_A$ and $|Q_B| = m_B$, the same analysis results in the upper bound

$$\omega_q \leq \frac{1}{2}\left(1+\frac{m_A+m_B}{2}\|\Phi\|\right), \tag{E.7}$$

which is worse then the bound given by Theorem 3.2.3.

Theorem E.1.1. *The adjacency matrix of an* XOR*-game graph* $\mathcal{G}(\Phi)$

$$\begin{aligned}\mathcal{A}(\mathcal{G}(\Phi)) =& \mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) \otimes \sigma_X + \tfrac{1}{2}|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m \otimes (\mathbb{1}_2 + \sigma_X) \\ & - \tfrac{1}{2}[D(|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m)D] \otimes (\mathbb{1}_2 - \sigma_X)\end{aligned} \tag{E.8}$$

has the following spectrum and corresponding degeneracies:

$$spec(\mathcal{A}(\mathcal{G}(\Phi))) = \begin{cases} 2m-1 & \times 1 \\ m-1 & \times 2m-2 \\ -1 & \times (m-1)^2 \\ 1-m \pm \lambda_z & \times 1 \\ 1 & \times m(m-2) \end{cases}. \tag{E.9}$$

where λ_z *denotes the* m *singular values of* $\tilde{\Phi}$*.*

Proof. We start by nothing that the adjacency matrix, Eq. (E.8), can be written in the form

$$\begin{aligned}\mathcal{A}(\mathcal{G}(\Phi)) =& (\mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) + |\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m) \otimes |+\rangle\langle+| \\ & - (\mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) + [D(|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m)D]) \otimes |-\rangle\langle-|,\end{aligned} \tag{E.10}$$

which allows us to write it as a direct sum

$$\mathcal{A}(\mathcal{G}(\Phi)) = \mathcal{A}_1 \oplus \mathcal{A}_2 \tag{E.11}$$

where

$$\begin{aligned}\mathcal{A}_1 &= (\mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) + |\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m) \\ \mathcal{A}_2 &= (-\mathbb{1}_m \otimes (|\mathbf{1}\rangle\langle\mathbf{1}| - \mathbb{1}_m) - [D(|\mathbf{1}\rangle\langle\mathbf{1}| \otimes \mathbb{1}_m)D]) .\end{aligned} \tag{E.12}$$

Therefore we can proceed to diagonalize $\mathcal{A}_1$ and $\mathcal{A}_2$ separately.

Let us start with the eigenvalues of $\mathcal{A}_1$. Note that $\mathcal{A}_1$ contains only the identity and the all 1's matrix $|\mathbf{1}\rangle\langle\mathbf{1}|$, therefore an eigenbasis for $\mathcal{A}_1$ is formed by the m^2 Fourier vectors $\{|v_i\rangle \otimes |v_j\rangle\}$, where

$$|v_j\rangle = \left(1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(m-1)j}\right) \tag{E.13}$$

with $j \in \{0, \ldots, m-1\}$, where $\zeta = \exp(2\pi I/m)$. Since $|\mathbf{1}\rangle\langle\mathbf{1}|\,|v_i\rangle = m\delta_{i,0}\,|v_i\rangle$ we have that

- $|v_0\rangle \otimes |v_0\rangle$ is an eigenvector of $\mathcal{A}_1$ with eigenvalue $2m-1$,
- $|v_0\rangle \otimes |v_{i\neq 0}\rangle$ and $|v_{i\neq 0}\rangle \otimes |v_0\rangle$ are eigenvectors with eigenvalue $m-1$,
- $|v_{i\neq 0}\rangle \otimes |v_{j\neq 0}\rangle$ are eigenvectors with eigenvalue -1.

which completes the diagonalization of $\mathcal{A}_1$.

Now let us proceed to find the eigenvalues of $\mathcal{A}_2$. First, note that, if $|\lambda_z^A\rangle$ and $|\lambda_z^B\rangle$ are the singular vectors of the game matrix Φ, corresponding to the singular value λ_z, then, by using the relation $\langle\lambda_z^A|\,\Phi\,|\lambda_z^B\rangle = \lambda_z$, we can derive that

$$\langle\lambda_z^A|\,\langle j|\,D\,|j\rangle\,|\lambda_{z'}^B\rangle = \lambda_z\delta_{z,z'}. \tag{E.14}$$

By using relation (E.14) one can verify that the following $2m$ vectors

$$|\eta_z^{\pm}\rangle = \frac{|\lambda_z^A\rangle\,|j\rangle \pm D\,|j\rangle\,|\lambda_z^B\rangle}{\sqrt{2(m \pm \lambda_z)}}, \tag{E.15}$$

are eigenvectors of $\mathcal{A}_2$, with respective eigenvalues $1-(m \pm \lambda_z)$.

The remaining eigenvalues of $\mathcal{A}_2$ are all equal to 1. This can be shown by the fact that subtracting an appropriate amount of the projector into the eigenvectors $\{|\eta_z^{\pm}\rangle\}$ leaves us with identity, *i.e.* the following equality holds

$$\mathcal{A}_2 + \sum_{z=1}^{m}(m+\lambda_z)\,|\eta_z^+\rangle\langle\eta_z^+| + \sum_{z=1}^{m}(m-\lambda_z)\,|\eta_z^-\rangle\langle\eta_z^-| = \mathbb{1}, \tag{E.16}$$

This completes the proof. □

E.2 On DIEWs

Bellow we list the projective measurements $\{M_x^a\} = \{|A_x^a\rangle\langle A_x^a|\}$, $\{M_y^b\} = \left\{\left|B_y^b\right\rangle\left\langle B_y^b\right|\right\}$, $\{M_z^c\} = \{|C_z^c\rangle\langle C_z^c|\}$ that allow the players to win the generalized Mermin game discussed in Section 7.5, Eq. (7.46), with probability 1 when they share the GHZ_3 state:

$$\left|A_0^0\right\rangle = \left|B_0^0\right\rangle = \frac{1}{\sqrt{3}}\left(1, \zeta^{4/3}, 1\right) \ , \ \left|C_0^0\right\rangle = \frac{1}{\sqrt{3}}\left(1, \zeta^{1/3}, 1\right) \ , \tag{E.17a}$$

$$\left|A_0^1\right\rangle = \left|B_0^1\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^2, \zeta^{7/3}, 1\right) \ , \ \left|C_0^1\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^2, \zeta^{4/3}, 1\right) \ , \tag{E.17b}$$

$$\left|A_0^2\right\rangle = \left|B_0^2\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta, \zeta^{1/3}, 1\right) \ , \ \left|C_0^2\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta, \zeta^{7/3}, 1\right) \tag{E.17c}$$

$$\left|A_1^0\right\rangle = \left|B_1^0\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{1/3}, 1, 1\right) \ , \ \left|C_1^0\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{1/3}, \zeta^2, , 1\right) \ , \tag{E.18a}$$

$$\left|A_1^1\right\rangle = \left|B_1^1\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{7/3}, \zeta, 1\right) \ , \ \left|C_1^1\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{7/3}, 1, 1\right) \ , \tag{E.18b}$$

$$\left|A_1^2\right\rangle = \left|B_1^2\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{4/3}, \zeta^2, 1\right) \ , \ \left|C_1^2\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{4/3}, \zeta, 1\right) \tag{E.18c}$$

$$\left|A_2^0\right\rangle = \left|B_2^0\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{8/3}, \zeta^{8/3}, 1\right) \ , \ \left|C_2^0\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{8/3}, \zeta^{5/3}, 1\right) \ , \tag{E.19a}$$

$$\left|A_2^1\right\rangle = \left|B_2^1\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{5/3}, \zeta^{2/3}, 1\right) \ , \ \left|C_2^1\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{5/3}, \zeta^{8/3}, 1\right) \ , \tag{E.19b}$$

$$\left|A_2^2\right\rangle = \left|B_2^2\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{2/3}, \zeta^{5/3}, 1\right) \ , \ \left|C_2^2\right\rangle = \frac{1}{\sqrt{3}}\left(\zeta^{2/3}, \zeta^{2/3}, 1\right) \tag{E.19c}$$

where $\zeta = e^{2\pi i/3}$.

Bibliography

[AB09] S. Arora and B. Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, (2009).

[ABB+10] M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acín, N. Gisin, and S. Pironio. *Guess Your Neighbor's Input: A Multipartite Nonlocal Game with No Quantum Advantage*. Phys. Rev. Lett., 104:230404, (2010). arXiv: 1003.3844.

[ACPA10] R. Augusiak, D. Cavalcanti, G. Prettico, and A. Acín. *Perfect Quantum Privacy Implies Nonlocality*. Phys. Rev. Lett., 104:230401, (2010). arXiv: 0911.3274.

[ACSA10] M. L. Almeida, D. Cavalcanti, V. Scarani, and A. Acín. *Multipartite fully nonlocal quantum states*. Phys. Rev. A, 81:052111, (2010). arXiv: 0911.3559.

[ADR82] A. Aspect, J. Dalibard, and G. Roger. *Experimental Test of Bell's Inequalities Using Time- Varying Analyzers*. Phys. Rev. Lett., 49:1804–1807, (1982).

[ADTA15] R. Augusiak, M. Demianowicz, J. Tura, and A. Acín. *Entanglement and Nonlocality are Inequivalent for Any Number of Parties*. Phys. Rev. Lett., 115:030404, (2015). arXiv: 1407.3114.

[AFLS15] A. Acín, T. Fritz, A. Leverrier, and A. B. Sainz. *A Combinatorial Approach to Nonlocality and Contextuality*. Communications in Mathematical Physics, 334(2):533–628, (2015). arXiv: 1212.4084.

[Ara] M. Araújo. *Understanding Bell's theorem*. More Quantum, Mateus Araújo's Blog. http://mateusaraujo.info/2016/07/15/understanding-bells-theorem-part-1-the-simple-version/.

[ATC14] B. Amaral, M. Terra Cunha, and A. Cabello. *Exclusivity principle forbids sets of correlations larger than the quantum set*. Phys. Rev. A, 89:030101, (2014). arXiv: 1306.6289.

[Bar02] J. Barrett. *Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality*. Phys. Rev. A, 65:042302, (2002). arXiv: quant-ph/0107045.

[BBB+12] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang. *A framework for the study of symmetric full-correlation Bell-like inequalities*. Journal of Physics A: Mathematical and Theoretical, 45(12):125301, (2012). arXiv: 1201.2055.

[BBGL11] J.-D. Bancal, N. Brunner, N. Gisin, and Y.-C. Liang. *Detecting Genuine Multipartite Quantum Nonlocality: A Simple Approach and Generalization to Arbitrary Dimensions*. Phys. Rev. Lett., 106:020405, (2011). arXiv: 1011.0089.

[BBGP13] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio. *Definitions of multipartite nonlocality*. Phys. Rev. A, 88:014102, (2013). arXiv: 1112.2626.

[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*. Phys. Rev. Lett., 96:250401, (2006). arXiv: quant-ph/0508042.

[BCHW15] S. Bauml, M. Christandl, K. Horodecki, and A. Winter. *Limitations on quantum key repeaters*. Nat Commun, 6, (2015). arXiv: 1402.5927.

[BCMdW10] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf. *Nonlocality and communication complexity*. Rev. Mod. Phys., 82:665–698, (2010). arXiv: 0907.3584.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. *Bell nonlocality*. Rev. Mod. Phys., 86:419–478, (2014). arXiv: 1303.2849.

[BDF+99] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. *Quantum nonlocality without entanglement*. Phys. Rev. A, 59:1070–1091, (1999). arXiv: quant-ph/9804053.

[Bel64] J. S. Bell. *On the Eintein Podolsky Rosen paradox*. Physics 1, 195-200, (1964).

[BFF+16] J. Bowles, J. Francfort, M. Fillettaz, F. Hirsch, and N. Brunner. *Genuinely Multipartite Entangled Quantum States with Fully Local Hidden Variable Models and Hidden Multipartite Nonlocality*. Phys. Rev. Lett., 116:130401, (2016). arXiv: 1511.08401.

[BGLP11] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio. *Device-Independent Witnesses of Genuine Multipartite Entanglement*. Phys. Rev. Lett., 106:250404, (2011). arXiv: 1102.0197.

[BM05] H. Buhrman and S. Massar. *Causality and Tsirelson's bounds*. Phys. Rev. A, 72:052103, (2005). arXiv: quant-ph/0409066.

[BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. *Multi-prover Interactive Proofs: How to Remove Intractability Assumptions*. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 113–131, New York, NY, USA, (1988). ACM.

[Bor26] M. Born. *Zur Quantenmechanik der Stossvorgänge*. (English translation: *On the quantum mechanics of collisions, in Quantum theory and measurement, section I.2, J. A. Wheeler and W. H. Zurek, Princeton University Press, 1983*). Zeitschrift für Physik, 37(12):863–867, (1926).

[BP05] J. Barrett and S. Pironio. *Popescu-Rohrlich Correlations as a Unit of Nonlocality*. Phys. Rev. Lett., 95:140401, (2005). arXiv: quant-ph/0506180.

[BPT00] H. Bechmann-Pasquinucci and W. Tittel. *Quantum cryptography using larger alphabets*. Phys. Rev. A, 61:062308, (2000). arXiv: quant-ph/9910095.

[BS15] M. Bavarian and P. W. Shor. *Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH*. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, ITCS '15, pages 123–132, New York, NY, USA, (2015). ACM. arXiv: 1311.5186.

[BTN13] A. Ben-Tal and A. Nemirovski. *Lectures on Modern Convex Optimization*. (2013). Online version: http://www2.isye.gatech.edu/~nemirovs/Lect_ModConvOpt.

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, (2004).

[BV12] N. Brunner and T. Vértesi. *Persistency of entanglement and nonlocality in multipartite quantum systems*. Phys. Rev. A, 86:042113, (2012). arXiv: 1207.3986.

[BZPZ04] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger. *Bell's Inequalities and Quantum Communication Complexity*. Phys. Rev. Lett., 92:127901, (2004). arXiv: quant-ph/0210114.

[CABV13] D. Cavalcanti, A. Acín, N. Brunner, and T. Vértesi. *All quantum states useful for teleportation are nonlocal resources*. Phys. Rev. A, 87:042104, (2013). arXiv: 1207.5485.

[CASA11] D. Cavalcanti, M. L. Almeida, V. Scarani, and A. Acin. *Quantum networks reveal quantum nonlocality*. Nat Commun, 2:184, (2011). arXiv: 1010.0900.

[CDLTP13] A. Cabello, L. E. Danielsen, A. J. López-Tarrida, and J. R. Portillo. *Basic exclusivity graphs in quantum correlations*. Phys. Rev. A, 88:032104, (2013). arXiv: 1211.5825.

[CGP+02] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani. *Bell-Type Inequalities to Detect True n-Body Nonseparability*. Phys. Rev. Lett., 88:170405, (2002). arXiv: quant-ph/0201058.

[CGRS16] D. Cavalcanti, L. Guerini, R. Rabelo, and P. Skrzypczyk. *General Method for Constructing Local Hidden Variable Models for Entangled Quantum States*. Phys. Rev. Lett., 117:190401, (2016). arXiv: 1512.00277.

[CH74] J. F. Clauser and M. A. Horne. *Experimental consequences of objective local theories*. Phys. Rev. D, 10:526–535, (1974).

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. *Proposed Experiment to Test Local Hidden-Variable Theories*. Phys. Rev. Lett., 23:880–884, (1969).

[CHTW04] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. *Consequences and limits of nonlocal strategies*. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249, (2004). arXiv: quant-ph/0404076.

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

[CMSS14] A. Chailloux, L. Mancinska, G. Scarpa, and S. Severini. *Graph-theoretical Bounds on the Entangled Value of Non-local Games*. In *9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2014)*, volume 27 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 67–75, (2014). arXiv: 1404.3640.

[Cob65] A. Cobham. *The intrinsic computational difficulty of functions*. In B.-H. Yehoshua, editor, *Proceedings of the 1964 International Congress*, Studies in logic and the foundations of mathematicss, pages 24–30. North-Holland Publishing Company, (1965).

[Coo71] S. A. Cook. *The Complexity of Theorem-proving Procedures*. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158, New York, NY, USA, (1971). ACM.

[CR12] R. Colbeck and R. Renner. *Free randomness can be amplified*. Nat Phys, 8(6):450–453, (2012). arXiv: 1105.3195.

[CRS12] D. Cavalcanti, R. Rabelo, and V. Scarani. *Nonlocality Tests Enhanced by a Third Observer*. Phys. Rev. Lett., 108:040402, (2012). arXiv: 1110.3656.

[CSUU08] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. *Perfect Parallel Repetition Theorem for Quantum Xor Proof Systems*. computational complexity, 17(2):282–299, (2008). arXiv: quant-ph/0608146.

[CSW10] A. Cabello, S. Severini, and A. Winter. *(Non-)Contextuality of Physical Theories as an Axiom*. (2010). arXiv: 1010.2163.

[CSW14] A. Cabello, S. Severini, and A. Winter. *Graph-Theoretic Approach to Quantum Correlations*. Phys. Rev. Lett., 112:040401, (2014). arXiv: 1401.7081.

[Die10] R. Diestel. *Graph Theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 4th edition, (2010). Electronic Edition: http://diestel-graph-theory.com/index.html.

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

[DLT02] D. P. DiVincenzo, D. Leung, and B. Terhal. *Quantum data hiding*. Information Theory, IEEE Transactions on, 48(3):580–598, (2002). arXiv: quant-ph/0103098.

[DO12] R. C. Drumond and R. I. Oliveira. *Small violations of full-correlation Bell inequalities for multipartite pure random states*. Phys. Rev. A, 86:012117, (2012). arXiv: 1209.1755.

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. *Three qubits can be entangled in two inequivalent ways*. Phys. Rev. A, 62:062314, (2000). arXiv: quant-ph/0005115.

[Ebe93] P. H. Eberhard. *Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment*. Phys. Rev. A, 47:R747–R750, (1993).

[ECG+13] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima. *Quantum key distribution session with 16-dimensional photonic states*. Scientific Reports, 3:2316, (2013). arXiv: 1308.0019.

[Edm87] J. Edmonds. *Paths, Trees, and Flowers*. In I. Gessel and G.-C. Rota, editors, *Classic Papers in Combinatorics*, Modern Birkhäuser Classics, pages 361–379. Birkhäuser Boston, (1987).

[EKB13] M. Epping, H. Kampermann, and D. Bruß. *Designing Bell Inequalities from a Tsirelson Bound*. Phys. Rev. Lett., 111:240404, (2013). arXiv: 1306.3805.

[Eke91] A. K. Ekert. *Quantum cryptography based on Bell's theorem*. Phys. Rev. Lett., 67:661–663, (1991).

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev., 47:777–780, (1935).

[EW02] T. Eggeling and R. F. Werner. *Hiding Classical Data in Multipartite Quantum States*. Phys. Rev. Lett., 89:097905, (2002). arXiv: quant-ph/0203004.

[Fey65] R. P. Feynman. *The character of physical law*. The M.I.T Press, (1965). The lectures can be watched at: www.cornell.edu/video/playlist/richard-feynman-messenger-lectures.

[Fin82] A. Fine. *Hidden Variables, Joint Probability, and the Bell Inequalities*. Phys. Rev. Lett., 48:291–295, (1982).

[FSA+13] T. Fritz, A. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acin. *Local orthogonality as a multipartite principle for quantum correlations*. Nat Commun, 4, (2013). arXiv: 1210.3018.

[GHH10] A. Gabriel, B. C. Hiesmayr, and M. Huber. *Criterion for K-separability in Mixed Multipartite States*. Quantum Info. Comput., 10(9):829–836, (2010). arXiv: 1002.2953.

[GJ90] M. R. Garey and D. S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., New York, NY, USA, (1990).

[GJV+06] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger. *Experimental quantum cryptography with qutrits*. New Journal of Physics, 8(5):75, (2006). arXiv: quant-ph/0511163.

[GVL96] G. H. Golub and C. F. Van Loan. *Matrix Computations (3rd Ed.)*. Johns Hopkins University Press, Baltimore, MD, USA, (1996).

[GVW+15] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. *Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons*. Phys. Rev. Lett., 115:250401, (2015). arXiv: 1511.03190.

[GWAN11] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués. *Quantum Correlations Require Multipartite Information Principles*. Phys. Rev. Lett., 107:210403, (2011). arXiv: 1107.3738.

[Hås01] J. Håstad. *Some Optimal Inapproximability Results*. J. ACM, 48(4):798–859, (2001).

[HBD+15] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*. Nature, 526(7575):682–686, (2015). arXiv: 1508.05949.

[HdV13] M. Huber and J. I. de Vicente. *Structure of Multidimensional Entanglement in Multipartite Systems*. Phys. Rev. Lett., 110:030501, (2013). arXiv: 1210.6876.

[HGBL05] P. Hyllus, O. Gühne, D. Bruß, and M. Lewenstein. *Relations between entanglement witnesses and Bell inequalities*. Phys. Rev. A, 72:012321, (2005). arXiv: quant-ph/0504079.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. *Separability of mixed states: necessary and sufficient conditions*. Physics Letters A, 223(1–2):1 – 8, (1996). arXiv: quant-ph/9605038.

[HHH98] M. Horodecki, P. Horodecki, and R. Horodecki. *Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?* Phys. Rev. Lett., 80:5239–5242, (1998). arXiv: quant-ph/9801069.

[HHH+08] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim. *Quantum Key Distribution Based on Private States: Unconditional Security Over Untrusted Channels With Zero Quantum Capacity*. Information Theory, IEEE Transactions on, 54(6):2604–2620, (2008). arXiv: quant-ph/0608195.

[HHHO05] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. *Secure Key from Bound Entanglement*. Phys. Rev. Lett., 94:160502, (2005). arXiv: quant-ph/0309110.

[HJ12] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, New York, NY, USA, 2nd edition, (2012).

[HLLO06] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim. *Quantum Key Distribution Based on Arbitrarily Weak Distillable Entangled States*. Phys. Rev. Lett., 96:070501, (2006). arXiv: quant-ph/0510067.

[HM15] K. Horodecki and G. Murta. *Bounds on quantum nonlocality via partial transposition*. Phys. Rev. A, 92:010301, (2015). arXiv: 1407.6999.

[Hor08] K. Horodecki. *General paradigm for distilling classical key from quantum states — On quantum entanglement and security*. PhD thesis, University of Warsaw, (2008).

[HP13] M. Huber and M. Pawłowski. *Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement*. Phys. Rev. A, 88:032309, (2013). arXiv: 1301.2455.

[HQBB13] F. Hirsch, M. T. Quintino, J. Bowles, and N. Brunner. *Genuine Hidden Quantum Nonlocality*. Phys. Rev. Lett., 111:160402, (2013). arXiv: 1307.4404.

[HQV+16] F. Hirsch, M. T. Quintino, T. Vértesi, M. F. Pusey, and N. Brunner. *Algorithmic Construction of Local Hidden Variable Models for Entangled Quantum States*. Phys. Rev. Lett., 117:190402, (2016). arXiv: 1512.00262.

[HS14] M. Huber and R. Sengupta. *Witnessing Genuine Multipartite Entanglement with Positive Maps*. Phys. Rev. Lett., 113:100501, (2014). arXiv: 1404.7449.

[JLL+08] S.-W. Ji, J. Lee, J. Lim, K. Nagata, and H.-W. Lee. *Multisetting Bell inequality for qudits*. Phys. Rev. A, 78:052103, (2008). arXiv: 0810.2838.

[JNP+11] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner. *Connes' embedding problem and Tsirelson's problem*. Journal of Mathematical Physics, 52(1), (2011). arXiv: 1008.1142.

[JP11] M. Junge and C. Palazuelos. *Large Violation of Bell Inequalities with Low Entanglement*. Communications in Mathematical Physics, 306(3):695–746, (2011). arXiv: 1007.3043.

[Kar72] R. Karp. *Reducibility among Combinatorial Problems*. In R. Miller, J. Thatcher, and J. Bohlinger, editors, *Complexity of Computer Computations*, The IBM Research Symposia Series, pages 85–103. Springer US, (1972).

[Kav] Kaveh(http://cs.stackexchange.com/users/41/kaveh). *What is the definition of P, NP, NP-complete and NP-hard?* Computer Science Stack Exchange. http://cs.stackexchange.com/q/18666 (version: 2013-12-06).

[KC16] M. Kleinmann and A. Cabello. *Quantum Correlations Are Stronger Than All Nonsignaling Correlations Produced by n-Outcome Measurements*. Phys. Rev. Lett., 117:150401, (2016). arXiv: 1505.04179.

[Ken11] A. Kent. *Unconditionally secure bit commitment with flying qudits*. New Journal of Physics, 13(11):113015, (2011). arXiv: 1101.4620.

[Ken12] A. Kent. *Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes*. Phys. Rev. Lett., 109:130501, (2012). arXiv: 1108.2879.

[KKMO07] S. Khot, G. Kindler, E. Mossel, and R. O'Donnell. *Optimal Inapproximability Results for MAX-CUT and Other 2-Variable CSPs?* SIAM J. Comput., 37(1):319–357, (2007).

[Knu94] D. E. Knuth. *The Sandwich Theorem*. The Electronic Journal of Combinatorics, 1:# A1, (1994). arXiv: math/9312214.

[KRT10] J. Kempe, O. Regev, and B. Toner. *Unique Games with Entangled Provers Are Easy*. SIAM J. Comput., 39(7):3207–3229, (2010). arXiv: 0710.0655.

[KT85] L. Khalfin and B. Tsirelson. *Quantum and quasi-classical analogs of Bell inequalities*. Symposium on the Foundations of Modern Physics 1985, pages 441–460, (1985).

[KTHW13] J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner. *Secure Bit Commitment From Relativistic Constraints*. Information Theory, IEEE Transactions on, 59(7):4687–4699, (2013). arXiv: 1206.1740.

[Lar13] C. E. Larson. *A Class of Graphs Where Alpha=Theta*. The Conjecturing Project, (2013). https://independencenumber.wordpress.com/2013/12/09/a-class-of-graphs-where-alphatheta/.

[LC97] H.-K. Lo and H. F. Chau. *Is Quantum Bit Commitment Really Possible?* Phys. Rev. Lett., 78:3410–3413, (1997). arXiv: quant-ph/9603004.

[Lev73] L. Levin. *Universal search problems (Russian: Universal'nye perebornye zadachi)*. Problems of Information Transmission (Russian: Problemy Peredachi Informatsii), 9(3):265–266, (1973). Translated into English by Trakhtenbrot, B. A. (1984). "A Survey of Russian Approaches to Perebor (Brute-Force Searches) Algorithms". Annals of the History of Computing 6 (4): 384–400.

[LLD09] Y.-C. Liang, C.-W. Lim, and D.-L. Deng. *Reexamination of a multisetting Bell inequality for qudits*. Phys. Rev. A, 80:052116, (2009). arXiv: 0903.4964.

[Lov79] L. Lovasz. *On the Shannon capacity of a graph*. Information Theory, IEEE Transactions on, 25(1):1–7, (1979).

[Lov09] L. Lovász. *Geometric representations of graphs*. (2009). Lecture notes: www.cs.elte.hu/~lovasz/geomrep.pdf.

[LPSW07] N. Linden, S. Popescu, A. J. Short, and A. Winter. *Quantum Nonlocality and Beyond: Limits from Nonlocal Computation*. Phys. Rev. Lett., 99:180502, (2007). arXiv: quant-ph/0610097.

[Mas03] L. Masanes. *Necessary and sufficient condition for quantum-generated correlations*. (2003). arXiv: quant-ph/0309137.

[May97] D. Mayers. *Unconditionally Secure Quantum Bit Commitment is Impossible*. Phys. Rev. Lett., 78:3414–3417, (1997). arXiv: quant-ph/9605044.

[MBL+13] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne. *Device-Independent Entanglement Quantification and Related Applications*. Phys. Rev. Lett., 111:030501, (2013). arXiv: 1302.1336.

[MCC+11] Z.-H. Ma, Z.-H. Chen, J.-L. Chen, C. Spengler, A. Gabriel, and M. Huber. *Measure of genuine multipartite entanglement with computable lower bounds*. Phys. Rev. A, 83:062325, (2011). arXiv: 1101.2001.

[Mer90] N. D. Mermin. *Extreme quantum entanglement in a superposition of macroscopically distinct states*. Phys. Rev. Lett., 65:1838–1840, (1990).

[MPA11] L. Masanes, S. Pironio, and A. Acin. *Secure device-independent quantum key distribution with causally independent measurement devices*. Nat Commun, 2:238, (2011). arXiv: 1009.1567.

[MRMT16] G. Murta, R. Ramanathan, N. Móller, and M. Terra Cunha. *Quantum bounds on multiplayer linear games and device-independent witness of genuine tripartite entanglement*. Phys. Rev. A, 93:022305, (2016). arXiv: 1510.09210.

[Mur12] G. Murta. *Não-Localidade em Sistemas Quânticos*. Master thesis. Programa de Pós-Graduação em Física - UFMG, (2012).

[MVWZ01] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. *Entanglement of the orbital angular momentum states of photons*. Nature, 412:313–316, (2001). arXiv: quant-ph/0104070.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, (2010).

[NCPGV12] M. Navascués, T. Cooney, D. Pérez-García, and N. Villanueva. *A Physical Approach to Tsirelson's Problem*. Foundations of Physics, 42(8):985–995, (2012). arXiv: 1105.3373.

[NPA08] M. Navascués, S. Pironio, and A. Acín. *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations*. New Journal of Physics, 10(7):073013, (2008). arXiv: 0803.4290.

[PAB+09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. *Device-independent quantum key distribution secure against collective attacks*. New Journal of Physics, 11(4):045021, (2009). arXiv: 0903.4460.

[Pal12] C. Palazuelos. *Superactivation of Quantum Nonlocality*. Phys. Rev. Lett., 109:190401, (2012). arXiv: 1205.3118.

[PAM+10] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. *Random numbers certified by Bell's theorem*. Nature, 464(7291):1021–1024, (2010). arXiv: 0911.3427.

[Pen89] R. Penrose. *The Emperor's New Mind: Concerning Computers, Minds, and the Laws of Physics*. Oxford University Press, Inc., New York, NY, USA, (1989).

[Per96a] A. Peres. *Collective tests for quantum nonlocality*. Phys. Rev. A, 54:2685–2689, (1996). arXiv: quant-ph/9603023.

[Per96b] A. Peres. *Separability Criterion for Density Matrices*. Phys. Rev. Lett., 77:1413–1415, (1996). arXiv: quant-ph/9604005.

[Per99] A. Peres. *All the Bell Inequalities*. Foundations of Physics, 29(4):589–614, (1999). arXiv: quant-ph/9807017.

[Pia09] M. Piani. *Relative Entropy of Entanglement and Restricted Measurements*. Phys. Rev. Lett., 103:160504, (2009). arXiv: 0904.2705.

[Pir04] S. Pironio. *Aspects of Quantum Non Locality*. PhD thesis, Université Libre de Bruxelles, (2004).

[Pop95] S. Popescu. *Bell's Inequalities and Density Matrices: Revealing "Hidden" Nonlocality*. Phys. Rev. Lett., 74:2619–2622, (1995). arXiv: quant-ph/9502005.

[PPK+09] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. *Information causality as a physical principle*. Nature, 461(7267):1101–1104, (2009). arXiv: 0905.2292.

[PR94] S. Popescu and D. Rohrlich. *Quantum nonlocality as an axiom*. Foundations of Physics, 24(3):379–385, (1994). arXiv: quant-ph/9508009.

[PV11] K. F. Pál and T. Vértesi. *Multisetting Bell-type inequalities for detecting genuine multipartite entanglement*. Phys. Rev. A, 83:062123, (2011). arXiv: 1102.4320.

[QBHB16] M. T. Quintino, J. Bowles, F. Hirsch, and N. Brunner. *Incompatible quantum measurements admitting a local-hidden-variable model*. Phys. Rev. A, 93:052115, (2016). arXiv: 1510.06722.

[Qui12] M. T. Quintino. *Black Box Correlations: Locality, Noncontextuality, and Convex Polytopes*. Master thesis. Programa de Pós-Graduação em Física - UFMG, (2012).

[Rai01] E. Rains. *A semidefinite program for distillable entanglement*. Information Theory, IEEE Transactions on, 47(7):2921–2933, (2001). arXiv: quant-ph/0008047.

[RAM16] R. Ramanathan, R. Augusiak, and G. Murta. *Generalized XOR games with d outcomes and the task of nonlocal computation*. Phys. Rev. A, 93:022333, (2016). arXiv: 1502.02974.

[RDLT+14] R. Rabelo, C. Duarte, A. J. López-Tarrida, M. Terra Cunha, and A. Cabello. *Multigraph approach to quantum non-locality*. Journal of Physics A: Mathematical and Theoretical, 47(42):424021, (2014). arXiv: 1407.5340.

[RKMH14] R. Ramanathan, A. Kay, G. Murta, and P. Horodecki. *Characterizing the Performance of XOR Games and the Shannon Capacity of Graphs*. Phys. Rev. Lett., 113:240401, (2014). arXiv: 1406.0995.

[RQS+17] R. Ramanathan, M. T. Quintino, A. B. Sainz, G. Murta, and R. Augusiak. *Tightness of correlation inequalities with no quantum violation*. Phys. Rev. A, 95:012139, (2017). arXiv: 1607.05714.

[RTHH16] R. Ramanathan, J. Tuziemski, M. Horodecki, and P. Horodecki. *No Quantum Realization of Extremal No-Signaling Boxes*. Phys. Rev. Lett., 117:050401, (2016). arXiv: 1410.0947.

[Sha48] C. Shannon. *A mathematical theory of communication*. Bell System Technical Journal, The, 27(3):379–423, (1948).

[Sha56] C. Shannon. *The zero error capacity of a noisy channel*. Information Theory, IRE Transactions on, 2(3):8–19, (1956).

[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**. Phys. Rev. Lett., 115:250402, (2015). arXiv: 1511.03189.

[SRH06] B. Synak-Radtke and M. Horodecki. *On asymptotic continuity of functions of quantum states*. Journal of Physics A: Mathematical and General, 39(26):L423, (2006). arXiv: quant-ph/0507126.

[SS02] M. Seevinck and G. Svetlichny. *Bell-Type Inequalities for Partial Separability in N-Particle Systems and Quantum Mechanical Violations*. Phys. Rev. Lett., 89:060401, (2002). arXiv: quant-ph/0201046.

[Sve87] G. Svetlichny. *Distinguishing three-body from two-body nonseparability by a Bell-type inequality*. Phys. Rev. D, 35:3066–3069, (1987).

[TDL01] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. *Hiding Bits in Bell States*. Phys. Rev. Lett., 86:5807–5810, (2001). arXiv: quant-ph/0011042.

[Ter99] A. Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, (1999). Cambridge Books Online.

[Ter00] B. M. Terhal. *Bell inequalities and the separability criterion*. Physics Letters A, 271(5–6):319 – 326, (2000). arXiv: quant-ph/9911057.

[Tsi80] B. Tsirelson. *Quantum generalizations of Bell's inequality*. Letters in Mathematical Physics, 4(2):93–100, (1980).

[Tsi87] B. Tsirelson. *Quantum analogues of the Bell inequalities. The case of two spatially separated domains*. Journal of Soviet Mathematics, 36(4):557–570, (1987).

[Tur37] A. M. Turing. *On Computable Numbers, with an Application to the Entscheidungsproblem*. Proceedings of the London Mathematical Society, s2-42(1):230–265, (1937).

[VB14] T. Vértesi and N. Brunner. *Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement*. Nat Commun, 5, (2014). arXiv: 1405.4502.

[vD13] W. van Dam. *Implausible consequences of superstrong nonlocality*. Natural Computing, 12(1):9–12, (2013). arXiv: quant-ph/0501159.

[vDGG05] W. van Dam, R. Gill, and P. Grunwald. *The statistical strength of nonlocality proofs*. Information Theory, IEEE Transactions on, 51(8):2812–2835, (2005). arXiv: quant-ph/0307125.

[Vid13] T. Vidick. *Three-Player Entangled XOR Games Are NP-Hard to Approximate*. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 766–775, (2013). arXiv: 1302.1242.

[VPRK97] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. *Quantifying Entanglement*. Phys. Rev. Lett., 78:2275–2279, (1997). arXiv: quant-ph/9702027.

[VV14] U. Vazirani and T. Vidick. *Fully Device-Independent Quantum Key Distribution*. Phys. Rev. Lett., 113:140501, (2014). arXiv: 1210.1810.

[Wan11] G. Wang. *Functional boxes, communication complexity and information causality*. (2011). arXiv: 1109.4988.

[Weh06] S. Wehner. *Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities*. Phys. Rev. A, 73:022110, (2006). arXiv: quant-ph/0510076.

[Wer89] R. F. Werner. *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*. Phys. Rev. A, 40:4277–4281, (1989).

[WLAR06] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro. *Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits*. Phys. Rev. Lett., 96:090501, (2006). arXiv: quant-ph/0510088.

[WPGF09] M. M. Wolf, D. Perez-Garcia, and C. Fernandez. *Measurements Incompatible in Quantum Theory Cannot Be Measured Jointly in Any Other No-Signaling Theory*. Phys. Rev. Lett., 103:230402, (2009). arXiv: 0905.2998.

[WW01a] R. F. Werner and M. M. Wolf. *All-multipartite Bell-correlation inequalities for two dichotomic observables per site*. Phys. Rev. A, 64:032112, (2001). arXiv: quant-ph/0102024.

[WW01b] R. F. Werner and M. M. Wolf. *Bell Inequalities and Entanglement*. Quantum Info. Comput., 1(3):1–25, (2001). arXiv: quant-ph/0107093.

[YDY14] N. Yu, R. Duan, and M. Ying. *Distinguishability of Quantum States by Positive Operator-Valued Measures With Positive Partial Transpose*. Information Theory, IEEE Transactions on, 60(4):2069–2079, (2014). arXiv: 1209.4222.

[ZHHH98] M. Żukowski, R. Horodecki, M. Horodecki, and P. Horodecki. *Generalized quantum measurements and local realism*. Phys. Rev. A, 58:1694–1698, (1998). arXiv: quant-ph/9608035.

[Zie95] G. M. Ziegler. *Lectures on Polytopes*, volume 152 of *Graduate Texts in Mathematics*. Springer-Verlag New York, (1995).