ON QUANTUM NONLOCALITY AND THE DEVICE-INDEPENDENT PARADIGM

RAFAEL LUIZ DA SILVA RABELO

NATIONAL UNIVERSITY OF SINGAPORE

2013

ON QUANTUM NONLOCALITY AND THE DEVICE-INDEPENDENT PARADIGM

RAFAEL LUIZ DA SILVA RABELO
(*Master in Physics, Universidade Federal de Minas Gerais, Brazil*)

A THESIS SUBMITTED
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

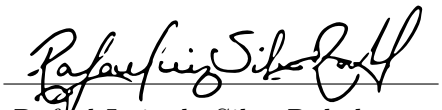
CENTRE FOR QUANTUM TECHNOLOGIES
NATIONAL UNIVERSITY OF SINGAPORE

2013

Declaration

I hereby declare that this thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.



Rafael Luiz da Silva Rabelo
September 25, 2013

To my father, my mother, my brother, and my love.

Acknowledgments

First of all, I would like to thank Valerio Scarani, for giving me the opportunity of working with him at CQT and for being a great supervisor. Along these years, he has given me more advices, ideas and freedom to explore research topics than I could take advantage of, and, for all that, I am truly grateful.

I would not be in CQT, or even working on quantum physics, if it was not for Marcelo Terra Cunha. I cannot thank him enough for opening so many doors, and encouraging me to go through them.

Among all the great people that made my stay in Singapore as good as possible, there are three, in particular, that I would like to specially thank: Daniel Cavancanti, Marcelo França Santos and Pawel Kurzynski. Thank you very much, guys!

I would also like to thank the whole Conneqt group, for the nice group environment and the great discussions we had along these years. Special thanks to my office mates Melvyn, Cai Yu, Thinh and Tzyh Haur. Also, I would like to thank Jean-Daniel Bancal, who has kindly proofread this text. Any errors that may have remained are of my entire responsability.

To all my friends, in Brazil and Singapore, too many to be named, thank you! There is a little bit of each one of you in this thesis. And to all the people who have helped me in any way - you know who you are - , my sincere thanks!

Finally, I would like to thank all my family, in special my father, José Luiz, my mother, Vera Lúcia, and my brother, Rodrigo. Your unconditional

support was crucial for any single bit of this PhD. I cannot thank you enough.

Last, but not least, I would like to specially thank my dear Camila, for keeping our correlations as strong as possible, despite the space-like separation between us.

Abstract

Nonlocality is one of the most fascinating aspects of quantum theory. It is a concept that refers to stronger-than-classical correlations between the components of space-like separated systems, and a clear manifestation of entanglement, although these two concepts are not trivially related. With the recent advent of quantum information theory, nonlocality has gained the status of resource: it can be used to securely evaluate particular tasks without relying on assumptions about the devices that are supposed to implement such protocols - a device-independent assessment.

The thesis is focused on the study of nonlocality theory and its applications to device-independent assessment of quantum phenomena. Special emphasis is given to a protocol for device-independent assessment of measurement devices and to a device-independent formulation of Hardy's test of nonlocality. Also, on more fundamental grounds, recent developments on the relation between entanglement and nonlocality are presented, regarding, specially, the idea of activation of nonlocality on multipartite quantum networks.

List of Publications

This thesis is based on the following publications:

- **R. Rabelo**, M. Ho, D. Cavalcanti, N. Brunner, V. Scarani, "Device-Independent Certification of Entangled Measurements", Physical Review Letters **107**, 050502 (2011).
- D. Cavalcanti, **R. Rabelo**, V. Scarani, "Nonlocality Tests Enhanced by a Third Observer", Physical Review Letters **108**, 040402 (2012).
- **R. Rabelo**, Y. Z. Law, V. Scarani, "Device-Independent Bounds for Hardys Experiment", Physical Review Letters **109**, 180401 (2012).

Contents

List of Figures

1

Introduction

About ninety years have passed since the birth of quantum mechanics, on the beginning of the twentieth century. Throughout this period, quantum theory has developed and become a powerful and successful scientific theory, able to describe with high precision a wide variety of physical phenomena. On the other hand, despite the great experimental and theoretical advances achieved, little is known about the foundations of quantum theory. There is no consensus regarding the interpretation of its formalism, and it is not known if there are physical principles that would, on a fundamental level, lead to the observed quantum phenomena.

Among the many non-intuitive aspects of quantum mechanics, one, in particular, has troubled physicists and philosophers since its early days: its probabilistic character. Quantum mechanics can be understood as a set of rules for the computation of probabilities of the outcomes of measurements performed on prepared systems. On the level of a single run of the experiment, it is, in general, not possible to predict which outcome will be obtained.

The search for hidden variables

The probabilistic nature of quantum mechanics has led many scientists, including some of its founding fathers, to question the completeness of the theory. The most prominent example is, probably, Albert Einstein, who, together with Boris Podolsky and Nathan Rosen, published a seminal paper on 1935 [1], arguing about the completeness of quantum theory, a result that

became known as *EPR paradox*. Defining physical reality, and properties of its elements, they conclude that quantum mechanics, in particular, the wave function, could not describe it properly. A complete theory should be able to predict deterministically the elements of reality, and the key to this theory could be *hidden variables*, properties which, for fundamental or technological reasons, are not yet accessible or observable. It started, thus, a search for hidden variable theories that could reintroduce determinism in this new physics, while reproducing the predictions of quantum mechanics on a statistical level.

The best known example of hidden variable theory is due to David Bohm, who rediscovered the *pilot wave theory* of Louis deBroglie [2]. As desired, this theory is successful in reproducing the predictions of quantum mechanics, adding to that determinism on a single measurement level. However, the hidden variable - the pilot wave - is *nonlocal*, meaning, in this context, that some of its properties, in a specific point of space, may depend on different regions of space, at the same instant of time, implying that some action at distance is necessary.

Another important result regarding hidden variable theories is presented in the seminal paper of Simon Kochen and Ernst Specker [3], published on 1967. The authors show that, due to the structure and properties of quantum measurements, any hidden variable theory that reproduces the predictions of quantum mechanics must present an interesting non-intuitive feature: *contextuality*. Contextuality is the assumption that the outcomes of a measurement performed on a physical system - regarded as properties of the system in question - can depend on other compatible measurements that are performed on the system. The statement that no noncontextual theories can reproduce the predictions of quantum mechanics is known as *Kochen-Specker theorem.*

The nonlocal hidden variable theory of Bohm was not yet satisfactory due to the action at distance necessary, a property that became undesired in any theory after the development of the theory of relativity. On 1964, John Bell revisited the seminal paper of EPR and introduced an elegant formalism that encompassed all *local hidden variable theories* [4], regard-

less of particular properties each one could have. Surprisingly, Bell showed that it was hopeless to consider such class of theories, since none of them could reproduce certain correlations between outcomes of measurements performed on two physical systems as predicted by quantum mechanics. This result became known as *Bell's theorem*, and is one of the most important results within the foundations of quantum mechanics. The property of such strong correlations, non-reproducible by any local theories, is now known as *nonlocality*.

An important highlight of Bell's seminal work is that, by means of an inequality introduced by him, it became possible to test experimentally his results and check if Nature would behave as predicted by quantum mechanics or would allow a classical, local theory as a model. In fact, the one introduced by Bell himself was the first of several *Bell inequalities*, important tools that bound the correlations of any local hidden variable theory. A Bell inequality more suitable for experimental verification of nonlocality was introduced by John Clauser, Michael Horne, Abner Shimony and Richard Holt, and is known as the *CHSH inequality* [5].

Several experiments have been performed to test Bell inequalities, implemented in various different physical systems. Although all of them agree with the quantum predictions to a high degree of precision, they are open to certain *loopholes* that, in principle, allow local theories to simulate nonlocal correlations, and it remains a challenge to perform a loophole-free Bell test.

Quantum nonlocality and entanglement

Behind the nonlocality of quantum correlations is an interesting property of composite quantum systems known as *entanglement*. The name is derived from the german word *verschränkung*, used by Erwin Schrödinger to describe strongly correlated states allowed by the quantum theory [6]. Since then, this concept has been used as a synonym of quantum correlations, with little or no distinction with the idea of nonlocality already present in the papers of EPR [1] and Bell [4], in particular because entanglement is a crucial ingredient in both results.

On 1989, Reinhardt Werner presented, on a seminal paper [7], the formalization of the concept of entanglement. Remarkably, he also showed that there are entangled states that do not display any nonlocality, thus showing that these two concepts, although closely related, are not equivalent. Interestingly, though, some form of equivalence holds for pure states: every entangled pure state violates some Bell inequality, adding more to this interesting relation. This result is due to Nicolas Gisin [8], later extended to multipartite systems by Sandu Popescu and Daniel Rohrlich [9], and is known as *Gisin's theorem*.

Inspired by the weak equivalence introduced by Gisin's theorem, and the conjecture that entangled states should display some form of nonlocality, more complex scenarios were introduced. On 1995, Sandu Popescu considered the possibility of processing the quantum system prior to measurements associated to the CHSH inequality, with the possibility of selecting particular outcomes of the processing procedure, which became known as *local filtering* [10]. By applying this method, Popescu showed that the states considered by Werner, proved to be local, in the sense that they cannot display any nonlocality in standard measurement scenarios, could display their "hidden" nonlocality after the suitable filtering procedure. The approach of Popescu was then extended by Asher Peres, who considered the case where the filtering can be applied not only to a single copy but to several copies of the quantum system, achieving results similar to those of Popescu [11].

Recently, a new approach has been introduced by Daniel Cavalcanti, Mafalda Almeida, Valerio Scarani and Antonio Acín [12]. With the same motivation of exploring the relations between entanglement and nonlocality, they show that, even though there are entangled states that are local on the single copy level, several copies of the same states can be displayed in multipartite network configurations where their nonlocality can be "activated". Some examples of such states and activation schemes are presented in this thesis.

The road to device-independence

On the end of the decade of 1980, and the beginning of the decade of 1990, a new field of research emerged based on the idea that quantum systems could be used to perform computational tasks more efficiently than classical ones: *quantum information and computation theory*.

The beginning of this theory can be traced back to three seminal papers. The first, published on 1984 and authored by Charles Bennett and Gilles Brassard, presents the first *quantum cryptography* protocol, known as *BB84* [13]. The third, in chronological order, was published on 1993, also by Bennett and Brassard, together with co-authors Claude Crápeau, Richard Jozsa, Asher Peres and William Wooters. They showed that entangled states could be used as channels to teleport quantum information, thus presenting the notorious *quantum teleportation protocol* [14]. Finally, the second paper, published on 1991 by Artur Ekert, introduced an entanglement-based quantum cryptography protocol in which security was based on the quantum nonlocality discovered by Bell [15]. From this point on, nonlocality was no more a concept exclusive of the foundations of physics and gained the status of a practical resource for quantum information.

The following decades have seen great development of quantum information theory, both from the theoretical and experimental points of view. However, as quantum technologies became more developed and closer to industrialization and commercialization, it became clear that the advantages provided by quantum devices relied on assumptions that could not always be checked. This led to the development of *device-independent formalism*, an approach that, instead of relying on specific quantum systems, dynamics and measurements - that is, on the inner mechanics of the devices - , provided ways of certifying the proper function of the devices based mostly on observable classical data.

Nowadays, the device-independent formalism has evolved and several information processing protocols have been developed, of which important examples are *quantum key distribution* [16] and *randomness generation* [17]. In fact, some of its basic ideas have grown outside its applied scope, and sim-

ilar methods have been developed to assess fundamental properties quantum systems, such as its dimension [18], or, as presented in this thesis, the entanglement-related properties of measurement devices [19] and bounds for a particular test of nonlocality [20].

Objectives

The main objective of this thesis is to present the original results co-authored by the candidate in a coherent, consistent manner, contextualizing the work within the fields of foundations of quantum mechanics and the new device-independent approach to quantum theory.

Structure of the thesis

The thesis is intended to provide as much background information as possible in order to support the main results. It is structured as follows.

Chapter 2 presents a brief introduction to some of the very basic concepts of quantum theory. Preliminary, it provides some background both in the mathematics and the notation used throughout the thesis.

Chapter 3 presents the main ideas behind the theory of nonlocality. It introduces the device-independent formulation of Bell tests, and the sets of correlations that emerge in such scenarios: the local, quantum and no-signalling correlations. Bell's theorem is proved, and it is shown how entanglement is necessary for nonlocal correlations to be achieved with quantum systems. The Bell inequalities appear naturally in this formalism, and some examples of such important tools are given.

Chapter 4 is devoted to the intricate relations between entanglement and quantum nonlocality. It starts with a brief review of some concepts from the theory of entanglement, such as characterization criteria and entanglement quantifiers. It proceeds by presenting some examples of local entangled states, that is, entangled states that can only lead to local correlations in standard Bell scenarios. Then, two more general scenarios are presented where the "hidden" nonlocality of such states can be revealed or

activated. The first of such scenarios is the one where local filtering operations are allowed prior to the Bell tests. The second is the new multipartite network approach, where examples of schemes of activation of nonlocality are presented.

Chapter 5 presents a brief review of the device-independent paradigm: a collection of protocols and tools that allow for the certification of information processing tasks or of properties of unknown physical system by making as few assumptions as possible about the systems and devices. The protocols cover quantum key distribution, randomness amplification, state and entanglement estimation and dimension witnesses. Two important tools are also presented: the self-testing methodology, and the NPA hierarchy.

Chapter 6 presents an original device-independent protocol for the assessment of measurement devices. Given that some conditions are met, it is possible, by means of the protocol, to certify that a measurement device is entangled, that is, it has eigenvectors that are not separable. By considering a particular case where the systems are assumed to be known, quantitative bounds on how entangled is the device are derived.

Chapter 7 presents a second original device-independent result. The seminal Hardy's test of nonlocality is considered, and new device-independent bounds for this test are derived. It is shown that the simplest systems already lead to maximal nonlocality, and that only a very specific family of states can lead to such result, regardless of the dimension of the system.

Finally, in the Conclusions, the main results are reviewed and further directions of work are presented. They are followed by an appendix, where some of the lemmas stated throughout the thesis are proved.

2

Quantum theory

This preliminary chapter, based on the first chapter of [21], is intended to serve as a brief introduction to the basic concepts of quantum theory referred throughout this thesis. It is not intended to be a complete survey of quantum mechanics; for this purpose, the excellent books of Peres [22], Feynman [23], Cohen-Tannoudji [24], von Neumann [25], and Nielsen and Chuang [26] are suggested.

2.1 Systems and states

What is the scope of quantum theory? Historically, quantum mechanics was developed from the study of atoms and atomic particles, later expanding its domains to subatomic particles, on one hand, and to systems of more than one atom and molecules, on the other. One could then say that the quantum theory is the theory of tiny little things, the physics of the very small scale. This definition could not be considered far from precise for most of the time since the early days of the theory, but, nowadays, it is possible to create and control macroscopic objects that display quantum phenomena[1].

What, then, is a quantum system? Not afraid to be redundant, Asher Peres answers this question [22]:

[1] An example of such object is a *Bose-Einstein condensate* - roughly, a relatively dense cloud of atoms cooled down to *very* low temperatures.

> A quantum system is whatever admits a closed dynamical description within quantum theory.

This definition reflects an interesting fact about quantum theory: almost a century after its foundation, the theory is little more than the description of its mathematical formalism.

The mathematics behind quantum theory is governed by linear algebra. To every quantum system is associated a complex *Hilbert space*, denoted $\mathcal{H}$ - a special case of vector space with a defined inner product. In this thesis only systems associated with Hilbert spaces of finite dimension will be considered; if the dimension d of $\mathcal{H}$ is particularly important in some context, the Hilbert space will be denoted $\mathcal{H}^d$.

An arbitrary vector of $\mathcal{H}$ will be written, using of the convenient Dirac notation, as $|\psi\rangle$, read as *ket* psi. The inner product between two vectors $|\psi\rangle$ and $|\chi\rangle$ will be denoted $\langle\psi \mid \chi\rangle$. By means of the inner product, a linear functional $\langle\chi|$ - read as *bra* chi - is defined for every vector $|\chi\rangle$; the inner product, thus, forms a *bracket*. The norm of a vector is defined as $||\psi\rangle| \equiv \sqrt{\langle\psi \mid \psi\rangle}$.

It is possible, with this notation, to define an *outer product*, $|\psi\rangle\langle\chi|$. This, contrary to the inner product, represents a *linear operator*[2], and not a scalar. Important examples are the *identity operator*, denoted $\mathbf{1}$ and defined by the equation $\mathbf{1}|\psi\rangle \equiv |\psi\rangle$, for all $|\psi\rangle \in \mathcal{H}$, and the *projector*, denoted, in general, Π, which projects a vector into a subspace of the Hilbert space. *Unidimensional projectors* are particularly important; the unidimensional projector into the subspace spanned by $|\psi\rangle$ is written as $\Pi = |\psi\rangle\langle\psi|$.

The mathematical object used to describe a physical system in an instant of time is named *state*. In quantum mechanics, the state is an operator ρ that acts on the Hilbert space associated with the physical system it describes. The *density operator* ρ is defined by means of the following conditions:

[2]A linear operator between spaces $\mathcal{H}^{d_1}$ and $\mathcal{H}^{d_2}$ is a function $A : \mathcal{H}^{d_1} \to \mathcal{H}^{d_2}$. Defined bases for these spaces, an operator can be identified with a matrix $d_2 \times d_1$. Usually $A|\psi\rangle$ is used to denote $A(|\psi\rangle)$.

- ρ is positive semi-definite, $\rho \geq 0$, *i.e.*, for all $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\,\rho\,|\psi\rangle \geq 0$;
- ρ is normalized, $\mathrm{Tr}\,(\rho) = 1$, where $\mathrm{Tr}\,(\cdot)$ denotes the trace of the matrix that represents the operator.

Every density operator can be written as the *convex combination* of unidimensional projectors,

$$\rho = \sum_i q_i \,|\psi_i\rangle\,\langle\psi_i|\,; \quad \sum_i q_i = 1, \quad q_i \geq 0, \tag{2.1}$$

given that $||\psi_i\rangle| = 1$ for all i. This decomposition is, in general, not unique. Counter-examples are states given by single unidimensional projectors, $\rho = |\psi\rangle\,\langle\psi|$. Such states are called *pure states*; by definition, they are the extremal points of the convex set of quantum states of a given system and, with no ambiguity, can be described by the normalized vector $|\psi\rangle$. States that are not pure are called *mixed states*.

The simplest, non-trivial quantum systems are the ones associated with Hilbert spaces of dimension two, $\mathcal{H} = \mathbb{C}^2$. They became notorious, specially in *quantum information theory*, as the quantum analogues of the classical *bits*. This analogy comes from the fact that - for reasons that will become clear further in this chapter - an usual measurement on a qubit has two possible outcomes, and, due to it, these systems are usually called *quantum bits*, or *qubits*. Examples of qubits are spin-1/2 particles (electrons, positrons, and any other fundamental fermions), two-level atoms, *SQUIDS* - superconducting quantum interference devices - , and the polarization degree of freedom of photons.

A general qubit state can be written as

$$\rho = \frac{1}{2}\left(\mathbf{1} + \vec{a}\cdot\vec{\sigma}\right), \tag{2.2}$$

where $|\vec{a}| \leq 1$ and $\vec{\sigma}$ is a vector whose components are the *Pauli matrices*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.3}$$

There is a one-to-one correspondence between the states ρ and the vectors $\vec{a}$. Hence, the state space of a qubit system can be identified with the unit ball embedded in $\mathbb{R}^3$, known, in this context, as the *Bloch ball*. It is easy to note that this correspondence respects convex combinations, and, thus, the pure states are identified as the points of the two-dimensional *Bloch sphere*.

2.2 Composite systems and entanglement

The Hilbert space associated with a quantum composite system is given by the *tensor product* of the spaces associated with the subsystems; a bipartite system, for instance, whose constituent subsystems are associated with the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, is associated with the Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Let $\{|\xi_i\rangle\}$ e $\{|\varphi_j\rangle\}$ be orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Any pure state of $\mathcal{H}_{AB}$ can be written as

$$|\psi\rangle \;=\; \sum_{i=1}^{d_A}\sum_{j=1}^{d_B} c_{ij}\,|\xi_i\rangle \otimes |\varphi_j\rangle\,, \quad \sum_{ij} |c_{ij}|^2 = 1, \tag{2.4}$$

where d_A and d_B are the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$. There is an important theorem, known as *Schmidt decomposition*, that is stated as follows: for all $|\psi\rangle \in \mathcal{H}_{AB}$, there are orthonormal bases $\{|\xi'_i\rangle\}$ of $\mathcal{H}_A$ and $\{|\varphi'_j\rangle\}$ of $\mathcal{H}_B$, and non-negative real numbers c_i such that

$$|\psi\rangle \;=\; \sum_{i=1}^{d_A} c_i\,|\xi'_i\rangle \otimes |\varphi'_i\rangle\,, \quad \sum_{i} c_i^2 = 1. \tag{2.5}$$

The sum has only one index, and is assumed that $d_A \leq d_B$. There are infinite orthonormal bases in which a bipartite pure state can be decomposed in a Schmidt form; the coefficients c_i, however, are unique. It is worth mentioning that there are extensions of the Schmidt decomposition for multipartite systems, but they are not trivial extensions of the form presented above.

Suppose, now, that a bipartite quantum system is in a pure state $|\psi\rangle$ of which two or more of its Schmidt coefficients c_i are non-zero. It is, then, not possible to write the state $|\psi\rangle$ as the tensor product of the states of the subsystems, $|\psi\rangle \neq |\xi\rangle \otimes |\varphi\rangle$. States with this characteristic present an important property called *entanglement*.

The term entanglement - based in the german word *verschränkung*, - was created by Erwin Schrödinger on 1935 [6] to describe those strongly correlated quantum states. A formal definition, though, came much later, and is due to Reinhardt Werner, on 1989 [7].

Consider a bipartite quantum system, whose Hilbert space is $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. A *product state* of this system is a state that can be written in the form $\rho_{AB} = \rho_A \otimes \rho_B$, where ρ_A and ρ_B are the states of subsystems A and B, respectively. A product state can be easily prepared by two devices that work independently and prepare the states ρ_A and ρ_B. Now, suppose that each of the preparing devices is capable of preparing n different states; by choosing a number $r \in \{1, 2, ..., n\}$, the devices prepare subsystems A in the state ρ_A^r and subsystem B in the state ρ_B^r. If a random number generator that generates numbers $r \in \{1, 2, ..., n\}$ with probability $q(r)$ works together with the preparation devices, it is possible to correlate the preparations and obtain states of the form

$$\rho \;=\; \sum_{r=1}^{n} q(r)\rho_A^r \otimes \rho_B^r, \quad q(r) \geq 0, \quad \sum_{r=1}^{n} q(r) = 1. \tag{2.6}$$

Such states are said *separable*. States that cannot be prepared by means of classically correlated local preparations are said *entangled*.

In many situations, one has exclusive interest in only one part of a composite system. The *partial trace* is the operation that represents the discard of subsystems, and is used to obtain the *reduced state* of the remaining system.

Consider a bipartite quantum system in the state ρ, such that, defined bases $\{|\xi_i\rangle\}$ of $\mathcal{H}_A$ and $\{|\varphi_\mu\rangle\}$ of $\mathcal{H}_B$ - latin indices are associated with

subsystem A and greek indices with subsystem B - , can be written as

$$\rho = \sum_{i,\mu,j,\nu} \rho_{i\mu,j\nu} \left|\xi_i\, \varphi_\mu\right\rangle \left\langle \xi_j\, \varphi_\nu\right| . \tag{2.7}$$

where $|\xi\, \varphi\rangle = |\xi\rangle \otimes |\varphi\rangle$. The reduced state ρ_A of subsystem A, in this basis, can be represented by

$$\rho_A = \mathrm{Tr}_B\left(\rho\right) = \sum_{i,j} \sum_{\mu} \rho_{i\mu,j\mu} \left|\xi_i\right\rangle \left\langle \xi_j\right| . \tag{2.8}$$

Analogously, the reduced state ρ_B of subsystem B is

$$\rho_B = \mathrm{Tr}_A\left(\rho\right) = \sum_{\mu,\nu} \sum_{i} \rho_{i\mu,i\nu} \left|\varphi_\mu\right\rangle \left\langle \varphi_\nu\right| . \tag{2.9}$$

In general, the state of the composite system is not the tensor product of the reduced states. This is only true for product states since, with the partial trace, all correlations are ignored.

2.3 Measurements

What sort of information about the system a quantum state carries? The answer to this question is related to one of the most intriguing aspects of quantum theory: its probabilistic nature. In the words of Ashes Peres [22]:

> In a strict sense, quantum theory is a set of rules allowing the computation of probabilities for the outcomes of tests which follow specified preparations.

It is not possible, according to the traditional quantum formalism, to predict deterministically the result of all the measurements that can possibly be performed on the quantum system, even if one has the best possible knowledge about the system[3].

[3] In quantum theory, the best possible description of a system is given by a pure state. This is due to the fact that, for pure states, there is at least one complete measurement for which the result can be deterministically predicted.

A quantum measurement is described by a set of *measurement operators* that act on the Hilbert space of the system. Each operator is associated with a possible result of the measurement, and its mathematical nature varies according to the class of measurements considered. Here, two of the most important classes of quantum measurements will be presented: the *projective measurements* and the *measurements by positive operators*(POVMs)[4].

In a projective measurement x, performed on a quantum system whose Hilbert space is $\mathcal{H}^d$, each result a is associated with a projector $\Pi_{a|x}$, such that different results are associated with projectors onto orthogonal subspaces, *i.e.*, $\mathrm{Tr}\left(\Pi_{a|x}\Pi_{a'|x}\right) = \delta_{a,a'}$, and $\sum_{a=0}^{d'-1}\Pi_{a|x} = \mathbf{1}$. The results are labelled $a \in \{0, ..., d'-1\}$, where $d' \leq d$ is the number of possible results of the measurement. The projective measurement is said *complete* if $d' = d$; in such case, all projectors correspond to unidimensional subspaces of $\mathcal{H}^d$.

Given that measurement x is performed on a system whose state is ρ, the probability that the result a is obtained is given by

$$p(a|x) \;=\; \mathrm{Tr}\left(\rho\,\Pi_{a|x}\right). \tag{2.10}$$

An important property of projective measurements is *repeatability*: in case the same projective measurement is performed more than once, in a consecutive manner, the result which was obtained in the first realization is re-obtained on the following with probability 1, whatever it is. This property is reflected in the formalism by means of the state of the system after the measurement. Suppose that measurement x is performed and result a is obtained. The system is then described by the state

$$\rho' \;=\; \frac{\Pi_{a|x}\,\rho\,\Pi_{a|x}}{\mathrm{Tr}\left(\rho\,\Pi_{a|x}\right)}. \tag{2.11}$$

Another important concept related to projective measurements is that of *observable*. An observable is an hermitian operator that acts on the Hilbert space of the system, associated with a projective measurement. The idea is to link the results of the measurement with real numbers o_a that represent

[4]The acronym POVM stands for positive operator-valued measure.

the values of the measured property. The observable O is associated with the measurement x by means of the spectral decomposition

$$O_x \equiv \sum_{a=0}^{d'-1} o_a \Pi_{a|x}. \tag{2.12}$$

This way, the mean value of the observable is given by

$$\langle O_x \rangle_\rho = \sum_{a=0}^{d'-1} o_a \, p_{a|x} = \mathrm{Tr}\left(\rho \, O\right). \tag{2.13}$$

Suppose that the measurement of the observable O_1 is performed on a quantum system, followed by the measurement of observable O_2. Suppose, also, that a second measurement of O_1 is performed after the measurement of O_2 and it reproduces the outcome of the first. If this holds for every outcome of O_1 and O_2, than these observables are said *compatible*. Compatibility between two observables allows the results of both measurements to be simultaneously determined, since they do not depend on the order these measurements are performed. Two observables are compatible if, and only if, they *commute*, *i.e.*, $[O_1, O_2] \equiv O_1 O_2 - O_2 O_1 = 0$.

POVMs form a class of measurements more general than projective ones. On the other hand, they lack, in general, the property of repeatability and, in most cases, the concept of after-measurement state.

In a POVM x, performed on a system whose Hilbert space is $\mathcal{H}^d$, the possible results a are associated with operators $E_{a|x}$ called *effects*. They must satisfy the following properties:

- $E_{a|x} \geq 0$;
- $\sum_{a=0} E_{a|x} = \mathbf{1}$.

The probability that result a is obtained when POVM x is performed on a system whose state is ρ is given by

$$p_{a|x} = \mathrm{Tr}\left(\rho E_{a|x}\right). \tag{2.14}$$

Contrary to what happens in projective measurements, the number of effects, and, consequently, the number of possible results, is not limited by the dimension of the Hilbert space of the system. In general, POVMs are not repeatable, and it is not possible to determine the state of the system after the measurement. A special case is that in which all the effects are of the form $E_{a|x} = M_{a|x}^{\dagger} M_{a|x}$, for a set of operators $\left\{M_{a|x}\right\}$. Then, if these operators are known, the state after the measurement can be written as

$$\rho' \;=\; \frac{M_{a|x}\,\rho\,M_{a|x}^{\dagger}}{\mathrm{Tr}\left(\rho\,E_{a|x}\right)}. \tag{2.15}$$

In particular, the operators $M_{a|x}$ can be projectors, a case in which the POVM is reduced to a projective measurement. In this sense, the class of POVMs is more general than the class of projective measurements. On the other hand, all the probabilities that can be obtained by means of a POVM performed on a system associated with a Hilbert space $\mathcal{H}^d$ can be reproduced on a projective measurement performed on a system of space $\mathcal{H}^{d'}$, where $d' \geq d$. This is, roughly, the statement of a result known as *theorem of Neumark* [22].

3

Nonlocality

One of the most intriguing aspects of quantum mechanics is its *nonlocality*. Nonlocality, here, refers to stronger-than-classical correlations between the outcomes of measurements performed on space-like separated systems, correlations such that cannot be reproduced by any local realistic theory.

The discovery that quantum correlations may be nonlocal is due to John Bell [4]. Since Bell's theorem, as it became known, the theory of nonlocality has evolved and developed, and the rich mathematical structures derived from Bell's pioneer ideas have been explored, culminating with a new device-independent formalism that relies on Bell inequalities and observable data to assess and certify properties of unknown systems and devices.

This chapter presents some of the basic results related to the theory of nonlocality and the device-independent formalism. Bell scenarios are introduced, and special sets of correlations that arise in such scenarios are presented. Bell inequalities are defined, and the notorious Bell's theorem is stated. To conclude, some of the most important experiments concerning violations of Bell inequalities are reviewed.

The contents of this chapter are partially based on the references [21] and [27]. For a recent review of the theory of nonlocality, please refer to [28].

3.1 Bell scenarios

Consider a pair of particles A and B created at a common source and sent to the laboratories of two experimentalists, Alice and Bob, respec-

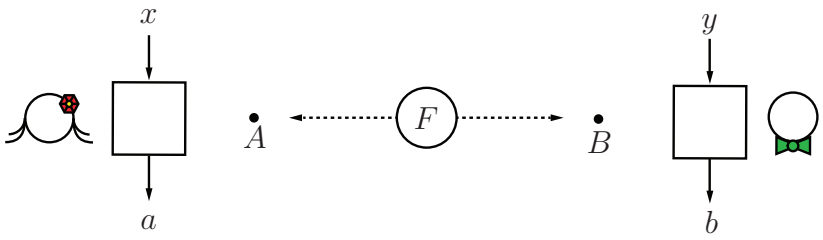


Figure 3.1: A bipartite Bell test. Pairs of particles A and B are produced at a source F, and submitted to measurements x and y, respectively. The outcomes obtained are a and b.

tively. Alice performs, on its particle, a measurement x, of a set $X = \{0, \ldots, m_A - 1\}$ of possible measurements, and obtains an outcome a, of a set $A_x = \{0, \ldots, r_{A_x - 1}\}$ of possible outcomes. Similarly, Bob performs measurement y, of a set $Y = \{0, \ldots, m_B - 1\}$ of possible measurements, and obtains outcome b of $B_y = \{0, \ldots, r_{B_y} - 1\}$. It is assumed that the numbers of possible measurements m_A and m_B and the possible outcomes of each measurement, r_{A_x} and r_{B_y}, are finite. This idealized experiment will be referred as a *Bell test* (fig. 3.1).

If no further details are provided regarding the nature of the particles and the measurements performed, the best description of these experiments is given by the joint, conditional probabilities

$$p\left(a, b|x, y\right) \quad \forall \quad a, b, x, y. \tag{3.1}$$

Locally, though, Alice and Bob can describe their experiments by means of the *marginal probabilities*

$$p_A(a|x, y) = \sum_b p(a, b|x, y), \tag{3.2}$$

$$p_B(b|x, y) = \sum_a p(a, b|x, y). \tag{3.3}$$

Now, define a *measurement event* as the space-time region that comprises the volume in space where the measurement is performed and the interval of time between the choice of measurement and the obtention of

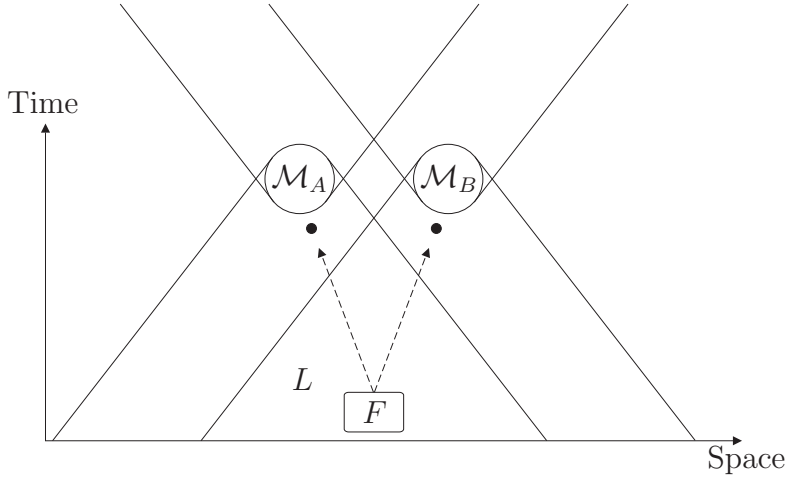


Figure 3.2: Space-like separated measurement events $\mathcal{M}_A$ and $\mathcal{M}_B$.

the outcome. Suppose the measurement events are *space-like separated*, *i.e.*, the laboratories are sufficiently distant from each other and the measurement processes are brief enough so that the measurement events are outside each other's light cone in any inertial reference frame (fig. 3.2). Taking into account the relativistic principle that no signal can travel faster than light, this assumption implies the following *no-signalling conditions*:

$$p_A(a|x) = \sum_b p(a,b|x,y) \,\forall\, a,x,y \tag{3.4}$$

$$p_B(b|y) = \sum_a p(a,b|x,y) \,\forall\, b,x,y. \tag{3.5}$$

In words, the no-signalling conditions state that the marginal probabilities of Alice cannot depend on the choice of the measurement performed by Bob, and, analogously, that the marginal probabilities of Bob cannot depend on the choice of measurement performed by Alice. If these conditions do not hold, the dependence of the marginals on the choice of measurements by the other party could be used for faster-than-light communication.

The numbers m_A, m_B, r_{A_x} and r_{B_y}, together with the assumption that measurement events are space-like separated, define a bipartite *Bell scenario*. Multipartite extensions are straightforwardly defined and must in-

clude the number of parties. More general Bell scenarios can be characterized by means of the notation

$$\left(r_{A_1},\ldots,r_{A_{m_A-1}};r_{B_1},\ldots,r_{B_{m_B-1}};\ldots;r_{N_1},\ldots,r_{N_{m_N-1}}\right), \tag{3.6}$$

where the semicolon separate the parties and the commas separate the measurements, indicated by the number of possible outcomes. In commonly considered scenarios, the number of outcomes will be the same for all the measurements of a given party, and the number of measurements will be the same for all the parties. In this case, a scenario with n parties, m measurements per party and r outcomes per measurement can be characterized by means of the simpler notation (n, m, r).

3.2 Device independence

Although it may be convenient to think of Bell scenarios in terms of measurements performed on physical systems, it can also be viewed, more abstractly, as a collection of black boxes that, each, admits an input, from a set of possible inputs, and returns an output, from a set of possible outputs. The inner mechanics of these boxes are usually not accessible, and the best way to describe their behavior is by means of the joint probabilities of their outputs, conditioned on the inputs. It is usual, in this context, to refer to the whole collection of boxes as a single one, composed of space-like separated "sub-boxes".

This example highlights one of the main properties of Bell scenarios: its formalism is independent of the nature and of the mechanics of the devices. The outputs may be generated by means of measurements performed on physical systems or may follow some predetermined rule given by some unknown theory. This *device-independent* formalism is the key to a new paradigm in quantum information theory, of which some protocols are presented in this thesis. Throughout the text, the "measurement" language and the "black box" language will be used interchangeably, without explicit notice.

The joint probabilities $p(a, b|x, y)$ that describe the Bell experiment can be conveniently represented as components of a vector $\mathbf{p} \in \mathbb{R}^t$,

$$\mathbf{p} \;=\; \begin{pmatrix} \vdots \\ p_{a,b|x,y} \\ \vdots \end{pmatrix}, \tag{3.7}$$

where $t = \sum_{x=0}^{m_A-1} \sum_{y=0}^{m_B-1} r_x r_y$. Clearly, not all points of $\mathbb{R}^t$ are valid probability distributions. They must satisfy *non-negativity conditions*,

$$p(a, b|x, y) \;\geq\; 0, \quad \forall\, a, b, x, y; \tag{3.8}$$

and *normalization conditions*,

$$\sum_a \sum_b p(a, b|x, y) \;=\; 1, \quad \forall\, x, y. \tag{3.9}$$

The set of all points $\mathbf{p}$ that satisfy the above conditions will be denoted $\mathcal{V}$.

3.3 Sets of correlations

In general, the measurement events at the distinct laboratories are not independent, despite the non-signalling conditions. That implies that the joint probabilities are not, necessarily, the product of the marginal probabilities of Alice and Bob, *i.e.*,

$$p\,(a, b|x, y) \neq p_A\,(a|x)\, p_B\,(b|y)\,. \tag{3.10}$$

This equation implies the existence of *correlations* between the two measurement events.

Correlations can usually be established in two ways: the first is by means of a direct causal relation between the events, that is, one event is the direct cause of the other; the second is by means of a common cause that correlates both events. Either way, an idea of *locality* is implicit, which means

that the information that establishes the causal relation must be carried by signal propagating no faster than the speed of light, forbidding, thus, instantaneous influences. This idea is known as *Reichenbach's principle.*

In Bell scenarios, where measurement events are, by definition, space-like separated, not even signals propagating at the speed of light can establish a direct causal relation between the events. Nothing, though, prevents the correlations arising from common local causes. The set of such "classical" correlations is named *set of local correlations*, denoted $\mathcal{L}$.

The local correlations are not, however, the most general correlations that can arise in a Bell scenario. These are given by the all the probability distributions that satisfy the no-signalling conditions. Thus, this set is named *set of no-signalling correlations*, denoted $\mathcal{P}$.

In between those sets is a very special one: the set of correlations that can be obtained in quantum Bell scenarios, where the measurements are performed on quantum systems; this is the *set of quantum correlations*, denoted $\mathcal{Q}$.

3.4 Local correlations

Consider a bipartite Bell scenario, and assume the *locality* condition holds: all the correlations are product of common local causes. Let $\lambda \in \Lambda$ represent the variables in the common causal past of the measurement events. Then, if the value of λ is known, there are, by definition, no other factors that could correlate the events, which, thus, become independent,

$$p(a, b|x, y, \lambda) = p_A(a|x, \lambda)p_B(b|y, \lambda). \tag{3.11}$$

The correlations arise from the fact that λ is, in general, not known[1], and this lack of knowledge is reflected by an average over such variables,

$$p(a,b|x,y) \;=\; \int_\Lambda p_A(a|x,\lambda)p_B(b|y,\lambda)q(\lambda)\mathrm{d}\lambda, \tag{3.12}$$

where $q(\lambda)$ is a measure on the set Λ. Joint probability distributions that can be written in the above form are called *local realistic*, or simply *local*.

The points $\mathbf{p} \in \mathcal{V}$ for which there is a set Λ, a measure $q(\lambda)$ and probabilities $p_A(a|x,\lambda)$ and $p_B(b|y,\lambda)$ such that the (3.12) holds compose the set of local correlations $\mathcal{L}$.

3.4.1 Bell inequalities

It is easy to note that every local correlation satisfies the no-signalling conditions. The reciprocal, though, is not true; there are points in $\mathcal{P}$ that are not in $\mathcal{L}$, thus, $\mathcal{L} \subset \mathcal{P}$.

By definition, the set $\mathcal{L}$ is convex. Its extremal points are the elements of the *set of local deterministic points*, denoted $\mathcal{D}$, and defined as the set of uncorrelated probabilities $\mathbf{p}_d$ such that

$$p_d(a,b|x,y) = p_A(a|x)p_B(b|y), \quad \text{and} \quad p_A(a|x), p_B(b|y) \in \{0,1\}\,. \tag{3.13}$$

The definition of Bell scenarios demands that the number of possible measurements and outcomes be finite, and this implies that $\mathcal{D}$ has a finite number of elements. This means that, for every point $\mathbf{p} \in \mathcal{L}$, there is a set Λ, of variables λ that label the points $\mathbf{p}_d(\lambda) \in \mathcal{D}$, and a probability distribution $q(\lambda)$ such that

$$p(a,b|x,y) \;=\; \sum_{\lambda\in\Lambda} q(\lambda)p_d(a,b|x,y,\lambda). \tag{3.14}$$

[1]Due to the *hidden* character of λ and to the locality assumption, this variable has been known, in this context, as *local hidden variable*. In different contexts, λ can be seem as a random variable shared between Alice and Bob, usually as a resource to perform some task that involves the establishment of correlations. Then, in this context, it has been known as *shared randomness*.

The above property implies that $\mathcal{L}$ is a *polytope*. There is a basic result in convex geometry known as the *theorem of Minkowski* that states that a polytope can be represented in two equivalent forms:

- as the convex hull of a finite set of points,

$$\mathcal{L} = \left\{ \mathbf{p} \in \mathbb{R}^t \,|\, \mathbf{p} = \sum_{\lambda} q(\lambda)\mathbf{p}_d(\lambda),\, q(\lambda) \geq 0,\, \sum_{\lambda} q(\lambda) = 1 \right\}; \quad (3.15)$$

- as the intersection of a finite number of semi-spaces,

$$\mathcal{L} = \left\{ \mathbf{p} \in \mathbb{R}^t \,|\, \mathbf{b}_i.\mathbf{p} \leq c_i,\, \forall\, i \in I \right\}, \quad (3.16)$$

  where $\{(\mathbf{b}_i, c_i)\,, i \in I\}$ denotes a finite set of inequalities.

Each of the sets $\{\mathbf{p} \in \mathbb{R}^t \,|\, \mathbf{b}_i.\mathbf{p} = c_i\}$ defines a hyperplane in $\mathbb{R}^t$, and is a *face* of the polytope. Let d denote the dimension of the polytope, embedded in $\mathbb{R}^t$. The faces of dimension zero are called *vertices*, and the one of highest dimension, that is, those with dimension $(d-1)$, are called *facets*. The inequalities associated to the facets of the polytope are sufficient to fully characterize it. Thus, to satisfy all of them is a necessary and sufficient condition for a correlation to be local. These inequalities are known as *Bell inequalities*[2].

3.4.2 The CHSH inequality

The simplest, nontrivial Bell scenario is denoted as $(2, 2, 2)$; it is composed of two parties, where each party is allowed to perform two measurements, each of which has two distinct results. In this scenario, there is only one

[2]A weaker definition says that a Bell inequality is an inequality that separates the local polytope from any point outside it. The inequalities that touch the polytope are said *tight Bell inequalities*.

nontrivial[3] Bell inequality, the *CHSH inequality* [5]

$$p(a=b|0,0)-p(a\neq b|0,0)+p(a=b|0,1)-p(a\neq b|0,1)+$$
$$p(a=b|1,0)-p(a\neq b|1,0)-p(a=b|1,1)+p(a\neq b|1,1)\leq 2, \quad (3.17)$$

where

$$p(a=b|x,y) = p(0,0|x,y)+p(1,1|x,y), \quad (3.18)$$
$$p(a\neq b|x,y) = p(0,1|x,y)+p(1,0|x,y). \quad (3.19)$$

This inequality, named after John Clauser, Michael Horne, Abner Shimony and Richard Holt, is unique up to local relabeling of measurements and outcomes. If one defines the *correlators*

$$E_{xy}=p(a=b|x,y)-p(a\neq b|x,y), \quad (3.20)$$

the CHSH inequality can be written in the more elegant form

$$E_{00}+E_{01}+E_{10}-E_{11} \leq 2. \quad (3.21)$$

There are, however, many constraints imposed by the normalization and no-signalling conditions that have not been explored. Together, they impose 8 linearly independent constraints, implying that the no-signalling polytope and, also, the local polytope, are 8-dimensional bodies, embedded in $\mathbb{R}^{16}$.

It may be convenient, then, to choose an 8-dimensional representation to describe the probability distributions, one where all the elements are independent probabilities. A possible choice is given by the four joint probabilities of obtaining outcomes $a=b=0$, for all x and y, plus the four marginals of obtaining outcomes $a=0$, for all x, and $b=0$, for all y. With these eight probabilities and the normalization and no-signalling conditions it is possible to reconstruct the whole table of 16 joint probabilities. In

[3]The non-negativity conditions (3.8) and the normalization conditions (3.9) are faces of the local polytope and may be regarded as *trivial Bell inequalities.*

this representation, the CHSH inequality can be rewritten in the following form, without redundancies, known as *CH inequality* [29], named after John Clauser and Michael Horne,

$$p_A(0|0) + p_B(0|0) - p(0,0|0,0) - p(0,0|0,1) - p(0,0|1,0) + p(0,0|1,1) \leq 0. \quad (3.22)$$

3.4.3 Other Bell inequalities

Bell inequalities are, probably, the most significant tools within the device-independent formalism. It is, thus, important to list such inequalities for different Bell scenarios. The task of finding the facets of a polytope, given its vertices - the set of deterministic local points, in the context of the local polytope - , is a problem known as *facet enumeration* or *convex hull problem.*

In exceptionally simple cases, it is possible to obtain all the facets of a polytope by means of computational methods and specialized software, like PORTA [30]. However, the computational resources required grow fast with the number of parties, measurements and results, and this strategy soon becomes impractical. Due to this, few Bell scenarios have been completely solved. Below, some of the known Bell inequalities are presented. It is, however, important to remark that the positivity conditions are all trivial facets of the local polytope. Also, different inequalities can be obtained from existing ones by relabeling the parties, measurements and outcomes. Thus, it is sufficient to present one representative of each class of inequalities.

- $(2, 2, 2)$: The simplest nontrivial Bell scenario. The only inequality is CHSH [31].
- $(2, 2; 2, \ldots, 2)$: The only inequality of this scenario is CHSH, independent of how many measurements are performed by Bob [32, 33].
- $(r_{x=0}, r_{x=1}; r_{y=0}, r_{y=1})$: Different scenarios, with r_x and r_y less than 4 have been investigated, and the only nontrivial inequalities found

were CHSH and CGLMP, introduced bellow [33].

- $(2, 3, 2)$: This scenario presents two nontrivial inequalities: the CHSH inequality, and the one known as I_{3322} [34, 33]:

$$\begin{aligned} P_A(0|0) + p_B(0|0) - p(0,0|0,0) - p(0,0|0,1) - \\ p(0,0|0,2) - p(0,0|1,0) - p(0,0|2,0) - \\ p(0,0|1,1) + p(0,0|1,2) + p(0,0|2,1) \geq -1. \end{aligned} \quad (3.23)$$

- $(3, 2, 2)$: This scenario has been completely solved [32], and it presents are 46 nonequivalent inequalities. Interestingly, all the extremal points of the no-signalling polytope have been listed recently [35], and they can be classified, also, in 46 nonequivalent classes.

- The scenarios $(2, 2, r)$ have not been completely solved, but it is known that the *CGLMP inequalities* [36] are facets of the local polytope. They are,

$$\begin{aligned} \sum_{k}^{\lfloor r/2 \rfloor - 1} \left(1 - \frac{2k}{r-1}\right) [p(a = b + k|0,0) + p(b = a + k + 1|0,1) + \\ + p(a = b + k|1,1) + p(b = a + k|1,0) - \\ p(a = b - k - 1|0,0) - p(b = a - k|0,1) - \\ p(a = b - k - 1|1,1) - p(b = a - k - 1|1,0)] \leq 2, \end{aligned} \quad (3.24)$$

where $\lfloor r/2 \rfloor$ denotes the integer part of $r/2$ and

$$p(a = b + k|x, y) = \sum_{b=0}^{r-1} p(b \oplus k, b|x, y), \quad (3.25)$$

where $\oplus$ denotes addition modulo r.

3.5 No-signalling correlations

The set of no-signalling correlations, $\mathcal{P}$, is defined as the set of points $\mathbf{p} \in \mathcal{V}$ for which the no-signalling conditions hold. It is easy to note that this set is convex, and that the no-signalling conditions, being linear functions of the probabilities, define hyperplanes in $\mathbb{R}^t$; the set $\mathcal{P}$ is defined as the intersection of finitely many half-spaces and is, like the set of local correlations $\mathcal{L}$, a polytope embedded in $\mathbb{R}^t$.

The extremal points of $\mathcal{P}$ can be divided in two classes. The *local* ones are the deterministic local points, $\mathcal{D}$, extremal points of the local polytope $\mathcal{L}$. The *nonlocal* ones are not so easily characterized, and few examples, in the simplest Bell scenarios, are known [35].

Consider, for instance, the $(2, 2, 2)$ scenario. The 16 local extremal points of the no-signalling polytope can be expressed as

$$p(a, b|x, y) = \begin{cases} 1 & : \quad a = \alpha x \oplus \beta \\ & \quad\;\; b = \gamma y \oplus \delta; \\ 0 & : \quad \text{otherwise}, \end{cases} \tag{3.26}$$

where $\alpha, \beta, \gamma, \delta \in \{0, 1\}$, and $\oplus$ denotes addition modulo 2. The 8 nonlocal extremal points can be expressed as [37]

$$p(a, b|x, y) = \begin{cases} 1/2 & : \quad a \oplus b = xy \oplus \alpha x \oplus \beta y \oplus \gamma \\ 0 & : \quad \text{otherwise}. \end{cases} \tag{3.27}$$

Each of these points violate a suitable CHSH inequality up to its algebraic maximum 4, and, thus, do not possess a local decomposition (3.12) and, hence, are nonlocal. All local and nonlocal extremal points can be obtained from any single one by means of local relabeling of measurements and outcomes. The nonlocal extremal point for which $\alpha = \beta = \gamma = 0$ is known as *PR-box*, named after Sandu Popescu and Daniel Rohrlich [38].

3.6 Quantum correlations

A particular Bell scenario is one where the physical systems shared by the parties are quantum systems. In this quantum Bell scenario, the parties perform POVMs on their subsystems, and, in general, the results obtained will be correlated. The correlations observed on a quantum Bell scenario will be called *quantum correlations*.

Consider a bipartite quantum Bell scenario. The set $\mathcal{Q}$ of quantum correlations is defined as the set of points $\mathbf{p} \in \mathcal{V}$ for which there exist:

- a quantum state ρ, acting on an arbitrary Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$;
- for every measurement x of party A, a POVM $\left\{E_{a|x}\right\}$, where each effect is associated with an outcome a;
- for every measurement y of party B, a POVM $\left\{F_{b|y}\right\}$, where each effect is associated with an outcome b;

such that the components of $\mathbf{p}$ are

$$p(a,b|x,y) \;=\; \mathrm{Tr}\left(\rho\left(E_{a|x} \otimes F_{b|y}\right)\right). \tag{3.28}$$

The set of quantum correlations $\mathcal{Q}$ has several interesting properties. First, $\mathcal{Q}$ is strictly contained in the set of no-signalling correlations, $\mathcal{Q} \subset P$. It is easy to note that all quantum correlations respect the no-signalling conditions. The fact that there are points in $\mathcal{P}$ that are not in $\mathcal{Q}$ is not trivial, and becomes clear once the *Tsirelson bound* is introduced. Also, it is a convex set, but, contrary to $\mathcal{L}$, it has infinitely many extremal points, even in the simplest Bell scenarios, and is not a polytope. Another interesting property is that the set of local correlations is contained in the set of quantum correlations. A very important fact is that the $\mathcal{L}$ is *strictly* contained in $\mathcal{Q}$. This result is known as *Bell's theorem*, of which a proof (an example of quantum nonlocal correlation) is given below.

3.6.1 Bell's theorem

Consider the Bell scenario $(2, 2, 2)$. Suppose Alice and Bob share a quantum system in state ρ, acting on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and perform projective measurements associated to *dichotomic observables* - observables whose spectrum is $\{\pm 1\}$ - A_0 and A_1, acting on $\mathcal{H}_A$, corresponding to the measurements of Alice, and B_0 and B_1, acting on $\mathcal{H}_B$, corresponding to the measurements of Bob. Associating the outcomes 0 and 1 with the eigenvalues -1 and 1, respectively, of the observables of both Alice and Bob, one can define the *CHSH operator* $\mathcal{B}$ as

$$\mathcal{B} \;=\; A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)\,, \tag{3.29}$$

such that, given a state ρ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, the CHSH inequality can be conveniently written as

$$S = \langle \mathcal{B} \rangle_\rho \leq 2. \tag{3.30}$$

Now, let Alice and Bob share a two-qubit system in the pure state

$$|\psi\rangle \;=\; \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{3.31}$$

let the observables of Alice be

$$A_0 = \sigma_1, \qquad A_1 = \sigma_3; \tag{3.32}$$

and the observables of Bob be

$$B_0 = -\frac{1}{\sqrt{2}}\,(\sigma_1 + \sigma_3)\,, \qquad B_1 = \frac{1}{\sqrt{2}}\,(\sigma_1 - \sigma_3)\,. \tag{3.33}$$

Then, evaluating the mean value of the CHSH operator one obtains

$$S = \left\langle \psi^- \right| \mathcal{B} \left| \psi^- \right\rangle = 2\sqrt{2}, \tag{3.34}$$

thus violating the CHSH inequality, implying that the correlations associ-

ated to this quantum experiment are not local.

The violation of $2\sqrt{2}$ obtained in the above example, with a two-qubit system, is, in fact, the maximum quantum violation of the CHSH inequality that can be obtained by performing measurements on any quantum system, of any dimensionality. This statement, and this value, in particular, is known as *Tsirelson's bound*, named after Boris Tsirelson [39]. The proof that follows is due to [40].

Lemma 1. *The CHSH value achieved by quantum correlations is bounded by* $S_Q \leq 2\sqrt{2}$.

Proof. Consider the CHSH operator,

$$\mathcal{B} = A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)\,, \tag{3.35}$$

where A_0, A_1, B_0 and B_1 are dichotomic observables, acting on the local Hilbert spaces of the bipartite system. The square of this operator can be written as

$$\mathcal{B}^2 = 4\mathbf{1} + [A_0, A_1]\,[B_0, B_1]\,, \tag{3.36}$$

where $[C, D]$ denotes the commutator of operators C and D. The *maximum norm* of the operator, defined as its largest eigenvalue, is bounded, via the Cauchy-Schwartz inequality, by

$$\left|\mathcal{B}^2\right| \leq 4 + |[A_0, A_1]| \otimes |[B_0, B_1]|\,. \tag{3.37}$$

The maximum quantum violation of the CHSH inequality is given by the largest eigenvalue of the CHSH operator, which, in its turn, is given by the square root of the above expression,

$$|\mathcal{B}| \leq \sqrt{4 + |[A_0, A_1]|\,|[B_0, B_1]|}. \tag{3.38}$$

Since the observables are dichotomic, the norm of the commutator reaches the maximum value of 2 if, and only if, the observables *anti-commute*, that

is, $[C, D] = 2CD$. It follows, then, Tsirelson's bound,

$$S_Q \leq 2\sqrt{2}. \tag{3.39}$$

□

Recall that the PR-box is a no-signalling correlation that violates the CHSH inequality up to its algebraic limit, 4. This fact, associated to the Tsirelson's bound, proves that there are points in $\mathcal{P}$ that are not in $\mathcal{Q}$.

An interesting corollary that follows from the proof above is that non-commutativity of the local observables, in both parties, is a necessary condition for the violation of the CHSH inequality. If any of the doubles commute, the largest eigenvalue of the CHSH operator is upper bounded by 2. Another necessary condition for the violation of the CHSH inequality - in fact, of any Bell inequality - is entanglement. If the quantum state is separable, then any correlation obtained by performing measurements on it will give rise to local correlations.

Consider, for instance, a bipartite separable state ρ, written as

$$\rho = \sum_r q(r)\rho_A^r \otimes \rho_B^r, \tag{3.40}$$

where $q(r) \geq 0$, for all r, $\sum_r q(r) = 1$, and ρ_A^r and ρ_B^r are density operators of subsystems A and B. Let $E_{a|x}$ and $F_{b|y}$ be POVM effects associated to outcomes a, of measurement x, and outcome y, of measurement y, respectively. The joint probabilities of observing such results is given by

$$\begin{aligned}
p(a, b|x, y) &= \mathrm{Tr}\left(\rho\left(E_{a|x} \otimes F_{b|y}\right)\right) && \text{(3.41a)}\\
&= \mathrm{Tr}\left(\sum_r q(r)\rho_A^r \otimes \rho_B^r \left(E_{a|x} \otimes F_{b|y}\right)\right) && \text{(3.41b)}\\
&= \sum_r q(r)\mathrm{Tr}\left(\rho_A^r E_{a|x}\right)\mathrm{Tr}\left(\rho_B^r \Pi_{b|y}\right) && \text{(3.41c)}\\
&= \sum_r q(r)p_A(a|x)p_B(b|y), && \text{(3.41d)}
\end{aligned}$$

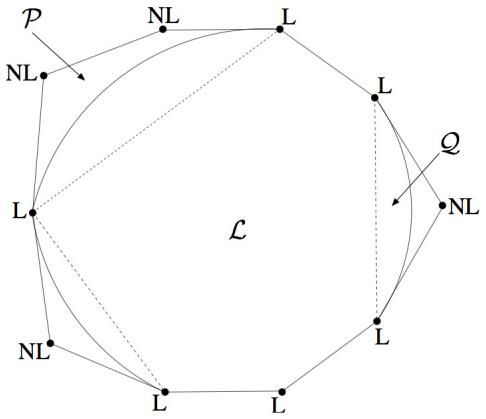


Figure 3.3: Representation of the space of no-signalling correlations. The local extremal points are denoted L, and the nonlocal one are denoted NL. The Bell inequalities are facets denoted by dashed lines.

a local probability distribution. This proof can trivially be extended to multipartite separable states. By inverting the proof above one can easily build separable states and local measurements that will give a quantum realization for any local probability distribution, thus proving that the the set $\mathcal{L}$ is indeed contained in $\mathcal{Q}$ (fig. 3.3).

3.6.2 Experimental tests of nonlocality

Since the seminal work of Bell, many experiments have been implemented to demonstrate quantum nonlocality. On the vast majority of these experiments, the predictions of quantum theory were confirmed with great precision, however, it was not possible, in any of them, to conclude that the observed correlations are, in fact, nonlocal. The reason lies in the so-called *loopholes*, that, in principle, allow for local models to mimic nonlocal correlations.

There are two main loopholes: the *locality loophole* and the *detection loophole*. The locality loophole is related to the assumption that the measurement events are space-like separated. If this assumption is not satisfied, it is possible that the parts exchange information during the measurement, and this is sufficient for nonlocal correlations to be established. There is

also a *free will* condition linked to that, since, from definition, the measurement events start with the choice of measurement. So, the measurements have to be randomly and independently chosen by the parties, otherwise, if the choices are deterministic, in some sense, this information could be available, *a priori*, to the other party, which, in principle, is sufficient to reproduce nonlocal correlations.

The detection loophole is particularly important in experiments that involve photon counting. Optical systems are good sources of entangled states, and for this reason most of the performed experiments are subject to this loophole. It is based on the assumption that the low efficiency of the detectors comes from the fact that the detections are governed by the hidden variables λ. This way, even though the system is classical and there is a local model for the set of probability distributions that govern the experiment, only the convenient detections are kept, and this subset of events may lead to an erroneous estimation of a nonlocal probability distribution.

The critical detection efficiency from which it is possible to close the detection loophole depends on the Bell inequality considered. For the CHSH inequality, assuming that Alice and Bob perform measurements with the same detection efficiency, it is known that the critical value of such is $\eta \geq 2/3$ [41]. An strategy to overcome such loophole in photonic experiments is to consider homodyne measurements, which are measurements on the quadrature variables of the photons that are highly efficient. Recently, several experimental proposals have been made, along these lines, with the goal of closing the detection loophole, even considering hybrid homodyne-photon counting experiments [42, 43, 44, 45, 46]

The first experimental test of nonlocality was performed by Freedman and Clauser, on 1972 [47]. Pairs of photons entangled in polarization were created from cascade electronic transitions in atoms of calcium and sent to detection. With the obtained data and the computed statistics, a violation of the CHSH inequality was observed. However, since the choice of measurements was static and the detectors were inefficient, this experiment was open to both loopholes.

Ten years later, Aspect, Dalibard and Roger performed the first experiment where the choice of measurements varied in time, on a try to close the locality loophole [48]. Opto-acoustical mechanisms simulated random choices of measurements, performed on photons produced on a calcium atoms source similar to the one used by Freedman and Clauser. Although this is considered a seminal experiment, once more reproducing the predictions of quantum mechanics, it is open to both the locality and detection loopholes, the first due to the quasi-deterministic behavior of the opto-acoustical mechanisms.

Since 1988, calcium atoms sources were replaced by nonlinear crystals that, by means of spontaneous parametric down conversion, are able to produce entangled photons more efficiently. The first experiments of non-locality with these sources were performed by Ou and Mandel [49], and, independently, by Alley and Shih [50], both open to the loopholes of locality and detection.

It is accepted that the locality loophole was closed on 1998, in an experiment performed by Weihs and co-authors [51]. In this experiment, the measurements were chosen by mechanisms that implemented random and independent choices. The detection loophole, however, remained a open.

Although a serious problem in photonic experiments, the detection loophole can be easily closed in experiments performed with trapped ions, since the detection efficiency of such systems is close to 100%. The experiment performed by Rowe and co-authors [52], on 2001, closed this loophole. However, since the ions were separated by few micrometers, the locality loophole remained open.

Recently, with great technological development of detectors, reports of photonic experiments claiming to have closed the detection loophole have appeared [53, 54].

4

Entanglement and quantum nonlocality

For many decades, since the early years of quantum mechanics, entanglement and nonlocality, even though not formally defined, have been thought to be similar manifestations of the same quantum phenomenon. However, on 1989, Reinhardt Werner published a seminal paper [7] where he not only formalizes the concept of entanglement but also shows that there are entangled states that cannot display nonlocality. This was the first evidence that these closely related concepts are not equivalent, thus revealing an interesting relation between them.

This chapter is devoted to the study of the relations between entanglement and nonlocality of bipartite quantum states. First, some basic properties of entanglement are presented. Then, the relation between entanglement and nonlocality is explored three different scenarios. The first is the standard Bell scenario, where measurements are performed on single copies of quantum systems. Some examples of entangled states that can only display local correlations on such scenarios are presented. The second scenario is more general than the first, since processing is allowed on multiple copies of the state before the Bell test is performed. In this scenario, it is possible to reveal the "hidden" nonlocality of states that are local in standard Bell scenarios. The third and final scenario allows for multiple copies of the entangled states to be distributed in multipartite quantum networks. In this novel scenario, a state that is local on a single copy level can lead to nonlocal correlations when multiple copies are considered, thus showing activation of nonlocality.

This chapter is partially based on the results of [55].

4.1 Entanglement revisited

Entanglement is a concept that is in the core of quantum theory. The non-classical properties related to this quantum phenomenon have intrigued and surprised physicists and philosophers since the seminal work of Schrödinger [6] and the classic Einstein-Podolski-Rosen paper [1]. Despite its fundamental character, and the deep relation between entanglement and quantum nonlocality, with the recent advent of quantum information theory entanglement became particularly important as a resource for quantum information processing tasks, such as quantum teleportation [14] and quantum key distribution [15]. In this context, it became important to characterize and quantify this resource efficiently. In this section, some basic characterization criteria and quantification notions will be briefly presented. For a complete review of the theory of entanglement, refer to [56].

4.1.1 Characterization

A bipartite entangled state is a state of a composite quantum system, acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, that cannot be written as [7]

$$\rho = \sum_r q(r)\rho_A^r \otimes \rho_B^r, \quad q(r) \geq 0, \quad \sum_r q(r) = 1, \tag{4.1}$$

where ρ_A^r are states that act on $\mathcal{H}_A$ and ρ_B^r are states that act on $\mathcal{H}_B$. This definition, however, is of little help if one needs to determine if a given state is entangled or not.

There are, however, several methods that can be applied to this problem and are computable, for sufficiently simple systems. These are known as *separability criteria*.

Entanglement witnesses

The *entanglement witnesses* [57] constitute an important separability criterion. The key idea behind this criterion follows from a basic property of the set of separable states: it is convex and closed. The *Hahn-Banach theo-*

rem, an important result in convex analysis in finite dimension, guarantees that, given a closed convex set and a point outside the set, there exists a functional that separates the point from the set. Applied to the separability context, this result leads to the following definition of entanglement: a state ρ is entangled if, and only if, there is an operator W, acting on the Hilbert space of the system, such that

$$\mathrm{Tr}\,(\rho W) < 0, \quad \mathrm{Tr}\,(\sigma W) \geq 0, \forall\, \sigma \in \mathcal{S}, \tag{4.2}$$

where $\mathcal{S}$ denotes the set of separable states. The operator W is known as an entanglement witness.

An interesting observation is that Bell inequality operators are examples of entanglement witnesses [58]. Usually, such witnesses are not optimal [59], but have the advantage of being device-independent, holding for Hilbert spaces of any dimension.

The Peres-Horodecki criterion

Now, let ρ be the density operator of a quantum system and $\{|\phi_i\rangle\}$ be an orthonormal basis of the Hilbert space $\mathcal{H}$. In this base, ρ can be written as

$$\rho = \sum_{i,j} \rho_{i,j} \left|\phi_i\right\rangle \left\langle\phi_j\right|. \tag{4.3}$$

The *transpose* of ρ, in this basis, is defined as

$$\rho^T = \sum_{i,j} \rho_{i,j} \left|\phi_j\right\rangle \left\langle\phi_i\right|. \tag{4.4}$$

The transposition of a density operator preserves both of its defining properties: positivity and normalization. The transpose of a density operator is a density operator, and, hence, a valid state of the system.

Now, let ρ be the state of a bipartite quantum system, associated with the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. It is possible to define the transposition operation on a single subsystem; the resulting operators are called *partial*

transposes, and are denoted ρ^{T_A} and ρ^{T_B}, respectively, for the subsystems A and B. Let $\{|\xi_i\rangle\}$ be a basis of $\mathcal{H}_A$ and $\{|\varphi_\mu\rangle\}$ be a basis of $\mathcal{H}_B$ such that the state ρ is written as

$$\rho = \sum_{i,\mu,j,\nu} \rho_{i\mu,j\nu} \left|\xi_i\, \varphi_\mu\right\rangle \left\langle \xi_j\, \varphi_\nu\right| ; \tag{4.5}$$

the latin indices refer to subsystem A and the greek indices to subsystem B. The partially transposed states of the subsystems are given, in the defined bases, by

$$\rho^{T_A} = \sum_{i,\mu,j,\nu} \rho_{i\mu,j\nu} \left|\xi_j\, \varphi_\mu\right\rangle \left\langle \xi_i\, \varphi_\nu\right| , \tag{4.6}$$

$$\rho^{T_B} = \sum_{i,\mu,j,\nu} \rho_{i\mu,j\nu} \left|\xi_i\, \varphi_\nu\right\rangle \left\langle \xi_j\, \varphi_\mu\right| . \tag{4.7}$$

Although the partial transposition preserves the normalization of the state, it may not preserve its positivity. However, it is easy to see that partial transposition preserves the positivity of a whole class of density operators: the separable states. This is the essence of the *Peres criterion* [60]: if the state ρ has a *negative partial transpose* (NPT), *i.e.*, at least one negative eigenvalue, then it is necessarily entangled.

For systems whose dimension of the Hilbert space is less or equal than 6, the Peres criterion is necessary and sufficient to certify entanglement; in such systems, only separable states have positive partial transposes (PPT) [57]. This stronger version of the Peres criterion has been known as the *Peres-Horodecki criterion*. For systems whose dimension of the Hilbert space is greater than 6, there are entangled states whose partial transposes are positive. These are known as PPT entangled states.

k-extensibility criterion

Separable states have other interesting properties that can be explored as separability criteria. A particularly important one is that this class of states admits arbitrary *symmetric extensions*. Let ρ_{AB} be the state of a bipartite

quantum system, associated with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The state ρ_{AB} has a (k_A, k_B) symmetric extension if there is a state $\rho_{A_1,\ldots,A_{k_A};B_1,\ldots,B_{k_B}}$, PPT over every bipartition $A \times B$ - that is, over all bipartitions with i_A subsystems of A and i_B subsystems of B, where i_A ranges from 1 to k_A and i_B from 1 to k_B - , and acting on a Hilbert space $\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_{k_A}} \otimes \mathcal{H}_{B_1} \otimes \cdots \otimes \mathcal{H}_{B_{k_B}}$, such that

$$\rho_{A_i B_j} = \mathrm{Tr}_{\bar{A}_i \bar{B}_j} \left(\rho_{A_1,\ldots,A_{k_A};B_1,\ldots,B_{k_B}} \right) = \rho_{AB}, \, \forall \, i \leq k_A, j \leq k_B, \tag{4.8}$$

where $\bar{A}_i$ denotes the list of all A_k such that $k \neq i$, and $\bar{B}_j$ is similarly defined.

Let ρ_{AB} be a bipartite separable state, written as

$$\rho_{AB} = \sum_r q(r) \rho_A^r \otimes \rho_B^r, \tag{4.9}$$

for density operators $\rho^r{}_A$ of subsystem A and $\rho^r{}_B$ of subsystem B. A (k_A, k_B) symmetric extension of ρ_{AB} is trivially given by

$$\rho_{A_1,\ldots,A_{k_A};B_1,\ldots,B_{k_B}} = \sum_r q(r) \left(\rho_A^r\right)^{\otimes k_A} \otimes \left(\rho_B^r\right)^{\otimes k_B} . \tag{4.10}$$

This construction holds for all k_A and k_B, and can easily be extended to multipartite systems. Having a symmetric extension is, thus, a necessary condition for a state to be separable. It follows that the set of separable states is contained in all the sets of symmetric extendible states, each of which defined for particular values of k_A and k_B. If $\mathcal{S}_{k_A,k_B}$ denotes the set of (k_A, k_B) symmetrically extendible states, it holds that $\mathcal{S}_{k_A,k_B} \supset \mathcal{S}_{k_A+1,k_B+1}$ for all k_A and k_B. Thus, each double k_A, k_B defines a step in a hierarchy of necessary conditions for separability. In the limit where k_B tends to infinity, it has been proven that the set $\mathcal{S}_{1,k_B}$ already converges to the set of separable states [61], and, thus, the condition of having a $(1, k \to \infty)$-symmetric extension becomes necessary and sufficient for separability.

The task of finding a symmetric extension for a given state ρ_{AB} and fixed (k_A, k_B) is, contrary to the general separability problem, efficiently

computable. The reason is it can be formulated as a *semidefinite program*, a class of convex optimization problems for which there are powerful methods and techniques available [62].

4.1.2 Quantification

Entangled states are defined as the states that cannot be prepared by means of local preparations, even with the aid of classical communication that could possibly correlate the states of the parts. In this sense, entanglement can be seen as genuine quantum correlations between the systems, apart from the classical correlations that can be created by means of this mechanism. In general, it is understood that entanglement cannot be created, or increased, by means of *local operations and classical communication* (LOCC). These operations include correlated local unitaries, addition of ancillary systems and discard of subsystems. The entanglement of a state can be quantified via functions known as *entanglement monotones* [63, 64]. An entanglement monotone is a function $E(\rho)$ that does not increase, on average, under LOCC.

A *maximally entangled state* is a bipartite pure state $|\Psi_d\rangle \in \mathcal{H}^d \otimes \mathcal{H}^d$ defined via its Schmidt decomposition,

$$|\Psi_d\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle \,. \tag{4.11}$$

This definition encompasses the fact that entanglement does not change under local unitary operations; thus, every state of the form

$$|\psi\rangle = (U_A \otimes U_B) |\Psi_d\rangle \tag{4.12}$$

is maximally entangled.

The *singlet fraction*, or *singlet fidelity*, of a state, denoted $f(\rho)$, is defined as the maximum projection probability of the state ρ over all maximally

entangled states of the Hilbert space where ρ acts,

$$f(\rho) = \max_{|\psi\rangle \in \{|\Psi_d\rangle\}} \mathrm{Tr}\left(\rho \left|\psi\right\rangle \left\langle\psi\right|\right), \tag{4.13}$$

where $\{|\Psi_d\rangle\}$ is the set of maximally entangled states in $\mathcal{H}^d \otimes \mathcal{H}^d$. This quantity is important in many applications inside the quantum information theory, in particular it bounds the fidelity of teleportation if the state ρ is used as a quantum channel [65].

LOCC cannot increase, on average, the entanglement of a given state, but can be used to dilute the entanglement of a quantum state into several copies of a second state, less entangled. Conversely, this class of operations can be used to concentrate the entanglement of several copies of a given state into copies of second state, more entangled.

Related to the first process is a quantifier known as *cost of entanglement* [66]. If there is a LOCC process Λ_{LOCC} that transforms m copies of a two-qubit maximally entangled state[1] into n copies of a state ρ, the ratio m/n, in the limit where $n \to \infty$, gives an upper bound on the investment necessary, in terms of entanglement, to create the n copies of ρ. The cost of entanglement E_C is defined as the infimum of this quantify over all possible LOCC protocols,

$$E_C(\rho) = \inf_{\Lambda_{LOCC}} \lim_{n\to\infty} \frac{m}{n}. \tag{4.14}$$

The *distillable entanglement* [64, 67], on the other hand, is related to the number of copies m of two-qubit maximally entangled states that can be obtained, by means of LOCC, from n copies of the given quantum state ρ, in the limit where $m \to \infty$. It is defined as

$$E_D(\rho) = \sup_{\Lambda_{LOCC}} \lim_{m\to\infty} \sup \frac{n}{m}. \tag{4.15}$$

In general, these two quantities are not equivalent, and $E_C \geq E_D$. The reason is that there are entangled states that cannot be distilled by means of LOCC, a property known as *bound entanglement*. It is known that this

[1] Maximally entangled states of systems composed of two-qubits are usually regarded as units of entanglement, known as *e-bits*.

is the case of all PPT entangled states [68], but it is still an open question if there are NPT states with this property.

The singlet fidelity, defined above, gives a sufficient criterion for distillability. Every state ρ, acting on $\mathcal{H}^d \otimes \mathcal{H}^d$, for which $f(\rho) > 1/d$ can be distilled [65].

4.2 Standard Bell scenarios

In this section the focus is turned into the relation between entanglement and quantum nonlocal correlations. First, standard Bell scenarios are considered. In such scenarios, measurements are performed on single copies of the states, and no processing of the systems is allowed before the measurements are performed.

It is remarkable that, in standard Bell scenarios, even though every entangled pure state display some nonlocality, this equivalence does not hold for more general, mixed states. The first result is referred to as *Gisin's theorem*. The statement and proof of this important result is presented below, followed by examples of entangled states that can only lead to local correlations. These states are said *local states*. Entangled states that can display nonlocal correlations in standard Bell scenarios are said *nonlocal states*.

4.2.1 Gisin's theorem

Theorem 1. *Every entangled pure state is nonlocal.*

Proof. The proof of the theorem can be divided in two parts: the first, valid for bipartite systems, is due to Nicholas Gisin [8]; the second, the extension to multipartite systems, is due to Sandu Popescu and Daniel Rohrlich [9].

First, consider bipartite systems, and let $|\psi\rangle$ be a pure state in $\mathcal{H}^d \otimes \mathcal{H}^d$. Due to the Schmidt decomposition, there are local orthonormal bases in $\mathcal{H}_A$

and $\mathcal{H}_B$ such that $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{i=0}^{d-1} \lambda_i |ii\rangle , \quad \lambda \geq 0, \quad \sum_i \lambda_i^2 = 1. \tag{4.16}$$

If $|\psi\rangle$ is entangled, then at least two coefficients are nonzero. Assume that $\lambda_0, \lambda_1 \neq 0$. Then, the state $|\psi\rangle$ can be written as

$$|\psi\rangle = \sqrt{\lambda_0^2 + \lambda_1^2}\, |\psi'\rangle + \sqrt{1 - \lambda_0^2 - \lambda_1^2}\, |\psi'_\perp\rangle , \tag{4.17}$$

with

$$|\psi'\rangle = \frac{\lambda_0 |00\rangle + \lambda_1 |11\rangle}{\sqrt{\lambda_0^2 + \lambda_1^2}}, \qquad |\psi'_\perp\rangle = \frac{\sum_{i=2}^{d-1} |ii\rangle}{\sqrt{1 - \lambda_0^2 - \lambda_1^2}}, \tag{4.18}$$

where $|\psi'\rangle$ is a two-qubit state.

Now, let Alice and Bob perform measurements of the form $A_i = A'_i \oplus \mathbf{1}$ and $B'_j = B_j \oplus \mathbf{1}$, for $i, j \in \{0, 1\}$, where $\oplus$ denotes direct sum, A'_i and B'_j are dichotomic observables acting on the subspace spanned by the vectors $\{|0\rangle , |1\rangle\}$, and $\mathbf{1}$ is the identity operator on the subspace spanned by $\{|2\rangle , \ldots , |d-1\rangle\}$. By optimizing over the observables A'_i, B'_j, the state $|\psi'\rangle$ violates the CHSH inequality up to the value $2\sqrt{1 + \sin^2(2\varphi)}$, where $\tan(\phi) = \lambda_0/\lambda_1$ (see appendix for details). Because of the trivial measurements performed on its subspace, the state $|\psi'_\perp\rangle$ does not violate the CHSH inequality, but returns the limiting local value of 2. At the end, the CHSH value of the state $|\psi\rangle$ is given by the convex combination

$$S = q\left(2\sqrt{1 + \sin^2(\varphi)}\right) + 2(1 - q); \tag{4.19}$$

this value is always greater than 2, thus proving that every pure bipartite entangled state $|\psi\rangle$ is nonlocal.

The proof for multipartite systems is slightly more intricate. The results that lead to the desired proof can be summarized in the following two lemmas (proved in the appendix):

Lemma 2 (Popescu-Rohrlich 1 [69]). *For every entangled state $|\psi\rangle$ of an n-partite quantum system, associated with $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$, and for any two parties there exists a projection onto a direct product state of the remaining $(n-2)$-parties such that the resulting bipartite state is entangled.*

Lemma 3 (Popescu-Rohrlich 2 [69]). *Let ρ be a n-partite quantum state. If there are measurements on k parties such that, for a particular collection of outcomes, the resulting $(n-k)$-partite state is nonlocal, then ρ is nonlocal.*

Thus, according to the first lemma, given any pure n-partite entangled state $|\psi\rangle$, it is possible to obtain, by means of local projections on $(n-2)$ parties, a bipartite pure entangled state, say $|\phi\rangle$. By the bipartite version of Gisin's theorem, $|\phi\rangle$ is nonlocal, which, according to the second lemma, is a sufficient condition for $|\psi\rangle$ to be nonlocal. This proves that any pure entangled state is nonlocal. □

4.2.2 Local entangled states

Werner states

Werner states, denoted ρ_W, are states of bipartite systems, associated to Hilbert spaces $\mathcal{H}_A^d \otimes \mathcal{H}_B^d$, that are invariant under all unitary operations of the form $U \otimes U$,

$$\rho_W = (U \otimes U)\, \rho_W \left(U^\dagger \otimes U^\dagger\right). \tag{4.20}$$

They can be written as a convex combination of the (properly normalized) projectors over the *symmetric* and *antisymmetric subspaces* of the Hilbert space, Π_s and Π_a, respectively,

$$\rho_W = p_s \frac{2\Pi_s}{d^2+d} + (1-p_s)\frac{2\Pi_a}{d^2-d}, \tag{4.21}$$

where p_s is the only parameter that defines a state in this family. Werner states are entangled if, and only if, $p_s < 1/2$ [7].

Particularly important are the two-qubit Werner states. They can be written as

$$\rho_w = w \left|\psi^-\right\rangle \left\langle\psi^-\right| + (1-w)\,\frac{\mathbf{1}}{4}, \tag{4.22}$$

where $|\psi^-\rangle$ is the *singlet state*,

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \tag{4.23}$$

The parameter w is related to p_s by

$$w = 1 - \frac{4}{3}p_s, \tag{4.24}$$

which implies $-1/3 \leq w \leq 1$. For $w \geq 0$, the Werner state is a convex combination of the singlet state and the maximally mixed state; throughout the text, the focus will be on this special region. Also, the term Werner states will refer to two-qubit Werner states, unless otherwise stated.

From the original proof of Werner - and from the Peres-Horodecki criterion -, Werner states are entangled if, and only if, $w > 1/3$. Also, these states violate the CHSH inequality if, and only if, $w > 1/\sqrt{2}$ (details in the appendix), which gives an upper bound on the parameter region for which ρ_w is nonlocal[2].

Interestingly, there are Werner states that, despite being entangled, give rise to local correlations in any Bell scenario where projective measurements are performed. The local model of Werner [7] holds for every Werner state for which $p_s \geq (d+1)/2d^2$, and was the first evidence that entanglement and nonlocality are not equivalent concepts. A simple local model for two-qubit Werner states is presented below. Werner's local model, in such systems, holds for every state for which $w \leq 1/2$.

First, note that it suffices to construct a local model for $w = 1/2$, since, due to convexity, the local models for $w \leq 1/2$ can be obtained from

[2]To be precise, this upper bound has been slightly lowered in [70], where it has been shown that there is a Bell inequality, in a scenario where each party performs hundreds of measurements, that is violated for $w \gtrsim 0.705$.

the model for $w = 1/2$ by mixing the probabilities obtained with uniform probabilities. Suppose Alice and Bob perform projective measurements associated with dichotomic observables $A_x = \vec{x}\cdot\vec{\sigma}$ and $B_y = \vec{y}\cdot\vec{\sigma}$, respectively, where $\vec{x}$ and $\vec{y}$ are unit vectors in $\mathbb{R}^3$ and $\vec{\sigma}$ is a vector of Pauli matrices. The probabilities of obtaining outcomes a and b are given by

$$p(a,b|x,y) = \frac{1}{4}\left(1 - w\, a\, b\, \vec{x}\cdot\vec{y}\right), \tag{4.25}$$

where it is assumed that $a, b \in \{\pm 1\}$. Assume that, in each run, Alice and Bob have access to a pre-shared local variable $\vec{\lambda}$, a unit vector drawn uniformly from the unit sphere. The output of Alice's measurement x is randomly returned with probability

$$p_A(a|x,\vec{\lambda}) = \frac{1}{2}\left(1 + a\vec{x}\cdot\vec{\lambda}\right). \tag{4.26}$$

The output of Bob's measurement y, in its turn, is fixed and given by

$$b = -\text{sign}\left(\vec{y}\cdot\vec{\lambda}\right), \tag{4.27}$$

where

$$\text{sign}\,(z) = \begin{cases} -1 & \text{if} \quad z \leq 0 \\ 1 & \text{if} \quad z > 0 \end{cases} \tag{4.28}$$

The joint probability distribution of outcomes a and $b = 1$ is given by

$$p(a,1|x,y) = \int_{S^2} q(\vec{\lambda}) p_A(a|x,\vec{\lambda}) \delta_{\left(\vec{y}\cdot\vec{\lambda}\right)\leq 0} \mathrm{d}\vec{\lambda} \tag{4.29a}$$

$$= \frac{1}{4} + \frac{a}{2}\int_{\left(\vec{y}\cdot\vec{\lambda}\right)\leq 0} q(\vec{\lambda})\vec{x}\cdot\vec{\lambda}\mathrm{d}\vec{\lambda} \tag{4.29b}$$

$$= \frac{1}{4}\left(1 - \frac{a\,\vec{x}\cdot\vec{y}}{2}\right). \tag{4.29c}$$

An analogous calculation gives the joint probability distribution of outcomes

a and $b = -1$:

$$p(a, -1|x, y) \;=\; \frac{1}{4}\left(1 + \frac{a\,\vec{x}\cdot\vec{y}}{2}\right), \tag{4.30}$$

thus reproducing the predictions of quantum mechanics for all possible observables $A_{\vec{x}}$ and $B_{\vec{y}}$.

It is worth mentioning that, on 2002, Jonathan Barrett developed a local model for Werner states that is valid for the more general POVM measurements [71]. Barrett's model holds for $w \leq 5/12$, for Werner states of any local dimension. On the same paper, a second very interesting result is proved, stated here without proof: if a state ρ' can be deterministically obtained from ρ by means of local operations without classical communication, then any local model for the correlations of ρ implies the existence of a local model for the correlations of ρ'.

Isotropic states

Isotropic states, denoted ρ_{iso}, are states of bipartite systems, associated with Hilbert spaces $\mathcal{H}^d \otimes \mathcal{H}^d$, which are invariant under unitaries of the form $U \otimes U^*$. Similarly to Werner states, they constitute a one-parameter family of states that can be written as

$$\rho_{\text{iso}} \;=\; q\,|\Psi_d\rangle\,\langle\Psi_d| + (1-q)\,\frac{\mathbf{1}}{d^2}, \tag{4.31}$$

where $-1/\left(d^2-1\right) \leq q \leq 1$ and $|\Psi_d\rangle$ is the maximally entangled state. As for the case of Werner states, the region where $q \geq 0$ will be specially considered.

Isotropic states are separable if, and only if, $q \leq 1/\left(1+d\right)$ [65]. For $q > 1/\left(1+d\right)$, the isotropic states are not only entangled but also distillable, since the singlet fidelity, in this region, is greater than $1/d$. Regarding their locality properties, the isotropic states are known to be nonlocal, via violation of the CGLMP inequality, for $q \gtrsim 0.69$ for $d = 3$, and $q \gtrsim 0.67$ in the limit $d \to \infty$; the critical values of q decrease as the d increases, so these values are upper and lower bounds for all dimensions [36].

Again, due to their similarity with Werner states, the family of isotropic states is one of the few examples of entangled states for which there are known local models. The local model for isotropic states presented in [72] is similar to the one presented by Werner [7], and holds for all projective measurements. The values of the relative weight q for which the the local model is valid are

$$q \leq \frac{1}{d-1}\left(-1+\sum_{k=1}^{d}\frac{1}{k}\right). \tag{4.32}$$

In the limit when $d \to \infty$, the critical value tends to $\log(d)/d$, which is asymptotically $\log(d)$ larger than the separability critical value, $1/(1+d)$.

States with a symmetric quasiextension

There is a very interesting result stating that any state that has a symmetric extension is local in a wide range of Bell scenarios. It can formally stated as the following theorem [73]:

Theorem 2. *Let ρ_{AB} be a bipartite quantum state that admits a $(1,k)$-symmetric extension. Then, there are local models for the correlations obtained from ρ_{AB} for all Bell scenarios where Bob has, at most, k measurement settings. In any of these scenarios, the number of measurement settings of Alice is arbitrary.*

Proof. The proof makes use of the following result, referred here as Fine's lemma (details in the appendix).

Lemma 4 (Fine [31])**.** *Consider a bipartite Bell scenario where Alice and Bob can perform m_A and m_B measurements, respectively, and let x_i denote the i-th measurement of Alice, $x = i$, and a_i denote its outcome. Similarly, let y_j denote the j-th measurement of Bob, $y = j$, and b_j denote its outcome. Also, let $\vec{a}_m$ denote the string $a_0, \ldots, a_{m-1}$, and similarly for b, x and y. A probability distribution $p(a,b|x,y)$ is local if, and only if, there is a joint probability distribution for the outcomes of all measurements of*

Alice and Bob, $p(\vec{a}_{m_A};\vec{b}_{m_B}|\vec{x}_{m_A};\vec{y}_{m_B})$*, whose marginals are consistent with the distribution* $p(a,b|x,y)$*.*

Let ρ_{AB} have a $(1,k)$-symmetric extension, and consider a scenario where Alice can perform m measurements on her subsystem and Bob can perform k measurements on his subsystem. Define

$$p(a,\vec{b}_k|x,\vec{y}_k) = \mathrm{Tr}\left(\left(\Pi_{a|x}\otimes\Pi_{b_0|y_0}\otimes\cdots\otimes\Pi_{b_{k-1}|y_{k-1}}\right)\rho_{A;B_0,\ldots B_{k-1}}\right). \quad (4.33)$$

It follows that there is a well defined joint probability distribution for the measurements in subsystem B, given by

$$p(\vec{b}_k|\vec{y}_k) = \mathrm{Tr}\left(\left(\Pi_{b_0|y_0}\otimes\cdots\otimes\Pi_{b_{k-1}|y_{k-1}}\right)\rho_{B_0,\ldots B_{k-1}}\right), \quad (4.34)$$

where $\rho_{B_0,\ldots B_{k-1}} = \mathrm{Tr}_A\left(\rho_{A;B_0,\ldots B_{k-1}}\right)$. It is possible, then, to define a joint probability distribution for all the measurements of the experiment,

$$p(\vec{a}_m;\vec{b}_k|\vec{x}_m;\vec{y}_k) = \frac{p(a_1;\vec{b}_k|x_1;\vec{y}_k)\ldots p(a_m;\vec{b}_k|x_m,\vec{y}_k)}{\left[p(\vec{b}_k|\vec{y}_k)\right]^m - 1}. \quad (4.35)$$

The above distribution returns the correct marginals for the bipartite probabilities, and, from Fine's lemma, ρ_{AB} is local for any scenario where Bob performs at most k measurements. □

One example of a k-symmetrically extendible state is the *erased state*,

$$\rho_{\mathrm{era}} = \frac{1}{k}|\Psi_2\rangle\langle\Psi_2| + \left(1-\frac{1}{k}\right)\frac{\mathbf{1}}{2}\otimes|2\rangle\langle 2|, \quad (4.36)$$

where $|\Psi_2\rangle$ is the two-qubit maximally entangled state, and $|2\rangle$ is a state orthogonal to $|\Psi\rangle$. This can be viewed as a state of a qubit-qutrit[3], system, the result from sending one part of a maximally entangled state through an *erasure channel*, that, with probability $1/k$, leaves the state untouched but, with the complementary probability, 'erases' the information of the

[3]A *qutrit* is a quantum system associated to the Hilbert space $\mathcal{H}^3 = \mathbb{C}^3$.

respective subsystem, creating the 'flag' state $|2\rangle$ to indicate erasure has taken place [74].

4.3 Sequential measurements scenarios

In this section, a scenario more general than the standard Bell scenario is introduced. In this new scenario, measurements on multiple copies of the state are allowed, and the system may undergo local processing prior to the measurement. This pre-processing can be composed of LOCC followed by a preliminary measurement, of which the performance of the following Bell test can conditioned on the results obtained. In this sense, these operations are usually referred as *local filtering*.

The advantage of considering these sequential measurement scenarios is that states that are local in standard Bell scenarios may display some nonlocality after undergoing local filtering, thus revealing the "hidden" nonlocality in the state.

4.3.1 Hidden nonlocality of Werner states

The first protocol to reveal hidden nonlocality of a state is due to Popescu [10], and holds for Werner states of local dimension $d \geq 5$. First, note that the Werner state with $p_s = (d+1)/2^d 2$, for which the local model of Werner applies, can be written as

$$\rho_W = \frac{1}{d^2}\left(2\sum_{i,j=0|i<j}^{d-1} \left|\psi_{ij}^-\right\rangle\left\langle\psi_{ij}^-\right| + \frac{\mathbf{1}}{d}\right), \tag{4.37}$$

where $\left|\psi_{ij}^-\right\rangle = \left(|ij\rangle - |ji\rangle\right)/\sqrt{2}$. The protocol works as follows. In the first step, Alice and Bob perform projective measurements $\Pi_{a|0}$ and $\Pi_{b|0}$, respectively, where

$$\Pi_{0|0} = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad \Pi_{1|0} = \mathbf{1} - \Pi_{0|0}. \tag{4.38}$$

If they obtain outcomes $a = 0$ and $b = 0$, the post-measurement state is given by

$$\rho' = \frac{2d}{2d+4}\left(\left|\psi_{01}^{-}\right\rangle\left\langle\psi_{01}^{-}\right| + \frac{\mathbf{1}}{2d}\right). \tag{4.39}$$

The parties, then, proceed to perform suitable measurements on this state and evaluate the CHSH inequality. The optimal value is

$$S = \frac{2d}{2d+4}2\sqrt{2}, \tag{4.40}$$

which is greater than 2 - thus, violating the CHSH inequality - for $d \geq 5$.

The filtering, that is, the first measurement performed by the parties, divides the collected data into four distinct sub-ensemble, denoted (a, b). According to the protocol, nonlocal correlations are observed in the sub-ensemble $(0, 0)$, but it could be the case, however, that the probability distributions of the remaining sub-ensemble are local, in a way that the probability distribution of the whole ensemble is also local. The assumption made by Popescu is that this cannot be the case; if the probability distribution of the whole experiment is local, then the probabilities of all its sub-ensemble, defined by the local filtering, are necessarily local. This is indeed the case, as has been proven in [75].

A second protocol that reveals nonlocality of Werner states is due to Peres [11]. Instead of considering local filtering in single copies of Werner states, many copies of two-qubit Werner states were considered, and it was shown that, by applying suitable filtering operations, it is possible to observe a violation of the CHSH inequality already for 5 copies of the local $w = 1/2$ Werner states.

4.3.2 Assisted revelation of nonlocality

The most general preprocessing procedure consists of stochastic local operations and classical communication (SLOCC), that is, LOCC protocols that fail with some probability. In the first of a series of very interesting

papers, Lluis Masanes showed that, in what regards nonlocality and hidden nonlocality, stochastic local operations without communication (SLO) and deterministic LOCC are fully general, assuming that the processing is performed before the measurement events take place, that is, before the parties choose which measurements to perform. The main result of the first work [76], however, is the following theorem, that links distillability with hidden nonlocality in the $(2, 2, 2)$ Bell scenario:

Theorem 3. *A bipartite state ρ is distillable if, and only if, there exists a positive integer m and a SLO map Λ such that $\Lambda(\rho^{\otimes m})$ violates the CHSH inequality.*

The papers that followed [77, 78], presented, first, the bipartite, and, then, the multipartite results that show that, in some sense, all entangled states present some hidden nonlocality. This hidden nonlocality, however, require some assistance to be revealed. Define $\mathcal{C}_{12}^{CHSH}$ as the set of n-partite states that do not violate the CHSH inequality between parties 1 and 2 even after n-partite stochastic local operations without communication. The main result can be summarized in the following theorem:

Theorem 4. *A state ρ is entangled if, and only if, there exists a state $\sigma \in \mathcal{C}_{12}^{CHSH}$ such that $\rho \otimes \sigma$ is not in $\mathcal{C}_{12}^{CHSH}$.*

4.4 Multipartite network scenarios

This section presents a novel approach for the study of the nonlocal properties of entangled states. Contrary to the previously presented scenarios, here the measurements can be performed on several copies of the states distributed in multipartite settings. Once again, the main advantage is that entangled states that can only lead to local correlations in standard Bell scenarios can display nonlocality in these network scenarios.

4.4.1 Nonlocal resources

A state ρ is defined as a *nonlocal resource* if there exists a positive number m and a Bell scenario where $\rho^{\otimes m}$ is nonlocal. If, in a given scenario, a local state ρ is proven to be a nonlocal resource, it said that the nonlocality of the state has been activated.

The main tool used to reveal nonlocal resources is a previously stated lemma, by Popescu. It states that, given a n-partite state ρ, if there are measurements on k parties such that, for a particular collection of outcomes, the resulting $(n-k)$-partite state is nonlocal, then ρ is nonlocal. If this condition holds, then ρ is a nonlocal resource.

In the following section, some examples of nonlocal resources are presented. They are collected from the papers [12, 79], and [55], co-authored by the author of this thesis.

4.4.2 Revealing nonlocal resources

One-way distillable states

As observed by Daniel Cavalcanti and co-authors [12], every one-way distillable state is a nonlocal resource. One-way distillable states are bipartite entangled states whose entanglement can be distilled by protocols where one-way classical communication is sufficient. Such protocols can be formulated as follows: Alice performs a joint measurement on her subsystems and communicates the obtained outcome to Bob, who, thus, performs suitable operations on his subsystems and, then, performs a joint measurement. In the limit of infinitely many copies, the parties end up sharing a maximally entangled state. In general, there is one outcome of Alice's measurement for which Bob does not have to apply any correcting operation on his subsystems, and this is a crucial property of this class of protocols for the approach here presented.

Let ρ be a one-way distillable state. To show that it is a nonlocal resource, consider a tripartite scenario, where Charlie, in the center, shares m copies of ρ with Alice, $\rho_{AC}^{\otimes m}$, and m other copies with Bob, $\rho_{BC}^{\otimes m}$. Since

ρ is one-way distillable, there are outcomes of measurements performed by Charlie on his two collections of subsystems such that he ends up sharing states arbitrarily close to maximally entangled states with both Alice and Bob. Charlie, then, projects his subsystems onto a maximally entangled state, an operation which, if successful, results on Alice and Bob sharing a maximally entangled state. Note that the whole procedure applied by Charlie can be seen as a single measurement, for which there exists an outcome such that the remaining state of Alice and Bob is maximally entangled, thus, nonlocal. It follows from the lemma that ρ is a nonlocal resource.

There is a condition known as *hashing inequality* that is sufficient to certify one-way distillable entanglement [80]. The inequality reads:

$$\max\left[S\left(\rho_A\right), S\left(\rho_B\right)\right] > S\left(\rho_{AB}\right), \tag{4.41}$$

where $S\left(\rho\right) = -\mathrm{Tr}\left(\rho \log\left(\rho\right)\right)$ is the von Neumann entropy of ρ. In words, if the von Neumann entropy of any of the reduced states of ρ is greater than the entropy of ρ itself, than ρ is one-way distillable.

Isotropic states

The isotropic states configure one of the most interesting cases of activation of nonlocality. In what follows, two schemes that show the nonlocal resource character of isotropic states are presented: the first, weaker, was introduced in [55]; the second, more general, was presented in [79], and proves that every entangled isotropic state is a nonlocal resource, thus showing activation of nonlocality for such states.

The first scheme relies on the fact that there exist Bell inequalities and bipartite states $|\Phi\rangle$ in $\mathcal{H}^d \otimes \mathcal{H}^d$ that give rise to probability distributions $\mathbf{p}_{|\Phi\rangle}$ that achieve *unbounded violations* of such inequalities, with respect to d [81, 82]. The maximum violation of a probability distribution $\mathbf{p}$, in this context, is quantified by the following quantity,

$$\nu\left(\mathbf{p}\right) = \sup_{\mathcal{B}} \frac{\left|S_{\mathcal{B}}\left(\mathbf{p}\right)\right|}{\sup_{\mathbf{p}_L \in \mathcal{L}} \left|S_{\mathcal{B}}\left(\mathbf{p}_L\right)\right|}, \tag{4.42}$$

where $S_{\mathcal{B}}(p)$ denotes the value of Bell inequality $\mathcal{B}$ achieved by the probability distribution $\mathbf{p}$, $\mathcal{L}$ denotes the set of local correlations and the suprema are taken over all Bell inequalities of the given Bell scenario.

The unbounded character of the violation implies that probability distributions of the form

$$\mathbf{p} = q\mathbf{p}_{|\Phi\rangle} + (1-q)\,\mathbf{p}_L \tag{4.43}$$

are nonlocal for $q > q_c$, where q_c is a critical weight that tends to zero, with increasing d, at the same asymptotic rate as $\nu\left(\mathbf{p}_{|\Phi\rangle}\right)$ tends to infinity.

Consider a tripartite scenario, where Charlie, in the center, shares a copy of an isotropic state with Alice and a copy of a second isotropic state with Bob. He then performs a generalized measurement on his subsystems that consists of preparing state $|\Phi\rangle$ and teleporting its components to Alice and Bob, using the isotropic states as channels. According to the teleportation protocol, there is one outcome of Charlie's measurement for which the resulting state of Alice and Bob will be

$$\rho = q^2\,|\Phi\rangle\langle\Phi| + q\,(1-q)\,\sigma_A \otimes \frac{\mathbf{1}}{d} + q\,(1-q)\,\frac{\mathbf{1}}{d} \otimes \sigma_B + (1-q)^2\,\frac{\mathbf{1}\otimes\mathbf{1}}{d^2}, \tag{4.44}$$

where σ_A and σ_B are the reduced states of $|\Phi\rangle$. Then, by performing appropriate measurements, related to the inequality $\mathcal{B}$ that is unboundedly violated, Alice and Bob obtain a joint probability distribution of the form

$$\mathbf{p} = q^2\mathbf{p}_{|\Phi\rangle} + \left(1-q^2\right)\mathbf{p}_L. \tag{4.45}$$

This probability distribution is nonlocal for $q^2 > q_c$; the critical value q_c, in the limit $d \to \infty$, scales as [82]

$$q_c = O\left(\frac{\log(d)}{\sqrt{d}}\right). \tag{4.46}$$

Thus, isotropic states are nonlocal resources for

$$q > O\left(\frac{\sqrt{\log(d)}}{d^{1/4}}\right), \tag{4.47}$$

tending to zero as d tends to infinity. In fact, the above bound holds not only for isotropic states but for all states of the form

$$\rho = q\,|\Psi_d\rangle\langle\Psi_d| + (1-q)\,\sigma_L, \tag{4.48}$$

where σ_L is a bipartite local state.

The second scheme, like the first, makes use of unbounded violations of Bell inequalities. In this case, however, the protocol relies on the more recent results presented in [83], where is shown that the maximally entangled state $|\Psi_d\rangle$ may lead to unbounded violations of the *Khot-Visnoi inequalities*. The violations are of order

$$\nu\left(p_{|\Psi_d\rangle}\right) \gtrsim \frac{d}{(\log(d))^2}, \tag{4.49}$$

where $\gtrsim$ denotes inequality up to a constant that does not depend on d. The scenario is the following. Suppose Alice and Bob share k copies of an isotropic state, $\rho_{\text{iso}}^{\otimes k}$, which can be written as

$$\rho_{\text{iso}}^{\otimes k} = f^k\,|\Psi_d\rangle\langle\Psi_d|^{\otimes k} + \cdots + (1-f)^k\,\frac{(\mathbf{1} - |\Psi_d\rangle\langle\Psi_d|)^{\otimes k}}{(d^2-1)^k}, \tag{4.50}$$

where, for convenience, the isotropic states are parametrized by their singlet fidelity f. Note that many copies of a maximally entangled state are equivalent to a maximally entangled state of higher local dimension, that is, $|\Psi_d\rangle^{\otimes k} = |\Psi_{d^k}\rangle$. Then, the state can be re-written as

$$\rho_{\text{iso}}^{\otimes k} = f^k\,|\Psi_{d^k}\rangle\langle\Psi_{d^k}| + \cdots + (1-f)^k\,\frac{\mathbf{1} - |\Psi_d\rangle\langle\Psi_d|^{\otimes k}}{(d^2-1)^k}. \tag{4.51}$$

By performing suitable measurements and evaluating the Khot-Visnoi in-

equality, the parties obtain, at least, a value of order

$$\nu\left(\mathbf{p}_{\rho_{\text{iso}}^{\otimes k}}\right) \succcurlyeq f^k \frac{d^k}{\left(k\log\left(d\right)\right)^2}, \tag{4.52}$$

since only the contribution of the maximally entangled term is considered. Thus, if $f > 1/d$, there will be a number k' for which $\nu\left(p_{\rho_{\text{iso}}^{\otimes k'}}\right) > 1$, thus implying that ρ_{iso} is a nonlocal resource. Since $f = 1/d$ is exactly the separability bound of isotropic states, the conclusion is that every entangled isotropic state is a nonlocal resource.

States useful for teleportation

It is a well known result in quantum information theory that having a singlet fidelity $f > 1/d$ is a necessary and sufficient condition for a state ρ, acting on $\mathcal{H}^d \otimes \mathcal{H}^d$, to provide a quantum gain in the teleportation protocol [65]. It turns out that every state that is useful for teleportation is a nonlocal resource [79].

The demonstration follows directly from the fact that every entangled isotropic state is a nonlocal resource. The reason being that any quantum state ρ can be transformed into an isotropic state by LOCC, given by the *twirling procedure*:

$$\rho_{\text{iso}} = \int \left(U \otimes U^*\right) \rho \left(U \otimes U^*\right)^\dagger dU, \tag{4.53}$$

where dU denotes the Haar measure. By noting that the twirling does not change the singlet fidelity of the state, and that the unitaries can be absorbed in the local measurements performed by the parties, this procedure implies that any state ρ violates the Khot-Visnoi inequality by the same amount as the isotropic state of same singlet fidelity.

Erased states

Other interesting examples of nonlocal resources are erased states, since they are local in a wide range of Bell scenarios and activation of nonlocality

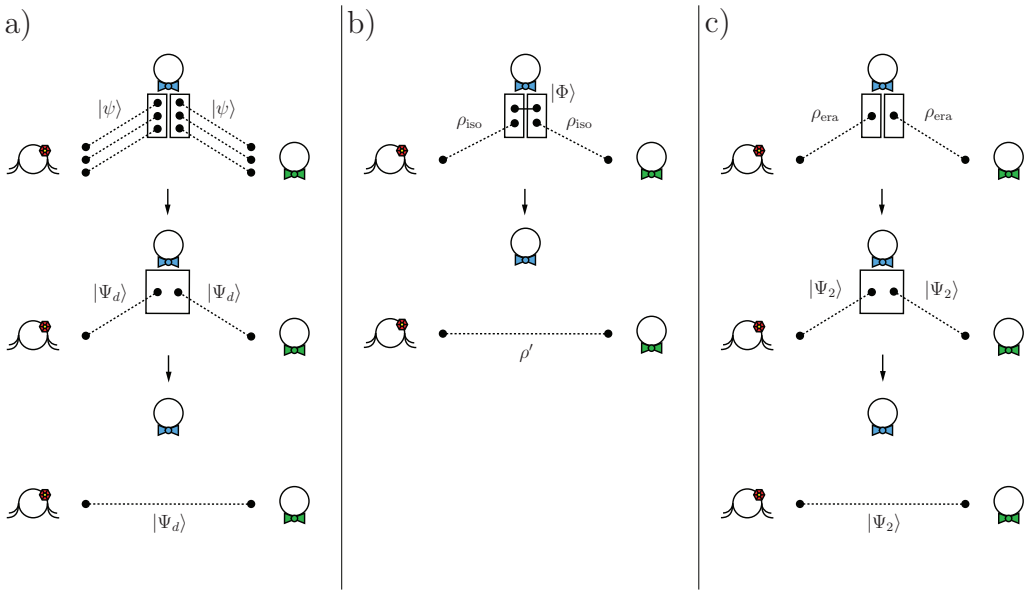


Figure 4.1: Measurement schemes of activation of nonlocality. a) One-way entanglement distillable states. First, Charlie performs one-way distillation on his subsystems, and ends up sharing maximally entangled states with Alice and Bob. Charlie, then, swaps the entanglement of his systems, thus resulting in Alice and Bob sharing a maximally entangled state. b) Isotropic states. Charlie sends the the "unbounded violation" state $|\Phi\rangle$ to Alice and Bob, using the isotropic states as channels. Alice and Bob end up sharing a noisy version of $|\Phi\rangle$, which is a function of the isotropic states, and is nonlocal for parameter regions where the isotropic states are local. c) "Erased" states. Charlie projects his subsystems into suitable subspaces. If he succeeds, he ends up sharing maximally entangled states with Alice and Bob. He then performs an entanglement swap and Alice and Bob end up sharing a maximally entangled state. In all the protocol the measurement procedures can be seen as a single measurement.

can be showed. The protocol that reveals the nonlocality of erased states is given in [55] and works as the following. Consider a tripartite scenario, where Charlie, at the center, shares a copy of an erased state with Alice and a second copy with Bob, and assume that he holds the qutrit subsystems. Charlie, then, performs a generalized measurement, consisting, first, of projective measurements that indicate if the flag states $|2\rangle$ were created. If negative results are obtained, both erased states are projected into maximally entangled states, and Charlie performs, on his subsystems, a projection in to a maximally entangled state, an operation which, if successful, results on Alice and Bob sharing a maximally entangled state. It is worth reiterating that the whole procedure applied by Charlie can be seen as a single measurement for which there is an outcome that projects the state of Alice and Bob in to a maximally entangled state. The protocol is valid for all k, implying that all erased states are nonlocal resources, whose nonlocality can be activated in a very simple two-copy, tripartite scenario.

Two-qubit states

A result presented in [12] reveals, by means of numerical tools, that there are two-qubit states that do not violate the CHSH inequality but are nonlocal resources, nonetheless. The algorithm works as follows. First, a random two-qubit density matrix is drawn according to the Hilbert-Schmidt measure [84]. Then, the necessary and sufficient criterion for violation of the CHSH inequality, proposed in [57], is checked. If the state does not violate the CHSH inequality, the sufficient criterion for one-way distillability is checked: if it is satisfied, the state is indeed a nonlocal resource, even though it does not violate the CHSH inequality. Of 10^6 random states, about 99.1% happened not to violate the CHSH inequality. Among these, 0.08% are one-way entanglement distillable, and, thus, nonlocal resources.

5

Device-independent protocols

With the development of quantum information theory, the formalism of nonlocality theory has been identified as an important tool, capable of certifying security and privacy of quantum cryptographic protocols, even in the most paranoid scenarios, due to its device-independent properties.

This formalism was soon extended to encompass different applied protocols, like randomness amplification, and adapted to more fundamental tasks, like state and entanglement estimation, and assessment of the dimension of physical systems. The ideas of device-independence became, themselves, independent of the nonlocality-based formalism, and different approaches were developed, like the self-testing methodology.

This chapter superficially presents some of the main device-independent protocols and tools used within the device-independent formalism.

5.1 Cryptography

Cryptography is the science and practice of hiding, transmitting and retrieving information privately and securely. On its grounds, lies the most studied and developed application of quantum information theory: quantum cryptography.

The main task of quantum cryptography is *quantum key distribution* (QKD). In an important class of cryptographic protocols, two parties interested in stablishing a secure communication channel must share cryptographic keys - collections of correlated random bits. One of the parties, say, Alice, uses its key to code the message she wants to transmit, in a way

that only Bob, who holds a corresponding key, can decode it. The coded message can, then, be sent through a public channel, since any third party, usually referred as Eve, possibly malevolent, will not be able to retrieve any information from the intercepted message. The only difficulty in such private key protocols is the first stage: key distribution. Eve focuses her efforts on this stage, with the hope of retrieving information about the keys.

The main advantage of using quantum systems for key distribution is that, in general, interventions of Eve during the key distribution process may damage the key, and, this way, may be detected by Alice and Bob *a posteriori*. This property allows them to distinguish between secure and nonsecure keys, and use only those that are provably trustable.

The first QKD protocol was created by Charles Bennett and Giles Brassard, in 1984, and became known as BB84 [13]. This protocol works as follows. In each round, Alice prepares a qubit system in one of the states $\left|\psi_{a|x}\right\rangle$

$$\left|\psi_{0|0}\right\rangle = |0\rangle\,, \qquad \left|\psi_{0|1}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \tag{5.1}$$

$$\left|\psi_{1|0}\right\rangle = |1\rangle\,, \qquad \left|\psi_{1|1}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \tag{5.2}$$

where a represents the state of basis x that Alice is preparing. She sends it to Bob, who, then, performs a randomly chosen projective measurement y on the system, each of which has outcomes b associated to the projectors $\Pi_{b|y} = \left|\psi_{b|y}\right\rangle\left\langle\psi_{b|y}\right|$. At the end of N iterations, Alice has two lists of bits, $\{a_i\}_{i=1}^N$ and $\{x_i\}_{i=1}^N$, while Bob has the lists $\{b_i\}_{i=1}^N$ and $\{y_i\}_{i=1}^N$. Now, Alice and Bob broadcast their lists of basis choices, x and y. For the entries i such that $x_i = y_i$, the values of a and b are supposed to be correlated, $a_i = b_i$, so, they keep those entries as the raw key and discard the remaining ones, for which the probability of correlation is $1/2$.

The security of this protocol relies on the fact that Eve cannot intercept the qubits, copy their information and resend them to Bob, due to the no-cloning theorem [26]. Eve, however, could intercept and measure the qubits, preparing different systems to send to Bob. This intervention would

destroy the perfect correlation between the bit strings of Alice and Bob, though, and by sacrificing a small sample of the key they could estimate how much of this correlation was destroyed and detect the eavesdropper on the line.

In fact, the strict security of this protocol relies on a few more assumptions, that may seen natural to assume, in principle, but are crucially delicate in real-world implementations. The first is freedom of choice and secrecy of the measurement settings x and y. The second, more obvious, is privacy of the outcomes a and b. So, there can be no leakage of information from any of the legit parties. There is, however, a third assumption, namely, that Alice and Bob have full control over their systems and the devices used to prepare and measure them.

In real-world implementations of cryptography, the devices are usually not developed by the end-users, but bought from a third party. The inner mechanics of such devices are, in general, not accessible, so the end-user does not have control over the systems or the measurements that are being implemented. If, for instance, the provider of the devices is Eve, she can easily obtain full information about the key while reproducing the perfect correlations expected by Alice and Bob [16].

This simple example highlights the importance of the device-independent approach in quantum cryptography. The first ideas of what would become device-independent QKD can be traced back to Artur Ekert's seminal paper [15], where an entanglement based QKD protocol makes use of Bell inequality violations to certify that the key could not be determined prior to measurement. Later, a similar, however more general and formal arguments were used by Barrett, Hardy and Kent [85] to prove security of QKD based on the observation of nonlocal correlations by the legit parties. Although the protocol is secure against the most general attacks, it holds only for an ideal noiseless scenario. The BHK protocol was, then, considered under more realistic scenarios, and security proofs against more restricted eavesdroppers were developed [86, 87, 16]. Later, other protocols were shown to be unconditionally secure [88, 89, 90, 91].

5.2 Randomness expansion and amplification

An interesting feature of nonlocality is the intrinsic randomness of the outcomes obtained in a Bell experiment. In fact, there are local correlations that appear locally random, but this can be seen as the result of lack of knowledge about the system; since the correlations are local, at least in principle it could be possible to predict the outcomes of the measurements if the hidden variables are known.

However, if a violation of a Bell inequality is observed, then the correlations are necessarily nonlocal and the observed randomness of the outcomes must be intrinsic, and not due to any lack of knowledge. This observation led to an interesting application of the device-independent formalism: *randomness expansion*. In this class of protocols, a Bell test is performed and the local outcomes can be certified to be random if a violation of the inequality is observed. Because this process already requires some randomness *a priori*, in the form of the choices of measurements performed by Alice and Bob, that must be already random, this protocol does not create *better* random bits, but *more* random bits - in fact, there is up to an *exponential* gain - , with the advantage inherited from QKD protocols that the new random bits are also private.

An example of randomness expansion protocol is presented by Stefano Pironio *et al.*, in [17]. The authors consider a Bell experiment where the CHSH inequality is evaluated, and compute the minimum amount of randomness - quantified by the largest min-entropy[1] among those evaluated for all the marginal probability distributions - over all joint probability distributions that could lead to a violation greater than or equal to the observed one. This gives a lower bound on the randomness of the marginal probability distributions compatible with the observed nonlocal correlations, and, in this sense, the violation of the CHSH inequality can be used to certify

[1]The min-entropy H_{min} is defined as the *information* of the maximum probability of a given distribution, that is, given a probability distribution $p(i)$, $H_{min}(p) = -\log(\max_i p(i))$.

such randomness. Ideally, this optimization should be performed over the set $\mathcal{Q}$ of quantum correlations. However, this set is complex and has not been fully characterized, even in the simplest Bell scenarios. To overcome this problem, the commonly used approach is to approximate the set of quantum correlations with the *NPA hierarchy* of sets of correlations that approximate the quantum set (*vide* section 5.6). With this approach, there is an efficient implementation of the problem by means of semi-definite programming.

In the particular Bell scenario considered in [17], the problem can be solved analytically, using some convenient properties of the CHSH operator - of which some are given on chapter 6. The optimal probability p^* leading to the minimum amount of local randomness is given, in terms of the CHSH parameter S, by

$$p^* = \frac{1}{2}\left[1 + \sqrt{2 - \left(\frac{S}{2}\right)^2}\right]. \tag{5.3}$$

From this one can see that a maximal quantum violation of the CHSH inequality certifies perfect randomness, while the observed value $S = 2$, attainable with local correlations, does not certify any randomness.

A second class of protocols explores the device-independent formalism to certify *randomness amplification*. In this class of protocols, Bell tests are used to create *better* random bits, in the sense that they are more random than the bits associated to the choices of measurements, as quantified, once more, by the min-entropy of the correspondent probability distributions.

The first device-independent randomness amplification protocol was presented by Colbeck and Renner [92]. By using a family of inequalities known as *chained Bell inequalities*, they authors prove that the outcomes obtained are slightly more random than the choice of measurements must be. The main drawback of this result, however, is the quality of the initial randomness, that must be, already, very high. This obstacle has been recently overtaken by Gallego *et al.*, [93]. In this new result, the authors consider a five-partite Bell scenario where device-independent randomness amplifica-

tion can be obtained even for sources that present a behaviour arbitrarily close to deterministic, that is, sources that return a certain outcome with probability arbitrarily close to one; however, as expected, the probability cannot be identically one.

5.3 Dimension witnessing

Another remarkable application of the device-independent approach is on estimating the dimension of a physical system.

Two distinct approaches have been developed to witness the dimension of physical systems. The first relies on nonlocality and Bell inequalities, in particular the CGLMP inequalities [36], presented in chapter 3. Some of these inequalities, defined in the $(2, 2, r)$ Bell scenario, have the interesting property that the maximum quantum violation possible with a given system depends on the dimension of the Hilbert space associated to such system [94]. This way, each of these maxima, together with the inequality, defines a dimension witness of the respective dimension d, and if a violation of such is observed, one can conclude that the system is at least $(d + 1)$-dimensional. In fact, this approach is general and applies to any Bell inequality for which quantum violation bounds depending on the dimension can be obtained [95, 96].

The second approach does not rely on nonlocality, but on measurements on a single system. The scenario is the following. Assume there is a preparing device, that admits an input x, of a set of possible inputs X, and prepares a system in state ρ_x. The system is, then, sent to a measuring device, that admits an input y, of a set of possible inputs Y, and returns an output b, of a set of possible outputs B. By repeating the experiment several times, it is possible to estimate the probabilities $p(b|x, y)$, for all b, x and y. These probability distributions have to obey several constraints that depend on the dimension of the system. In fact, like the local correlations, they are structured in convex sets with a finite number of extremal points, that is, in polytopes. By checking a collection of inequalities, it is possi-

ble, then, to estimate the classical and quantum dimensions of the system [18, 97, 98].

5.4 State and entanglement estimation

An essential task that must be carried out at some point in basically every experiment dealing with quantum systems is an estimation of the state of the system. This is usually accomplished by a procedure known as *quantum tomography* [99]. Like its classical counterpart, quantum tomography relies on performing several measurements on the system, and, by gathering all the collected partial information, obtain complete information about such system.

An efficient tomographic protocol is one where the least necessary number of measurements is performed to determine the complete state of the system. This procedure, however, relies heavily on the assumption that the dimension of the system is known, and that the measurement devices behave exactly as expected.

In order to overcome some of these assumptions and still be able to assess some properties of the state, a device-independent protocol for state estimation has been proposed [100]. The protocol is nonlocality-based, and uses several interesting properties of the CHSH operator[2] to assess quantitatively the entanglement of bipartite pure states.

Since entanglement is necessary for Bell inequality violation, Bell inequalities can be seem as device-independent entanglement witnesses [58]. Multipartite entanglement is known to have a complex structure, with many nonequivalent types of entanglement. Surprisingly, there are Bell inequalities that can be used to witness different types of entanglement in a device-independent manner [101].

[2]Many of the these properties are listed in chapter 6 and proved in the appendix.

5.5 Self-testing of quantum states and gates

Another instance of tasks that fit into the device-independent approach is the class of *self-testing protocols*. In fact, self-testing and device-independent may be, simply, different names for the same property, namely, the possibility of assessing some properties of given devices based solely on classical variables and on the statistics of such quantities.

The first self-testing protocol is due to Mayers and Yao [102, 103]. The key idea behind it is that there are specific measurements over two-qubit maximally entangled states that lead to probabilities that can only be achieved from that state and those measurements, up to *local isometries*[3].

If the observed statistics $p(a, b|x, y)$ are the only available data, the state of the system and the measurements that originate such probabilities can be characterized, at most, up to local isometries. If there are no assumptions about the dimension of the Hilbert space associated to the system, then, one can see that

$$p(a, b|x, y) = \mathrm{Tr}\left(\rho E_{a|x} \otimes F_{b|y}\right) = \mathrm{Tr}\left(\bar{\rho}\bar{E}_{a|x} \otimes \bar{F}_{b|y}\right), \tag{5.4}$$

where, for instance, $\bar{\rho} = \rho \otimes \sigma$, $\bar{E}_{a|x} = E_{a|x} \otimes \mathbf{1}$ and $\bar{F}_{b|y} = F_{b|y} \otimes \mathbf{1}$. As an example, consider the following pure state of a bipartite system, associated to the Hilbert space $\mathcal{H}^d \otimes \mathcal{H}^d$, where d is assumed to be even,

$$|\psi\rangle_{AB} = \sum_{i=0}^{d/2-1} c_i \frac{|2i, 2i\rangle + |2i+1, 2i+1\rangle}{\sqrt{2}}. \tag{5.5}$$

Assume that, at each party, are appended the subsystems of an ancillary two-qubit system in the state $|00\rangle_{A'B'}$, and local isometries $\Phi_{AA'}$ and $\Phi_{BB'}$

[3] An isometry is a distance-preserving map between metric spaces. In the context of self-testing, it is local in the sense that it respects the different partitions of a given scenario, even though it could act globally on all systems of a given party

are applied, where $\Phi_{CC'}$ is defined by

$$\Phi_{CC'} |2i, 0\rangle_{CC'} = |2i, 0\rangle_{CC'} ; \tag{5.6}$$

$$\Phi_{CC'} |2i + 1, 0\rangle_{CC'} = |2i, 1\rangle_{CC'} , \tag{5.7}$$

for C denotes either system A or B. Then, it follows that

$$(\Phi_{AA'} \otimes \Phi_{BB'}) |\psi\rangle_{AB} |00\rangle_{A'B'} = |\phi\rangle |\Psi_2\rangle_{A'B'} , \tag{5.8}$$

where $|\phi\rangle = \sum_{i=0}^{d/2-1} c_i |2i, 2i\rangle_{AB} |\Psi_2\rangle$ is the two-qubit maximally entangled state. Thus, it follows that the state $|\psi\rangle$ is equivalent to the two-qubit maximally entangled state, up to local isometries[4].

The argument of Mayers and Yao was later made robust against noise [104], and, recently, a different approach to self-testing, that links its ideas to nonlocality and Bell scenarios, has been introduced [105], where a robust self-testing of the singlet state is presented. In chapter 7, based on the results of [20], the first self-testing of a non-maximally entangled state is presented. Now, a wide class of non-maximally entangled states can be self-tested by means of the methods presented in [106].

5.6 The NPA hierarchy

The device-independent characterization of the set of quantum correlations $\mathcal{Q}$ of a given Bell scenario is known to be a hard problem, and even in the simplest scenarios little is known. This is due, partially, to the fact that this set, although convex, has infinitely many extremal points, and, contrary to the sets $\mathcal{L}$ and $\mathcal{P}$, is not a polytope.

However, it is possible to numerically approximate the set $\mathcal{Q}$ by a hierarchy of sets of correlations that can be efficiently implemented by means of semi-definite programs. This has been known as the *NPA hierarchy*, named after Miguel Navascués, Stefano Pironio and Antonio Acín [107].

[4]Strictly speaking, the state $|\psi\rangle \otimes |00\rangle$ is equivalent to the state $|\phi\rangle \otimes |\Psi_2\rangle$ by local isometries

Consider, first, the following lemma:

Lemma 5. *Let $\mathcal{G} = \{G_1, \ldots, G_n\}$ be a collection of operators acting on $\mathcal{H}$. The matrix*

$$[M]_{ij} = \mathrm{Tr}\left(\rho G_i^\dagger G_j\right), \tag{5.9}$$

is positive semi-definite for all density operators ρ acting on $\mathcal{H}$.

Proof. For any vector $|\psi\rangle \in \mathbb{C}^n$, it holds

$$\langle\psi| M |\psi\rangle = \mathrm{Tr}\left(\rho \left(\sum_i \psi_i G_i^\dagger\right)\left(\sum_j \psi_j G_j\right)\right) \geq 0; \tag{5.10}$$

because both ρ and any operator of the form $G^\dagger G$ are positive. □

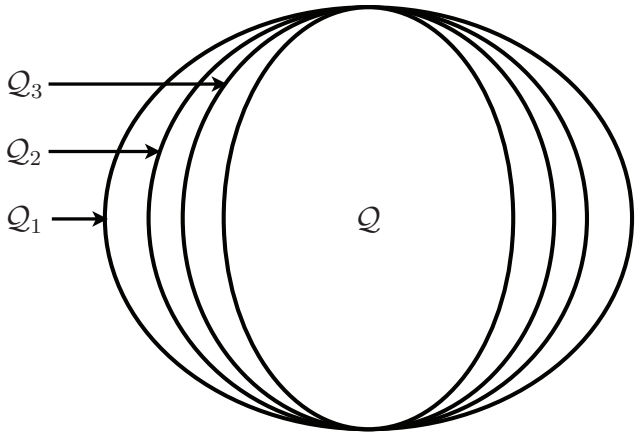


Figure 5.1: Representation of the sets $\mathcal{Q}_i$ of the NPA hierarchy. The set $\mathcal{Q}$ represents the set of quantum correlations.

Now, assume, for simplicity, the bipartite scenario $(2, 2, 2)$. Let $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{G}_1 = \mathbf{1} \cup E_a|x \otimes \mathbf{1} : a, x \in 0, 1 \cup \mathbf{1} \otimes F_b|y : b, y \in 0, 1$, where $E_{a|x}$ are arbitrary POVM effects acting on $\mathcal{H}_A$ and $F_{b|y}$ are arbitrary POVM effects acting on $\mathcal{H}_B$, for $a, b, x, y \in \{0, 1\}$. If a probability distribution

$p(a,b|x,y)$ is quantum, $p \in \mathcal{Q}$, there exist a state ρ and POVM effects $E_{a|x}$ and $F_{b|y}$ such that

$$p(a,b|x,y) = \mathrm{Tr}\left(\rho\left(E_{a|x} \otimes F_{b|y}\right)\right), \tag{5.11}$$

and the above joint probabilities can be assigned as entries of the matrix M. There are, however, some entries that cannot be observed experimentally: they are joint probabilities of the outcomes of non-compatible measurements, $p_A(a,a'|x,x')$ and $p_B(b,b'|y,y')$ for $x \neq x'$ and $y \neq y'$. According to the lemma, if $p(a,b|x,y)$ is quantum these probabilities can be assigned values $q_A(a,a'|x,x')$ and $q_B(b,b'|y,y')$, for $x \neq x'$ and $y \neq y'$, for all a,a',b,b', such that the matrix

$$M_1 = \begin{pmatrix}
1 & p_A(0|0) & p_A(1|0) & p_A(0|1) & p_A(1|1) & p_B(0|0) & p_B(1|0) & p_B(0|1) & p_B(1|1) \\
 & p_A(0|0) & 0 & q_A(0,0|0,1) & q_A(0,1|0,1) & p(0,0|0,0) & p(0,1|0,0) & p(0,0|0,1) & p(0,1|0,1) \\
 & & p_A(1|0) & q_A(1,0|0,1) & q_A(1,1|0,1) & p(1,0|0,0) & p(1,1|0,0) & p(1,0|0,1) & p(1,1|0,1) \\
 & & & p_A(0|1) & 0 & p(0,0|1,0) & p(0,1|1,0) & p(0,0|1,1) & p(0,1|1,1) \\
 & & & & p_A(1|1) & p(1,0|1,0) & p(1,1|1,0) & p(1,0|1,1) & p(1,1|1,1) \\
 & & & & & p_B(0|0) & 0 & q_B(0,0|0,1) & q_B(0,1|0,1) \\
 & & & & & & p_B(1|0) & q_B(1,0|0,1) & q_B(1,1|0,1) \\
 & & & & & & & p_B(0|1) & 0 \\
 & & & & & & & & p_B(1|1)
\end{pmatrix}$$

is positive semi-definite, where $p_A(a|x)$ and $p_B(b|y)$ are the marginal probabilities of $p(a,b|x,y)$ and the symmetric entries are omitted. The set of all the probability distributions $p(a,b|x,y)$ for which $M_1 \geq 0$ is strictly greater than the quantum set, and is denoted $\mathcal{Q}_1$. This is the first step of the NPA hierarchy, and any optimization over the set $\mathcal{Q}_1$, like, for instance, the maximization of the value of a given Bell inequality, can be easily and efficiently implemented as a semi-definite program.

The next sets of the hierarchy, $\mathcal{Q}_i$, are the sets of probability distributions $p(a,b|x,y)$ for which $M_i \geq 0$. The matrix M_i is based on new sets of operators $\mathcal{G}_i$, defined recursively as the sets whose elements are products of two elements of the previous set, $\mathcal{G}_i = \{J_1 J_2 | J_1, J_2 \in \mathcal{G}_{i-1}\}$. From the above definition, it becomes clear that $\mathcal{Q}_1 \subset \mathcal{Q}_2 \subset \ldots$, and, indeed, these sets are hierarchically organized. Finally, it has been proven that this hierarchy of sets converge to the set of quantum correlations, $\lim_{i\to\infty} \mathcal{Q}_i = \mathcal{Q}$ [107, 108]. It is worth stressing that, even though the above example is for the scenario

$(2, 2, 2)$, these techniques can be applied to any Bell scenario.

6

Device-independent certification of entangled measurements

This chapter presents the results in [19], where a device-independent protocol is presented to assess if a given measurement device is *entangled*, *i.e.*, at least one of its eigenvectors is not separable, or, in the case of POVMs, at least one of the effects do not factor in the subsystems.

To show that a given measurement is entangled, it is first shown that such measurement is *entangling* in an *entanglement swapping* [109] scenario, where, at first, a system A is entangled with a system C', and a system B is entangled with a system C'', but neither A and B nor C' and C'' are entangled among themselves; then, a measurement in systems $C'C''$ is entangling if there is an outcome such that the state after measurement of systems A and B are entangled.

All the tests are performed in a device-independent manner according to this novel protocol, and nothing is assumed despite the fact that the quantum formalism is correct and that two clearly defined systems may be assigned to Charlie. The particular case of two-qubit systems is studied in detail, where it is possible to extend the analysis to a quantitative one and estimate, based on the protocol, how entangled the measurement is.

6.1 The CHSH operator revisited

Let $\mathcal{B}$ be a CHSH operator, acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, given by

$$\mathcal{B} = A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)\,, \tag{6.1}$$

where A_x and B_y are dichotomic observables, acting on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. This important object has been widely studied, and plenty of interesting properties have been listed. Some of these properties are presented below as lemmas.

The following two lemmas apply for CHSH operators acting on bipartite Hilbert spaces of any dimension.

Lemma 6 (Landau [40])**.** *The maximum CHSH value achievable in an quantum Bell test with given observables A_0, A_1, B_0 and B_1 is given by the largest eigenvalue of the respective CHSH operator $\mathcal{B}$. This can be denoted by the maximum norm of $\mathcal{B}$, and is given by*

$$|\mathcal{B}| \leq \sqrt{4 + |[A_0, A_1]|\,|[B_0, B_1]|}. \tag{6.2}$$

Since this bound is tight, it follows that, for maximal violation of the CHSH inequality to be achieved, it is necessary that the local observables anti-commute, $[A_0, A_1] = 2A_0A_1$, $[B_0, B_1] = 2B_0B_1$.

The above lemma is proved in chapter 3, section 3.6.1.

Lemma 7 (Corollary of Masanes' lemma (appendix))**.** *There are subspaces $\mathcal{H}_{Ai}$ of $\mathcal{H}_A$ and $\mathcal{H}_{Bj}$ of $\mathcal{H}_B$ such that the CHSH operator can be written as $\mathcal{B} = \bigoplus_{i,j} \mathcal{B}_{ij}$, where $\mathcal{B}_{ij}$ is a CHSH operator acting on $\mathcal{H}_{Ai} \otimes \mathcal{H}_{Bj}$, and the dimensions of $\mathcal{H}_{Ai}$ and $\mathcal{H}_{Bj}$ are, at most, 2.*

The above lemma is a direct corollary of Masanes' lemma [76], proved in the appendix. It states that the CHSH operator can always be decomposed as a direct sum of two-qubit CHSH operators, acting on $\mathcal{H}^2 \otimes \mathcal{H}^2$, and, if necessary, of CHSH operators acting on lower-dimensional spaces.

So, there are properties of $\mathcal{B}$ that follow directly from the properties of the two-qubit CHSH operator. The following lemmas apply for CHSH operators acting on $\mathcal{H}^2 \otimes \mathcal{H}^2$.

Lemma 8 (Horodecki *et al.*, [110])**.** *Given a two-qubit state ρ, the maximum CHSH value achievable in a Bell test where projective measurements are*

performed on such state is given by

$$S = 2\sqrt{u_0 + u_1}, \tag{6.3}$$

where u_0 *and* u_1 *are the largest eigenvalues of the matrix* $U = T^T T$*, and the matrix* T *is defined as* $T_{mn} = \mathrm{Tr}\left(\rho\left(\sigma_m \otimes \sigma_n\right)\right)$*, where* σ_i *are the Pauli matrices.*

This lemma is proved in the appendix.

Lemma 9 (Scarani *et al.*, [111])**.** *The spectral decomposition of the CHSH operator is, up to local unitaries,*

$$\mathcal{B} = \sum_{i=1}^{4} \alpha_i \left|\psi_i\right\rangle \left\langle\psi_i\right|, \tag{6.4}$$

where the coefficients α_i *are functions of the local observables obeying* $\alpha_1 = -\alpha_3$*,* $\alpha_2 = -\alpha_4$*; and* $\alpha_1^2 + \alpha_2^2 = 8$*, and the states* $\left|\psi_i\right\rangle$ *are the* Bell states

$$\left|\psi_1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right), \qquad \left|\psi_2\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle - \left|11\right\rangle\right), \tag{6.5}$$

$$\left|\psi_3\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle + \left|10\right\rangle\right), \qquad \left|\psi_4\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle - \left|10\right\rangle\right). \tag{6.6}$$

This lemma is one of the main results of [111], where it is stated, in a more general form, and proved. It follows that the maximal violation of the CHSH inequality can be achieved if, and only if, the state of the system is maximally entangled, if the system is a two-qubit one. In fact, it has been proven, with different techniques, that, in arbitrary Hilbert spaces, maximal violation can be achieved if, and only if, the state of the system is maximally entangled, up to local isometries [105].

The last lemma here stated is a curious result, as it bounds an unconventional quantity: the maximal CHSH value achievable over separable states. Interestingly, for certain local observables, the local bound of the CHSH inequality cannot be achieved with separable states. The lemma holds for

CHSH operators acting on arbitrary Hilbert spaces, and is proved in the appendix.

Lemma 10 (Rabelo *et al.*, [19])**.** *For given local observables A_0, A_1, B_0 and B_1, the maximum CHSH value achievable on a quantum Bell test with separable states is*

$$S_{Sep} = \frac{\lambda + \sqrt{8 - \lambda^2}}{2}, \tag{6.7}$$

where λ is the smallest eigenvalue of $\mathcal{B}$ such that $\lambda > 2$.

6.2 The protocol

Consider a tripartite Bell scenario, where Alice and Bob can perform two possible measurements, denoted $x \in \{0, 1\}$ and $y \in \{0, 1\}$, each of which with two possible outcomes, $a \in \{0, 1\}$ and $b \in \{0, 1\}$, respectively. Charlie, however, can perform three possible measurements, denoted $z \in \{0, 1, 2\}$, with four possible outcomes each, $c \in \{0, 1, 2, 3\}$. It constitutes, thus, the $(2, 2; 2, 2; 4, 4, 4)$ Bell scenario. It is assumed that, in each run, all three parties choose randomly which measurement to perform. The goal is to guarantee in a device-independent fashion, that is, without making assumptions on the dimension and state of the system and on the measurements performed, that $z = 2$ is an entangled measurement (fig. 6.1).

After the experiment has been performed for a large number of times, and the joint probabilities of the outcomes, conditioned on the measurements performed, $p(a, b, c|x, y, z)$ has been estimated, the following tests are, then, performed, based on the measurement performed by Charlie:

- If Charlie has measured $z = 0$ or $z = 1$, the marginals $p_{AC}(a, c'|x, z)$ and $p_{BC}(b, c''|y, z)$ are used to test the CHSH inequalities of Charlie with Alice (S_{AC}) and of Charlie's with Bob (S_{BC}). For this, Charlie has to define a classical processing that transforms his four outcomes into two bits, c' and c'', to be correlated with Alice's outcome and with Bob's outcome, respectively.

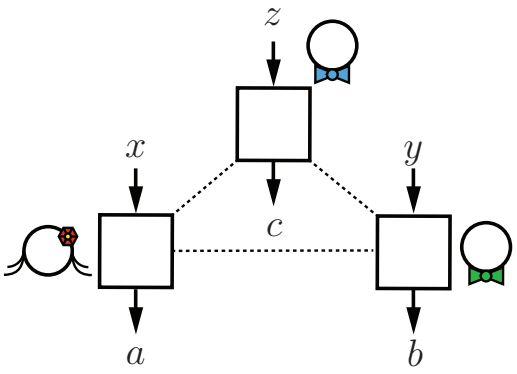


Figure 6.1: DI certification of entangled measurements protocol scenario. The scenario consists of three space-like separated parties. If Charlie performs measurement $z = 2$, then the CHSH inequality is evaluated for Alice and Bob's measured data. Otherwise, the CHSH inequality is evaluated both for Alice and Charlie and for Bob and Charlie.

- If Charlie has measured $z = 2$, the marginal $p_{AB}(a, b|x, y, c)$ is used to check the CHSH inequality between Alice and Bob. The form of the inequality, however, can depend on the outcome of Charlie, and the four CHSH values $S_{AB|c}$ are defined as

$$S_{AB|0} = E_{00|0} + E_{01|0} + E_{10|0} - E_{11|0}, \tag{6.8}$$
$$S_{AB|1} = E_{00|1} + E_{01|1} - E_{10|1} + E_{11|1}, \tag{6.9}$$
$$S_{AB|2} = -E_{00|2} - E_{01|2} + E_{10|2} - E_{11|2}, \tag{6.10}$$
$$S_{AB|3} = -E_{00|3} - E_{01|3} - E_{10|3} + E_{11|3} \tag{6.11}$$

  where $E_{xy|c} = p(a = b|x, y, c) - p(a \neq b|x, y, c)$. Note that Alice and Bob do not need to know c in each run, since their measurement settings are always the same; the above statistics can be evaluated at the end of the whole experiment.

The first step of the analysis is to certify, in a device-independent way, that the measurements of Charlie are performed on two systems that are not entangled *a priori*. This can be certified by S_{AC} and S_{BC}: if both S_{AC} and S_{BC} are equal to $2\sqrt{2}$, then:

- Charlie holds a bipartite system;
- the states ρ_{AB} of the systems of Alice and Bob and $\rho_{C'C''}$ of the systems of Charlie are both product states.

If $S_{AC} = 2\sqrt{2}$ and $S_{BC} = 2\sqrt{2}$, then the state of the tripartite system is, up to local isometries, $|\Psi_{AC'}\rangle \otimes |\Psi_{BC''}\rangle$, where $|\Psi\rangle$ denotes the maximally entangled state in the Hilbert spaces of the respective systems [112, 9, 105]. It follows from *monogamy of entanglement* [113] that, if two systems are in a maximally entangled state, then none of them can be correlated with any other system. Then, if Charlie holds a system C' that is maximally entangled to A, there must be a second system C'' that is maximally entangled with B, and the bipartite system $C'C''$ cannot be entangled, as well as the system AB cannot be entangled.

In fact, with a similar argument it is possible to show that both properties hold if either S_{AB} or S_{BC} is equal to $2\sqrt{2}$, provided that the other is greater than 2. It is easy to note that, if this condition holds, then $S_{AB|c} > 2$ implies that measurement $z = 2$ is entangled. The condition that both values are equal to the maximal violation, however, returns several useful properties, and a violation of the CHSH inequality by parties A and B is not even necessary, as stated in the following theorem.

6.3 Main theorem

Theorem 5. *If $S_{AC} = S_{BC} = 2\sqrt{2}$, and $z = 2$ is a separable measurement - i.e., all the eigenvectors of the associated observable are separable, or, in the case of POVMs, all the effects factor in the subsystems - , then $S_{AB|c} \leq \sqrt{2}$.*

Proof. As previously stated, if $S_{AC} = S_{BC} = 2\sqrt{2}$, then the states of bipartite systems AC' and BC' are, up to local isometries, maximally entangled and are completely uncorrelated from any other system. Thus, any state steered by measurement $z = 2$ - assuming it is separable - to parties AB will be separable, and will have support on at most in the same subspaces of $\mathcal{H}_A$ and $\mathcal{H}_B$ where the initial states have support on. Let $\mathcal{B}_{AC'} = \bigoplus_{i,j} \mathcal{B}_{i,j}$

and $\mathcal{B}_{BC''} = \bigoplus_{k,l} \mathcal{B}_{k,l}$ be the CHSH operators acting on he Hilbert spaces of systems AC' and BC'', respectively, decomposed according to Masanes' lemma. From the spectral decomposition of the two-qubit CHSH operator, $S_{AC} = S_{BC} = 2\sqrt{2}$ implies that the CHSH operators $\mathcal{B}_{i,j}$ and $\mathcal{B}_{k,l}$ have maximal eigenvalues $\alpha_{i,j} = \alpha_{k,l} = 2\sqrt{2}$. This immediately implies that, for the same subspaces, the CHSH operators in parties AB, $\beta_{i,k}$, will also have maximal eigenvalues $\alpha_{i,k} = 2\sqrt{2}$; this follows from lemma 6.

Thus, it is possible to conclude that, for all subspaces $\mathcal{H}_{Ai} \otimes \mathcal{H}_{Bk}$ where the final steered separable state of AB, ρ_{AB}, has support on, the two-qubit CHSH operators has eigenvalues $\pm 2\sqrt{2}$. Now, according to lemma 10, the maximum value of the CHSH operator achievable with a separable state is

$$S_{Sep} = \frac{\lambda + \sqrt{8 - \lambda^2}}{2}, \tag{6.12}$$

where λ is the smallest eigenvalue of $\mathcal{B}$ such that $\lambda > 2$. Since λ, in this case, is equal to $2\sqrt{2}$, it follows that

$$S_{AB|c} \leq \sqrt{2}. \tag{6.13}$$

□

The presented results rely on at least one between S_{AC} and S_{BC} being exactly $2\sqrt{2}$. Relaxing this constraint leads to one main difficulty: even for the smallest deviation from the ideal values, ρ_{AB} cannot be guaranteed to be separable anymore. Similarly, one cannot guarantee, in a device-independent way, that Charlie has two subsystems. This assumption may, however, be very natural in some implementations, in which Charlie receives one quantum signal from Alice and one from Bob.

6.4 Characterizing a specific measurement

An interesting particular case of the protocol is the extremal one, where

$$S_{AC} = S_{BC} = S_{AB|c} = 2\sqrt{2}. \tag{6.14}$$

This can be achieved in quantum theory, and, in fact, with qubits, by means of the *entanglement swapping protocol* [14]. If Charlie shares maximally entangled states of two-qubit systems with both Alice and Bob, and if $z = 2$ is a *Bell-state measurement*, that is, a projective measurement where the projectors are associated to the Bell states (6.5). Assume that the measurements of Alice are given by the dichotomic observables $A_0 = \sigma_3$ and $A_1 = \sigma_1$, the measurements of Bob are given by $B_0 = (\sigma_3 + \sigma_1)/\sqrt{2}$, the measurements of Charlie are $C_0 = (\sigma_1 + \sigma_3)/\sqrt{2}$, and $C_1 = (\sigma_3 - \sigma_1)/\sqrt{2}$. Finally, assume that projectors $\Pi_{c|2}$, associated to the outcomes c of measurement $z = 2$ are given by the Bell states, $\Pi_{c|2} = |\psi_c\rangle\langle\psi_c|$. Then, $S_{AC} = S_{BC} = S_{AB|c} = 2\sqrt{2}$ is obtained; the values of $S_{AB|c}$ are evaluated according to (6.8).

The protocol presented is valid under very specific conditions, but could, in principle, lead to a much finer statement. For instance, if one is close to satisfying (6.14), then measurement $z = 2$ should be close to an ideal Bell-state measurement. It should, therefore, be possible to bound the distance t between the actual and the ideal measurement as a function of the observed violations. The derivation of this bound, in a full device-independent scenario, $t \leq f_{DI}(S)$, hits several difficulties, but it is possible, under additional assumptions, to obtain a bound $t \leq f(S)$. Clearly, $f(S) \leq f_{DI}(S)$, and one can conclude that a device-independent estimate of t will be *at least as bad as* $f(S)$.

The scenario considered is a four-qubit scenario, similar to the one defined above. The states of the systems and measurements are defined to be exactly the same, except for measurement $z = 2$: it is no longer a perfect Bell-state measurement, but is still assumed to be projective, with projectors $\Pi_{c|2}$ associated to the results c. It is not clear, *a priori*, which Bell state to associate with each result c; however, once the measured data have been sorted out according to c, one can check the inequalities (6.8), observe those with higher values, and relabel the outcomes such that projector $\Pi_{c|2}$ is associated to the closest $|\Psi_c\rangle\langle\Psi_c|$, for each $c \in \{1, 2, 3, 4\}$.

An operational measure of the distance between measurement $z = 2$

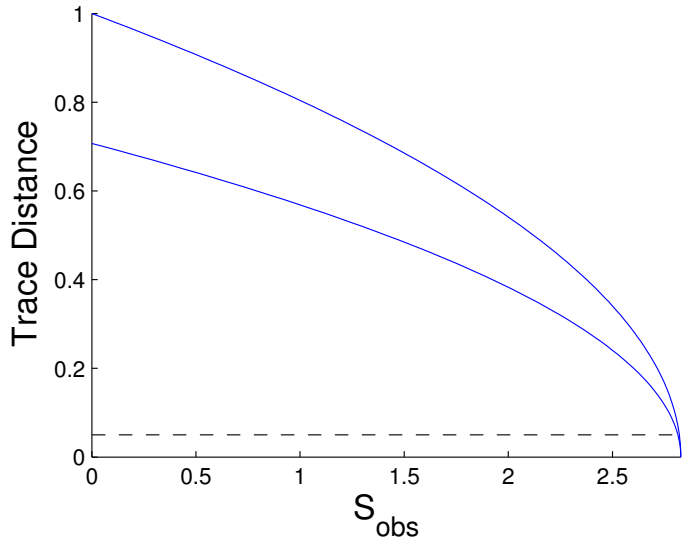


Figure 6.2: Bounds on the trace distance as functions of the observed CHSH inequality violation in the four-qubit scenario.

and an ideal Bell-state measurement is the trace distance

$$t \;=\; \max_c \sqrt{1 - \mathrm{Tr}\left(\Pi_{c|2} \left|\psi_c\right\rangle \left\langle\psi_c\right|\right)}. \tag{6.15}$$

Now, because of the choice of the local measurements of Alice and Bob, the Bell operators corresponding to the four definitions (**??**) read $\mathcal{B}_{AB|c} = 2\sqrt{2}\left(\left|\psi_c\right\rangle\left\langle\psi_c\right| - \left|\psi_{5-c}\right\rangle\left\langle\psi_{5-c}\right|\right)$. Therefore,

$$S_{AB|c} \;=\; 2\sqrt{2}\left(\mathrm{Tr}\left(\Pi_{c|2}\left|\psi_c\right\rangle\left\langle\psi_c\right|\right) - \mathrm{Tr}\left(\Pi_{c|2}\left|\psi_{5-c}\right\rangle\left\langle\psi_{5-c}\right|\right)\right), \tag{6.16}$$

and the two bounds $0 \leq \mathrm{Tr}\left(\Pi_{c|2}\left|\psi_{5-c}\right\rangle\left\langle\psi_{5-c}\right|\right) \leq 1 - \mathrm{Tr}\left(\Pi_{c|2}\left|\psi_c\right\rangle\left\langle\psi_c\right|\right)$ lead finally to

$$\sqrt{\frac{1}{2}\left(1 - \max_c \frac{S_{AB|c}}{2\sqrt{2}}\right)} \;\leq t \leq\; \sqrt{1 - \min_c \frac{S_{AB|c}}{2\sqrt{2}}}. \tag{6.17}$$

In particular, the upper bound is the expression for $f(S)$, and it indicates how stringent are the requirements for device-independent assessment of

a measurement. Recall that the trace distance is closely related to the probability of distinguishing the real case from the ideal one. Requesting that this probability is 5% looks like a pretty loose requirement; but, in order to confirm this assessment in a device independent way, one will have observe at least $\min_c S_{AB|c} \gtrsim 2.8214$ (fig. 6.2). This number is within 0.5% of the maximal value: no experiment has reached such a high violation and precision.

7

Device-independent bounds for Hardy's test of nonlocality

Introduced in 1991, *Hardy's test of nonlocality* [114, 115], or *Hardy's paradox*, is a proof of the nonlocality of quantum correlations that does not rely on Bell inequalities, but on a direct contradiction between the predictions of local theories and those of quantum mechanics, in the lines of the *GHZ paradox* [116]. Roughly, the test can be summarized as: under the assumption of local realism, a particular pair of outcomes in an experiment where two quantum systems are individually measured can never be jointly observed, given that some conditions are met. But, as any local theory predicts the probability of this event to be equal to zero, quantum mechanics predicts a nonzero probability, thus contradicting local realism.

Stated originally in terms of a thought experiment, where both the state of the system and the measurements are fixed, Hardy's test was soon extended to more general scenarios, at first to include different states and measurements, and then extended and formulated for higher-dimensional bipartite systems and multipartite systems [117, 118, 119, 120, 121, 122, 123, 124, 125]. Many experiments were performed [126, 127, 128, 129, 130], confirming, once more, the right predictions of quantum mechanics and the nonlocality of its correlations. Interestingly, though, no upper bound on the nonlocality of the quantum correlations involved, in the lines of Tsirelson's bound, was ever studied, except for very specific systems, and it has not been clear if higher-dimensional Hilbert spaces could lead to any advantages in such tests.

This chapter presents a review of the results in [20], where, for the first time, device-independent bounds were presented for Hardy's test of nonlocality. First, Hardy's original experiment is presented, followed by a straightforward device-independent reformulation of the test. The relations with the Bell scenario $(2, 2, 2)$ are highlighted, and the optimal solutions for two-qubit systems are presented. Finally, the main result is stated and proven: the optimal solutions for two-qubit systems are optimal for systems of any dimension, both in an ideal and in more realistic scenarios, where the assumed conditions are not necessarily satisfied. In the ideal case the proof is algebraic and, surprisingly, implies self-testing of a family of non-maximally entangled states, the first of the genre. In the non-ideal case, a numerical proof is presented.

7.1 Hardy's experiment

Consider an experimental setup consisting of two overlapping Mach-Zehnder interferometers, one for electrons and one for positrons, composed of $50:50$ beam splitters and detectors placed at the end of each output path. Alice and Bob, each one controlling one interferometer, for each interferometer, can freely chose to insert or remove the second beam splitter during each run of the experiment. Let the choice of removing or inserting the beam splitter be denoted $x = \{0, 1\}$, respectively, for Alice, and $y = \{0, 1\}$, respectively, for Bob; let, also, the detectors of Alice be denoted $a = \{0, 1\}$, and, the ones of Bob, $b = \{0, 1\}$ (fig. 7.1). The figures of merit are the joint probabilities $p(a, b|x, y)$ of obtaining outcomes a and b, given that the choices x and y were made[1].

The key idea behind this setup is that, if the electron and the positron both take the overlapping paths, they will annihilate each other and, thus, no detection will be observed. If both beam splitters are removed, $x = 0$, $y = 0$, the annihilation implies that outcomes $a = 0$ and $b = 0$ will never

[1]It is implicitly assumed that the measurement events are space-like separated

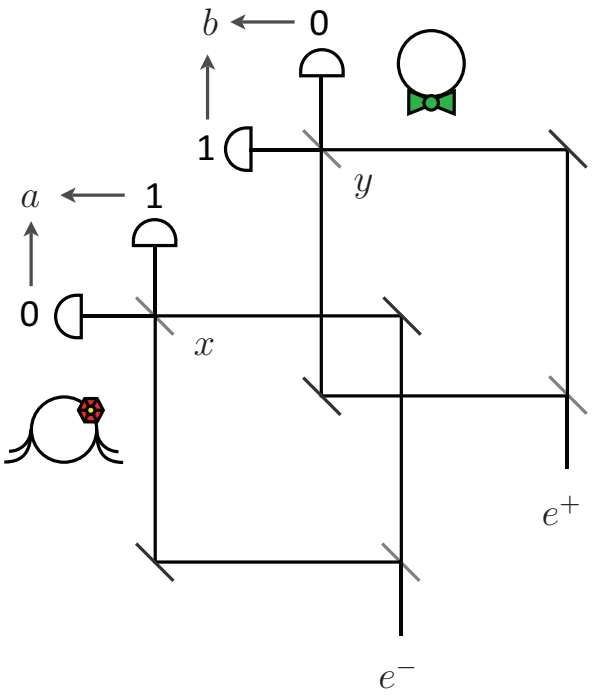


Figure 7.1: Hardy's experiment. Two Mach-Zehnder interferometers, one of electrons and the other for positrons, are arranged so that the central paths overlap. Each party has the option to include the second beam splitter, denoted by x and y. The particles are then detected in the detectors labelled by a and b.

be jointly observed, and, thus,

$$p(0,0|0,0) = 0. \tag{7.1}$$

Now, assume that each interferometer is perfectly balanced, in a way that, if each interferometer is individually considered - that is, if there is no overlap between the two of them - , detectors $a = 1$ and $b = 1$ will fire with certainty if the second beam splitters are in place, $x = 1$ and $y = 1$. Consider, then, the case where $x = 0$ and $a = 1$ is observed; the electron has certainly taken the upper path, and there is no influence of one interferometer with the other. Due to the balance of Bob's interferometer, if $y = 1$, outcome

$b = 1$ will fire with certainty, implying that joint observation of $a = 1$ and $b = 0$ when $x = 0$ and $y = 1$ is impossible,

$$p(1, 0|0, 1) = 0. \tag{7.2}$$

The same reasoning can be applied if $y = 0$ and $b = 1$ is observed: $a = 1$ fires with certainty if $x = 1$, and thus

$$p(0, 1|1, 0) = 0. \tag{7.3}$$

Now, assume that local realism holds, and each particle carries a set of instructions λ on which detector to trigger, depending on the presence of the second beam splitter. All correlations arise from the fact that these instructions are unknown, and must be averaged over,

$$p(a, b|x, y) = \int_{\Lambda} p_A(a|x, \lambda) p_B(b|y, \lambda) q(\lambda) \mathrm{d}\lambda, \tag{7.4}$$

where Λ is a set of variables λ and $q(\lambda)$ is a measure on this set. Under this assumption, (7.1) implies that either $p_A(0|0, \lambda) = 0$, for all λ, or $p_B(0|0, \lambda) = 0$, for all λ, or both.

- If $p_A(0|0, \lambda) = 0$, for all λ: $p_A(1|0, \lambda) = 1$, for all λ. It follows from (7.2) that $p_B(0|1, \lambda) = 0$, for all λ. This implies that $p(0, 0|1, 1) = 0$.
- If $p_B(0|0, \lambda) = 0$, for all λ: $p_B(1|0, \lambda = 1)$, for all λ. It follows from (7.3) that $p_A(0|1, \lambda) = 0$, for all λ. This implies that $p(0, 0|1, 1) = 0$.

Then, it follows from (7.1), (7.2), (7.3), and the assumption of local realism, that

$$p(0, 0|1, 1) = 0. \tag{7.5}$$

The probability $p(0, 0|1, 1)$ will be referred, from now on, as *Hardy's probability.*

According to quantum theory, though, Hardy's probability, in this experiment, in equal to $p(0,0|1,1) = 1/16$. The calculation is very simple, and details are given in [114]. To briefly summarize it, let $|a\rangle \in \mathcal{H}_A^2$ and $|b\rangle \in \mathcal{H}_B^2$ denote the states of systems A and B on the paths immediately before detectors a and b, and $|\gamma\rangle$ denote the state of the system - or the radiation it becomes - after annihilation. The global state of the system, $|\psi_{xy}\rangle \in \mathcal{H}_A^2 \otimes \mathcal{H}_B^2$, immediately before the detectors, depends on x and y - the presence of second beam splitters. They are:

$$|\psi_{00}\rangle = \frac{1}{2}\left(-|\gamma\rangle + i|01\rangle + i|10\rangle + |11\rangle\right), \tag{7.6}$$

$$|\psi_{01}\rangle = \frac{1}{2\sqrt{2}}\left(-\sqrt{2}|\gamma\rangle + i|00\rangle - |01\rangle + 2i|11\rangle\right), \tag{7.7}$$

$$|\psi_{10}\rangle = \frac{1}{2\sqrt{2}}\left(-\sqrt{2}|\gamma\rangle + i|00\rangle - |10\rangle + 2i|11\rangle\right); \tag{7.8}$$

which correctly return probabilities (7.1), (7.2) and (7.3), and

$$|\psi_{11}\rangle = \frac{1}{4}\left(-2|\gamma\rangle - |00\rangle + i|10\rangle + i|01\rangle - 3|11\rangle\right), \tag{7.9}$$

which gives

$$p(0,0|1,1) = \frac{1}{16}. \tag{7.10}$$

7.2 Device-independent formulation

Consider the Bell scenario $(2,2,2)$, where Alice and Bob can perform two measurements, each, on their respective subsystems, and each measurement has two possible outcomes (fig. 7.2). Without making any assumption on the nature of the physical systems or on the measurements performed,

Figure 7.2: DI formulation of Hardy's test. Pairs of particles A and B are submitted to measurements x and y, respectively. The outcomes obtained are a and b.

assume that Hardy's *constraint probabilities* hold,

$$p(0,0|0,0) = 0, \tag{7.11}$$

$$p(1,0|0,1) = 0, \tag{7.12}$$

$$p(0,1|1,0) = 0; \tag{7.13}$$

and the respective events are never observed. If the joint probability distributions that describe the Bell experiment are local, then Hardy's probability is, necessarily,

$$p(0,0|1,1) = 0. \tag{7.14}$$

Even though inspired by Hardy's experiment, the proof presented in the previous section does not assume any properties of the systems and measurements, and, thus, is device-independent. Thus, any probability distribution $p(a,b|x,y)$ for which (7.11) hold, and $p(0,0|1,1) > 0$ is nonlocal.

In the considered scenario, a probability distribution is nonlocal if, and only if, it violates the CHSH inequality. Hence, there must be a relation between this inequality and Hardy's test. This relation becomes clear if one considers the CH inequality, written as:

$$p_A(0|1) + p_B(0|1) - p(0,0|0,0) - p(0,0|0,1) - p(0,0|1,0) + p(0,0|1,1) \leq 0. \tag{7.15}$$

From the definition of marginal probabilities, one has

$$p_A(0|1) = p(0,0|1,0) + p(0,1|1,0), \tag{7.16}$$
$$p_B(0|1) = p(0,0|0,1) + p(1,0|0,1); \tag{7.17}$$

substituting this into the CH inequality, the following inequality is obtained:

$$p(0,0|1,1) \leq p(0,0|0,0) + p(0,1|1,0) + p(1,0|0,1). \tag{7.18}$$

If the constraint probabilities hold, the right-hand side of the inequality is null, implying that Hardy's probability must be equal to zero. The above inequality, however, is valid also in nonideal scenarios, giving local bounds for Hardy's probability in terms of the arbitrary values the constraint probabilities may have. The relation between Hardy's test and the CH inequality has been studied to a deeper extend on [131].

7.2.1 Optimal bounds for two-qubit systems

If one assumes a two-qubit system, it is possible to show that, by optimizing over all possible states and measurements, the maximum value of Hardy's probability is given by

$$p(0,0|1,1) = \frac{\left(5\sqrt{5}-11\right)}{2}. \tag{7.19}$$

It can be assumed that:

1. The state of the system is pure. For every mixed state ρ, if there are POVMs such that (7.11) hold, then (7.11) must hold for all pure states in the spectral decomposition of ρ, for the same POVMs. By convexity, the value of Hardy's probability obtained for ρ is upper bounded by the value obtained for one of the pure states in its spectral decomposition.

2. The measurements are projective. If the measurements are POVMs, each and every effect has to be rank 1, due to the constraint probabil-

ities; otherwise, the state is forced to be separable. Rank 1 effects, on their turn, must be proportional to rank 1 projectors, and, and the proportionality constant cannot be greater than 1. This implies that Hardy's probability will achieve higher values over such projectors than over the respective effects.

Note that these assumptions are only valid for the ideal case, where (7.11) hold.

Now, following [132], let the projectors associated with the results $a = 0$ and $b = 0$ of the measurements $x = 0$ and $y = 0$ of Alice and Bob, respectively, be $\Pi^A_{0|0} = |0\rangle\langle 0|$ and $\Pi^B_{0|0} = |0\rangle\langle 0|$. Then, the most general two-qubit pure state that obeys constraint $p(0,0|0,0) = 0$ can be written as

$$|\psi\rangle = a\,|01\rangle + b\,|10\rangle + ce^{i\varphi}\,|11\rangle\,, \tag{7.20}$$

where a, b, c and φ are real numbers such that $a^2 + b^2 + c^2 = 1$ and $0 \leq \varphi < 2\pi$. Now, from $p(0,1|1,0) = 0$, the fact that Bob's measurement $y = 0$ returned outcome $b = 1$ implies that Alice's projector associated to outcome $a = 0$ of measurement $x = 1$ has to be orthogonal to her resulting state after Bob's measurement, $\Pi^A_{0|1} = |\phi_A\rangle\langle\phi_A|$, where

$$|\phi_A\rangle \;=\; \frac{c\,|0\rangle - ae^{i\varphi}\,|1\rangle}{\sqrt{a^2 + c^2}}. \tag{7.21}$$

Analogously, from $p(1,0|0,1) = 0$, it can be inferred that Bob's projector associated to outcome $b = 0$ of measurement $y = 1$ is $\Pi^B_{0|1} = |\phi_B\rangle\langle\phi_B|$, where

$$|\phi_B\rangle \;=\; \frac{c\,|0\rangle - be^{i\varphi}\,|1\rangle}{\sqrt{b^2 + c^2}}. \tag{7.22}$$

It follows, then, that Hardy's probability is equal to

$$p(0,0|1,1) \;=\; \frac{a^2b^2c^2}{(a^2 + c^2)\,(b^2 + c^2)}. \tag{7.23}$$

This function can be easily optimized, and it has only one maximum, in the region of interest of the variables. This maximum is equal to $\left(5\sqrt{5}-11\right)/2$, achieved for

$$a = b = \sqrt{\frac{3-\sqrt{5}}{2}}. \tag{7.24}$$

This implies that, up to the phase φ and local choices of basis, there is only one two-qubit state, and a well defined set of measurements, that can achieve maximum Hardy's probability on the ideal Hardy's test.

7.3 Device-independent bounds for Hardy's test

Theorem 6. *Let $p(a,b|x,y)$, where $a,b,x,y \in \{0,1\}$, be a probability distribution for which* (7.11) *hold. Then, the maximum value of Hardy's probability for quantum systems of arbitrary finite dimension is $p(0,0|1,1) = \left(5\sqrt{5}-11\right)/2$, just as for qubits.*

Proof. Once more, it can be assumed that:

1. The state of the system is pure. The same argument used to justify this claim in the two-qubit case can be applied here.

2. The measurements are projective. According to Neumark's theorem, all probability distributions of the outcomes of POVMs can be obtained from projective measurements on systems associated with Hilbert spaces of higher dimension. Since the system, in this scenario, is arbitrary, this assumption can be applied.

Let ρ be the state of the system, acting on an arbitrary Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and $\Pi_{a|x}$, acting on $\mathcal{H}_A$, be the projectors associated with outcomes a of measurement x, of Alice, and $\Gamma_{b|y}$, acting on $\mathcal{H}_B$, be the projectors associated with the outcomes b of measurement y, of Bob. The core

of the proof exploits the following lemma, by Masanes [76], proved in the appendix:

Lemma 11 (Masanes [76])**.** *Let* $\Pi_{0|0}, \Pi_{1|0}, \Pi_{0|1}, \Pi_{1|1}$ *be four projectors acting on a Hilbert space* $\mathcal{H}$ *such that* $\Pi_{0|0} + \Pi_{1|0} = 1$ *and* $\Pi_{0|1} + \Pi_{1|1} = 1$*. There exists an orthonormal basis in* $\mathcal{H}$ *where the four projectors are simultaneously block diagonal, where the subspace* $\mathcal{H}_i$ *of* $\mathcal{H}$ *corresponding to block* i *is, at most, bidimensional,* $dim\,(\mathcal{H}_i) \leq 2$*, for all* i*.*

The lemma states that there is a basis of $\mathcal{H}_A$ where the projectors $\Pi_{a|x}$ can be written as $\Pi_{a|x} = \bigoplus_i \Pi^i_{a|x}$, where each $\Pi^i_{a|x}$ acts on $\mathcal{H}^i$, for all a and x; denote, also, $\Pi^i = \Pi^i_{+1|x} + \Pi^i_{-1|x}$ the projector on $\mathcal{H}^i_A$. The same applies to projectors $\Gamma_{b|y}$; they can be written as $\Gamma_{b|y} = \oplus_j \Gamma^j_{b|y}$, where each $\Gamma^j_{b|y}$ acts on $\mathcal{H}^j_B$, for all y and b. Then, the joint probabilities can be written as

$$p(a,b|x,y) = \sum_{i,j} q_{ij} \mathrm{Tr}\left(\rho_{ij} \Pi^i_{a|x} \otimes \Gamma^j_{b|y}\right) \tag{7.25a}$$

$$= \sum_{i,j} q_{ij} p_{ij}(a,b|x,y), \tag{7.25b}$$

where $q_{ij} = \mathrm{Tr}\left(\rho \Pi^i \otimes \Gamma^j\right)$ and $\rho_{ij} = \left(\Pi^i \otimes \Gamma^j \rho \Pi^i \otimes \Gamma^j\right)/q_{ij}$ is, at most, a two-qubit state; P^i and Γ^j denote projectors onto the $\mathcal{H}^i_A$ and $\mathcal{H}^j_B$ subspaces, respectively. Since $q_{ij} \geq 0$ for all i, j and $\sum_{i,j} q_{ij} = 1$, the constraint probabilities are satisfied for $\mathbf{p}$ if and only if they are satisfied for each of the $\mathbf{p}_{ij}$. But, then,

$$p(0,0|1,1) = \sum_{i,j} q_{ij} p_{ij}(0,0|1,1), \tag{7.26}$$

is a convex sum of Hardy's probabilities in each two-qubit subspace [2]. As a convex sum, it is upper bounded by the largest element in the combination, whose maximum value is known to be given by (7.19). This concludes the proof. □

[2]Note that for the maximum value of (7.26) to be reached it is necessary that, for all i, j such that $q_{ij} \neq 0$, the dimension of both $\mathcal{H}^i$ and $\mathcal{H}^j$ be equal to 2. This implies that the effective dimension d of the local Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of the system is even.

An alternative, simpler proof of the above theorem consists, basically, in noticing that any probability distribution that maximizes Hardy's probability is an extremal point of the set of quantum probability distributions. According to [76], every extremal point, in this scenario, can be obtained from projective measurements on two-qubit systems, thus proving the stated result. The reason for presenting the extensive proof is that it leads to interesting insights about the states that lead to such maximal violation, as discussed below. Both proofs cannot be trivially extended to the nonideal scenario later considered.

7.4 Self-testing of entangled states

It follows from the above proof that Hardy's probability $p(0,0|1,1)$ reaches its maximal value if and only if $p_{ij}(0,0|1,1)$ is maximal for every ij such that $q_{ij} \neq 0$. From the results presented in section 7.2.1, it follows that only a very specific class of two-qubit states and measurements can lead to this maximal value. Let $\Pi_{0|0} = \Gamma_{0|0} = |0\rangle\langle 0|$, $\Pi_{1|0} = \Gamma_{1|0} = |1\rangle\langle 1|$; then, this class of two-qubit states is given by

$$|\phi\rangle = a\left(|01\rangle + |10\rangle\right) + e^{i\theta}\sqrt{1-2a^2}\,|11\rangle\,, \tag{7.27}$$

where $a = \sqrt{\left(3-\sqrt{5}\right)/2}$ and θ is arbitrary, and the remaining measurement projectors are $\Pi_{0|1} = \Gamma_{0|1} = |+\rangle\langle +|$, and $\Pi_{1|1} = \Gamma_{1|1} = |-\rangle\langle -|$, with $|+\rangle = \frac{1}{\sqrt{1-a^2}}\left(\sqrt{1-2a^2}\,|0\rangle - e^{i\theta}a\,|1\rangle\right)$.

In view of this, one can conjecture that, if the maximal value of Hardy's probability $p(0,0|1,1)$ is observed, the state must somehow be a direct sum of copies of $|\phi\rangle$. This is indeed the case, as stated in the following theorem:

Theorem 7. *If* $p(0,0|1,1) = \left(5\sqrt{5}-11\right)/2$ *is observed in an ideal Hardy's test - i.e., together with* (7.11) *- , then the state of the system is equivalent, up to local isometries, to* $|\sigma\rangle_{AB} \otimes |\phi\rangle_{A'B'}$*, where* $|\phi\rangle$ *is given in* (7.27) *and* $|\sigma\rangle$ *is some bipartite state. In other words, the ideal Hardy's test constitutes a self-testing of* $|\phi\rangle$*.*

Proof. Without loss of generality, let $\Pi^i_{0|0} = |2i\rangle\langle 2i|$, $\Pi^i_{1|0} = |2i+1\rangle\langle 2i+1|$, $\Gamma^j_{0|0} = |2j\rangle\langle 2j|$, $\Gamma^j_{1|0} = |2j+1\rangle\langle 2j+1|$. Then,

$$p_{ij}(0,0|1,1) = \mathrm{Tr}\left(\rho_{ij}\Pi^i_{0|1}\otimes\Gamma^j_{0|1}\right) = \frac{5\sqrt{5}-11}{2} \tag{7.28}$$

if, and only if, $\rho_{ij} = |\phi_{ij}\rangle\langle\phi_{ij}|$, where

$$|\phi_{ij}\rangle = a\left(|2i,2j+1\rangle + |2i+1,2j\rangle\right) + e^{i\theta}\sqrt{1-2a^2}\,|2i+1,2j+1\rangle\,, \tag{7.29}$$

and $a = \sqrt{\left(3-\sqrt{5}\right)/2}$ and arbitrary θ. This way, a state $|\psi\rangle$ can lead to a maximal value of Hardy's probability if, and only if, it is given by

$$|\psi\rangle = \bigoplus_{i,j}\sqrt{q_{ij}}\,|\phi_{ij}\rangle\,. \tag{7.30}$$

The coefficients q_{ij} are arbitrary probabilities that, by definition, are of the form $q_{ij} = r_i s_j$, where $r_i, s_j \geq 0$, $\sum_i r_i = \sum_j s_j = 1$. The angle θ cannot depend on the indices i, j, because $\Pi^i_{0|1}$ is uniquely defined by θ, and, by definition, is independent of j; the same reasoning can be applied to $\Gamma^j_{0|1}$, uniquely defined by θ, and independent of i. Now, following the self-testing methods of [105], local ancilla qubits, prepared in the state $|00\rangle_{A'B'}$, are appended to the system, and are applied local isometries Φ_A and Φ_B, such that

$$(\Phi_A\otimes\Phi_B)\,|\psi\rangle_{AB}\,|00\rangle_{A'B'} = |\sigma\rangle_{AB}\,|\phi\rangle_{A'B'}\,, \tag{7.31}$$

where $|\sigma\rangle$ is a bipartite 'junk' state. This can indeed be achieved for $\Phi_A = \Phi_B = \Phi$, defined by the map

$$\Phi\,|2k,0\rangle_{CC'} \mapsto |2k,0\rangle_{CC'}\,, \tag{7.32a}$$

$$\Phi\,|2k+1,0\rangle_{CC'} \mapsto |2k,1\rangle_{CC'}\,, \tag{7.32b}$$

for both $C = A, B$. □

This is the first result of self-testing of non-maximally entangled states. More recently, Yang and Navascus have introduced new methods that implement self-testing of a wide class of bipartite pure states [106].

7.5 Hardy's test with realistic constraints

Suppose now that the constraint probabilities in Hardy's experiment are not exactly equal to zero. In this case, the local bound on Hardy's probability is no longer zero, either, and is given by inequality (7.18). Let, then, the constraint probabilities be

$$p(0,0|0,0) \leq \epsilon, \tag{7.33a}$$

$$p(0,1|1,0) \leq \epsilon, \tag{7.33b}$$

$$p(1,0|0,1) \leq \epsilon, \tag{7.33c}$$

for some $\epsilon \geq 0$. Notice that, if no-signaling holds, then $p(0,0|0,0) = \epsilon$ implies $p_A(0|0) \geq \epsilon$, and $p(1,0|0,1) = \epsilon$ implies $p_A(1|0) \geq \epsilon$. Therefore $\epsilon \leq \frac{1}{2}$. The region of interest is, in fact, $\epsilon \leq \frac{1}{3}$, because the local bound on Hardy's probability becomes

$$p(0,0|1,1) \leq 3\epsilon. \tag{7.34}$$

For $\epsilon \geq \frac{1}{3}$, the bound is trivial and quantum physics certainly cannot violate it; while for $0 \leq \epsilon < \frac{1}{3}$, quantum physics may lead to a violation of the local bound. As before, the goal is to assess the maximal quantum violation in a device-independent scenario, *i.e.*, without making any assumption on the Hilbert space dimension. The previously stated theorem cannot be extended, so a different approach is taken: first, semi-definite programs are applied to obtain an upper bound on Hardy's probability, using the NPA hierarchy; second, by optimizing over the states and measurements of two-qubit systems, it is possible to obtain a value that is certainly achievable with quantum systems, thus, a lower bound. If the values obtained coincide, it is possible to conclude that they are, indeed, the optimal value for Hardy's

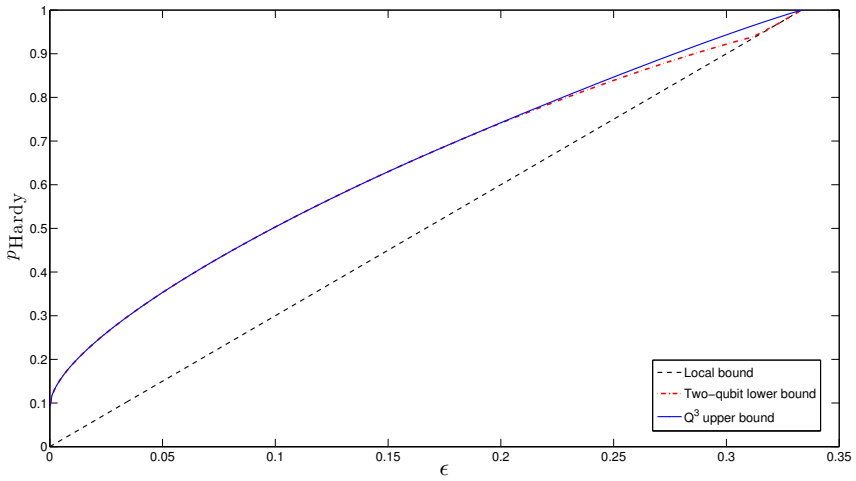


Figure 7.3: Upper and lower bounds on maximum Hardy's probability p_{Hardy} in terms of the bound ϵ on the constraint probabilities. The solid (blue) line is the upper bound, computed from the set $\mathcal{Q}_3$; the dotted (red) line is the lower bound, computed from two-qubit systems; the dashed (black) line is the local bound.

probability, and that this value can be achieved with two-qubit systems.

For several values of ϵ in the interval $0 \leq \epsilon \leq 1/3$, Hardy's probability is optimized over the set $\mathcal{Q}_3$, enforcing the constraints (7.33). The implementation was carried out in MATLAB using semi-definite programming [133, 134]. The results form the solid line in fig. 7.3. For the lower bound, the most general mixed states of two qubits and POVM elements acting on those were considered, and the maximal value of the Hardy's probability was estimated using constrained nonlinear optimization methods in MATLAB. These methods are not guaranteed to converge to global maxima, though, and are in fact rather sensitive to seed conditions; each point on the dotted line in fig. 7.3 is the maximum obtained over 10^4 runs, with random initial seeds.

The computed lower and upper bounds for Hardy's probability differ, at most, by values of order 10^{-2}; in the region $\epsilon \lesssim 0.2$ (where any experiment that aims at implementing Hardy's test will have to be), this difference is of order 10^{-6}. This proves that there is no advantage in using

higher-dimensional systems, as compared to two-qubit systems, even in the presence of imperfections.

8

Conclusions

One of the most intriguing facts in the field of foundations of quantum theory is the non-equivalence between entanglement and nonlocality. Although there are entangled states that can only lead to local correlations in standard Bell scenarios, there are more general scenarios where the "hidden" nonlocality of such states could be revealed. The first attempt to explore such scenarios considered local preprocessing of one or many copies of the state, an operation known as local filtering. This line of research has led to many interesting results, of which one of the most interesting states that every entangled state displays some hidden nonlocality that can be revealed if assisted by a suitable local state.

Along with the above scenario, this thesis presented a novel approach that shed new light on the complex relations between entanglement and nonlocality. By considering multipartite quantum networks composed of multiple copies of local quantum states, it is possible to show that nonlocal correlations can be retrieved, and, thus, that such states may be useful resources for applications of nonlocality.

Several examples of activation of nonlocality on quantum networks were presented. Among them, the proofs that every one-way entanglement distillable state, every "erased" state and that every state that is useful for teleportation are nonlocal resources. This last result implies the very interesting fact that every entangled isotropic state displays nonlocality in at least one scenario, thus proving a special equivalence between entanglement and nonlocality for this family of states. The main future directions in this line are to extend this special equivalence to all bipartite entangled

states, and, possibly, to all entangled states. A relation that remains unexplored is the one between the multipartite quantum network scenario and the filtering scenario previously presented.

Recently, a novel device-independent paradigm has been gaining strength within quantum information theory. The possibility of assessing quantum properties making very few assumptions on the systems and devices under consideration is noteworthy, and the possibilities opened by such approach are innumerous. On the applied side, device-independent protocols for quantum distribution of cryptographic keys and randomness expansion and amplification allow for the possibility of implementing such tasks securely and privately even under the most paranoic scenarios, for instance, those in which a malevolent party is the provider of the devices in use. On the fundamental side, different methods allow for device-independent assessment of the dimension of an unknown system, of how entangled it is, and if the entanglement is genuinely multipartite, or even allow for the assessment of the state of the systems, on self-testing protocols that, also, can be used to assess specific operations applied to the systems.

This thesis presented two novel results that contribute to the expanding field of device-independent assessment of properties. The first is a device-independent protocol for certification of entangling measurement devices, that is, measurement devices that are able to project the systems being measured onto entangled states. Such devices are crucial in many quantum information and computation tasks, including the seminal teleportation protocol. Thus, device-independent certification of the entangling character of a given device may be a very important issue for the implementation of quantum networks.

The protocol presented, although being an important proof of principle, is not robust, and the demanding conditions on which it is valid make an experimental implementation impossible, at this stage. However, it may be the first step for a robust, fully implementable protocol. Other possibilities that arise from it are extending the ideas to the multipartite domain. With the interesting structures presented by entanglement, in multipartite systems, it may be possible to certify, device-independently, not only that

the measurement devices are entangling but also the type of entanglement they present.

The second result gives novel device-independent bounds for the seminal Hardy's experiment, or Hardy's paradox. Hardy's experiment is the first bipartite example of a quantum nonlocality test that does not rely on inequalities, also known as an *all-versus-nothing* test. One of its curious properties is that it holds for all two-qubit states, except the maximally entangled one.

Since it was first introduced, many generalizations of Hardy's experiment followed, from higher-dimensional systems to multipartite ones, and several experiments have been performed. One question that remained unanswered is if higher-dimensional systems could lead to any advantage, either on ideal theoretical tests or on imperfect practical implementations. The bounds presented cover both situations, and it is proven that two-qubit systems are sufficient to reach maximal nonlocality in both cases. Another interesting result is that the ideal scenario where maximal nonlocality is observed is very special, and only a very specific class of states can achieve such correlations. This observation led to the first example of self-testing of non-maximally entangled states.

A

Proofs of some lemmas

Fine's lemma

The following lemma, due to Artur Fine [31], is formulated for Bell scenarios where two parties perform dichotomic measurements, but can be extended to more general scenarios.

Lemma (Fine [31])**.** *A probability distribution $p(a,b|x,y)$ is local if, and only if, there is a joint probability distribution $p(a,a',b,b')$ whose marginals are consistent with $p(a,b|x,y)$, where a and b denote the outcomes of measurements $x=0$ and $b=1$ and a' and b' denote the outcomes of measurements $x=1$ and $y=1$, respectively.*

Proof. Every local probability distribution can be written as

$$p(a,b|x,y)=\sum_{\lambda} q(\lambda)d_A(a|x,\lambda)d_B(b|y,\lambda), \tag{A.1}$$

where $d_A(a|x,\lambda)$ and $d_B(b|y,\lambda)$ are deterministic local probabilities. To prove that a joint probability distribution for all outcomes can be obtained from any local probability distribution, it suffices to define

$$p(a,a',b,b')=\sum_{\lambda} q(\lambda)d_A(a|0,\lambda)d_A(a'|1,\lambda)d_B(b|0,\lambda)d_B(b'|1,\lambda). \tag{A.2}$$

It follows, then, that the marginal distributions are equal to the initial

distribution,

$$p(a,b|x,y) = \sum_{a',b'} p(a,a',b,b'). \tag{A.3}$$

Now, to prove the converse, suppose there is a joint probability distribution $p(a,a',b,b')$. Let $\lambda_i = (a_i, a'_i, b_i, b'_i)$, and

$$p_A(a|0,\lambda_i) = \delta_{a,a_i}, \qquad p_A(a'|1,\lambda_i) = \delta_{a',a'_i}, \tag{A.4}$$

$$p_B(b|0,\lambda_i) = \delta_{b,b_i}, \qquad p_B(b'|1,\lambda_i) = \delta_{b',b'_i}. \tag{A.5}$$

If $q(\lambda_i) = p(a,a',b,b')$, then, the local probability distribution $p(a,b|x,y)$ can be retrieved by

$$p(a,b|x,y) \;\; = \;\; \sum_i q(\lambda_i) p_A(a|x,\lambda_i) p_B(b|y,\lambda_i). \tag{A.6}$$

□

Masanes' lemma

Also referred to as *Jordan's lemma* [111]. The statement and proof that follows is adapted from [76].

Lemma (Masanes [76])**.** *Let* $\Pi_{0|0}, \Pi_{1|0}, \Pi_{0|1}, \Pi_{1|1}$ *be four projectors acting on a Hilbert space* $\mathcal{H}$ *such that* $\Pi_{0|0} + \Pi_{1|0} = 1$ *and* $\Pi_{0|1} + \Pi_{1|1} = 1$*. There exists an orthonormal basis in* $\mathcal{H}$ *where the four projectors are simultaneously block diagonal, where the subspace* $\mathcal{H}_i$ *of* $\mathcal{H}$ *corresponding to block* i *is, at most, bidimensional,* $dim\,(\mathcal{H}_i) \leq 2 \forall i$*.*

Proof. Take the three positive operators $\Pi_{0|1}$, $\Gamma_{0|0} = \left(\Pi_{0|1}\Pi_{0|0}\Pi_{0|1}\right)$ and $\Gamma_{1|0}\left(\Pi_{0|1}\Pi_{1|0}\Pi_{0|1}\right)$. Their ranges are contained in the subspace where $\Pi_{0|1}$ acts like the identity, and $\Gamma_{0|0} + \Gamma_{1|0} = \Pi_{0|1}$. Thus, they can be simultaneously diagonalized. Let $|v\rangle$ be one of the simultaneous eigenvectors that satisfies $\Pi_{1|1}|v\rangle = \mathbf{0}$. Because $\Pi_{0|0} + \Pi_{1|0} = \mathbf{1}$, it cannot be that both $\Pi_{0|0}|v\rangle = \mathbf{0}$ and $\Pi_{1|0}|v\rangle = \mathbf{0}$ hold. Assume, first, that $\Pi_{0|0}|v\rangle = \mathbf{0}$. Then

$\Pi_{1|0}|v\rangle = |v\rangle$ and the span of $|v\rangle$, denoted $\mathcal{H}_v$, corresponds to a 1×1 diagonal block where $\Pi_{0|0}, \Pi_{1|0}, \Pi_{0|1}, \Pi_{1|1}$ have eigenvalues $0, 1, 1, 0$, respectively. The case $\Pi_{1|0}|v\rangle = \mathbf{0}$ is similar. Assume, then, that $\Pi_{0|0}|v\rangle \neq \mathbf{0}$ and $\Pi_{1|0}|v\rangle \neq \mathbf{0}$. Let $|\psi_{0|0}\rangle = \Pi_{0|0}|v\rangle$ and $|\psi_{1|0}\rangle = \Pi_{1|0}|v\rangle$ be orthogonal vectors in $\mathcal{H}_v$, defined now as $\mathcal{H}_v = \{\alpha_1|\psi_{0|0}\rangle + \alpha_2|\psi_{1|0}\rangle : \forall\, \alpha_1, \alpha_2 \in \mathbb{C}\}$. Clearly, $|v\rangle \in \mathcal{H}_v$, since $|v\rangle = |\psi_{0|0}\rangle + |\psi_{1|0}\rangle$. Because $\Pi_{0|1}|\psi_{0|0}\rangle \propto |v\rangle$ and $\Pi_{0|1}|\psi_{1|0}\rangle \propto |v\rangle$, there exists a $|w\rangle$ in $\mathcal{H}_v$ such that $\Pi_{0|1}|w\rangle = \mathbf{0}$ and $\Pi_{1|1}|w\rangle = |w\rangle$. So, $|\psi_{0|0}\rangle, |\psi_{1|0}\rangle \in \mathcal{H}_v$ are simultaneous eigenvectors of $\Pi_{0|0}, \Pi_{1|0}$, and $|v\rangle, |w\rangle \in \mathcal{H}_v$ are simultaneous eigenvectors of $\Pi_{0|1}, \Pi_{1|1}$. Therefore, the subspace $\mathcal{H}_v$ corresponds to a bidimensional subspace of $\mathcal{H}$ where $\Pi_{0|0}, \Pi_{1|0}, \Pi_{0|1}, \Pi_{1|1}$ are simultaneously block diagonal. The same construction can be made for all the simultaneous eigenvectors $|v\rangle$, and for the simultaneous eigenvectors of $\Pi_{1|1}$, $(\Pi_{1|1}\Pi_{0|0}\Pi_{1|1})$ and $(\Pi_{1|1}\Pi_{1|0}\Pi_{1|1})$. At the end, the Hilbert space $\mathcal{H}$ can be decomposed as a direct sum of subspaces $\mathcal{H}_i$ of dimension less or equal than 2 that contains two eigenvectors of each operator $\Pi_{0|0}, \Pi_{1|0}, \Pi_{0|1}, \Pi_{1|1}$. □

The following very useful corollaries follow directly from the lemma.

Corollary 1. *Let $O_A = \Pi_{0|0} - \Pi_{1|0}$ and $O_B = \Pi_{0|1} - \Pi_{1|1}$ be two observables acting on $\mathcal{H}$. Then, according to the lemma, there are subspaces $\mathcal{H}_i$ of $\mathcal{H}$ such that O_1 and O_2 are simultaneously block diagonalized, that is, the observables can be written as $O_1 = \bigoplus_i O_1^i$ and $O_2 = \bigoplus_i O_2^i$, where both O_1^i and O_2^i act on $\mathcal{H}_i$, for every i, and each block is of size 1×1 or 2×2.*

Corollary 2. *Let $\mathcal{B} = A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1)$ be a CHSH operator acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, where A_x and B_y are dichotomic observables. Then, there are subspaces $\mathcal{H}_{Ai}$ of $\mathcal{H}_A$ and $\mathcal{H}_{Bj}$ of $\mathcal{H}_B$ such that the CHSH operator can be written as $\mathcal{B} = \bigoplus_{i,j} \mathcal{B}_{ij}$, where $\mathcal{B}_{ij}$ is a CHSH operator acting on $\mathcal{H}_{Ai} \otimes \mathcal{H}_{Bj}$.*

Popescu-Rohrlich lemmas

Lemma (Popescu-Rohrlich 1 [9]). *For every entangled state $|\psi\rangle$ of an n-partite quantum system, associated with $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$, for any two parties there exists a projection onto a direct product state of the remaining $(n-2)$-parties such that the resulting bipartite state is entangled.*

Proof. Let $\{|\xi_{k_i}\rangle\}$ be an arbitrary orthonormal basis of $\mathcal{H}_i$, for all i. Suppose that the false conclusion of the lemma holds, that the projection onto all elements of $(n-2)$ of these bases result on a product state of the remaining 2 parties. Let

$$|\phi_1\rangle\,|\phi_2\rangle = [\langle\xi_{k_3}|\ldots\langle\xi_{k_n}|]\,|\psi\rangle\,. \tag{A.7}$$

The states $|\phi_1\rangle$ and $|\phi_2\rangle$ can be functions of the elements of the bases, that is $|\phi_1\rangle = |\phi_1\,(k_3,\ldots,k_n)\rangle$, $|\phi_2\rangle = |\phi_2\,(k_3,\ldots,k_n)\rangle$. However, in order for the resulting state to remain separable when projection onto different elements of the $(n-2)$ bases are taken, it is necessary that the states $|\phi_1\rangle$ and $|\phi_2\rangle$ are functions of disjoint sets of indices, as, for instance, $|\phi_1\rangle = |\phi_1\,(k_3,\ldots,k_l)\rangle$, $|\phi_2\rangle = |\phi_2\,(k_{l+1},\ldots,k_n)\rangle$, for some l. Otherwise, by taking a projection onto a superposition of two or more elements of a basis, one could end up with an entangled state on the remaining parties. It follows that the state ψ can be written as

$$|\psi\rangle = \sum_{k_3,\ldots,k_l} |\phi_1\,(k_3\ldots k_l)\rangle\,|e_{k_3}\ldots e_{k_l}\rangle \otimes \sum_{k_{l+1},\ldots,k_n} |\phi_2\,(k_{l+1}\ldots k_n)\rangle\,\left|e_{k_{l+1}}\ldots e_{k_n}\right\rangle \tag{A.8}$$

Repeating the argument for all pairs of parties, one ends up with similar representations over all possible bipartitions of the Hilbert space. It follows that the state $|\psi\rangle$ has, necessarily, to be fully separable, $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, which contradicts the assumption of the lemma. □

Lemma (Popescu-Rohrlich 2 [9]). *Consider an n-partite Bell scenario. If the joint probability distribution admits a local model, then the probability*

distribution of the outcomes of k parties, conditioned on the outcomes of the remaining (n − k) parties, admits a local model.

Proof. This proof is valid for a 3-partite scenario, but can be easily extended to scenarios with more parties. Let the probability distribution of the outcomes be local, written as

$$p(a,b,c|x,y,z) = \int_\Lambda p_A(a|x,\lambda)p_B(b|y,\lambda)p_C(c|z,\lambda)q(\lambda)\mathrm{d}\lambda. \quad \text{(A.9)}$$

Now consider the probability distribution of the outcomes of parties A and B, conditioned on a particular outcome c of measurement z,

$$p(a,b|c,x,y,z) = \frac{p(a,b,c|x,y,z)}{p(c|z)}, \quad \text{(A.10)}$$

where $p_C(c|z) = \sum_{a,b} p(a,b,c|x,y,z)$. Since the probability distribution $p(a,b,c|x,y,z)$ is local, one has

$$p(a,b|c,x,y,z) = \frac{\int_\Lambda p_A(a|x,\lambda)p_B(b|y,\lambda)p_C(c|x,\lambda)q(\lambda)\mathrm{d}\lambda}{p_C(c|z)} \quad \text{(A.11)}$$

$$= \int_\Lambda p_A(a|x,\lambda)p_B(b|y,\lambda)q'(\lambda)\mathrm{d}\lambda \quad \text{(A.12)}$$

where $q'(\lambda) = q(\lambda)p_C(c|z,\lambda)/p_C(c|z)$; that is, the probability distribution $p(a,b|c,x,y,z)$ is necessarily local. Thus, if $p(a,b|c,x,y,z)$ is nonlocal, then $p(a,b,c|x,y,z)$ must be nonlocal as well. □

Maximum violation of the CHSH inequality of a given two-qubit state

Lemma (Horodecki *et al.*, [57])**.** *Given a two-qubit state ρ, the maximum CHSH value achievable in a Bell test where projective measurements are performed on such state is given by*

$$S = 2\sqrt{u_0 + u_1}, \quad \text{(A.13)}$$

where u_0 and u_1 are the largest eigenvalues of the matrix $U = T^T T$, and the matrix T is defined as $T_{mn} = \mathrm{Tr}\left(\rho\left(\sigma_m \otimes \sigma_n\right)\right)$, where σ_i are the Pauli matrices.

Proof. Every two-qubit state, acting on $\mathcal{H}^2 \otimes \mathcal{H}^2$ can be written as

$$\rho = \frac{1}{4}\left(\mathbf{1}\otimes\mathbf{1} + \vec{r}\cdot\vec{\sigma}\otimes\mathbf{1} + \mathbf{1}\otimes\vec{s}\cdot\vec{\sigma} + \sum_{m,n=1}^{3} T_{mn}\sigma_m\otimes\sigma_n\right), \quad \text{(A.14)}$$

where $\vec{r}, \vec{s} \in \mathbb{R}^3$, such that $|\vec{r}| \leq 1$, $|\vec{s}| \leq 1$, and $T_{mn} = \mathrm{Tr}\left(\rho\left(\sigma_m \otimes \sigma_n\right)\right)$. Let $A_x = \vec{a}_x.\vec{\sigma}$ and $B_y = \vec{b}_y \cdot \vec{\sigma}$ be the observables of Alice and Bob, respectively. The mean value of the CHSH operator, on the state ρ, is

$$S_\rho = \vec{a}_0.\left(T\left(\vec{b}_0 + \vec{b}_1\right)\right) + \vec{a_1}\cdot\left(T\left(\vec{b}_0 - \vec{b}_1\right)\right). \quad \text{(A.15)}$$

The vectors $\vec{b}_0$ and $\vec{b}_1$ can be decomposed on an orthogonal basis $\{\vec{c}_0, \vec{c}_1\}$,

$$\vec{b}_0 + \vec{b}_1 = 2\cos\left(\theta\right)\vec{c}_0, \quad \vec{b}_0 - \vec{b}_1 = 2\sin\left(\theta\right)\vec{c}_1, \quad \text{(A.16)}$$

where $\theta \in [0, \pi/2]$. So, S_ρ is maximized over θ and vectors $\vec{a}_0, \vec{a}_1, \vec{c}_0, \vec{c}_1$:

$$\begin{aligned} \max S_\rho &= \max_{(\theta,\vec{a}_0,\vec{a}_1,\vec{c}_0,\vec{c}_1)} 2\left[\vec{a}_0\cdot(T\vec{c}_0)\cos\left(\theta\right) + \vec{a}_1\cdot(T\vec{c}_1)\sin\left(\theta\right)\right] \\ &= \max_{(\theta,\vec{c}_0,\vec{c}_1)} 2\left[|T\vec{c}_0|\cos\left(\theta\right) + |T\vec{c}_1|\sin\left(\theta\right)\right] \\ &= \max_{(\vec{c}_0,\vec{c}_1)} 2\sqrt{|T\vec{c}_0|^2 + |T\vec{c}_1|^2}. \end{aligned} \quad \text{(A.17)}$$

Define the matrix $U = T^T T$, and let u_0 and u_1 be its largest eigenvalues. The evaluation of the last maximum results in

$$\max S_\rho = 2\sqrt{u_0 + u_1}. \quad \text{(A.18)}$$

□

Pure states, written in their Schmidt decomposition $|\psi\rangle = \cos\left(\varphi\right)|00\rangle +$

$\sin(\varphi)|11\rangle$ can lead to a maximum violation of

$$\max S_{|\psi\rangle} = 2\sqrt{1+\sin^2(2\varphi)}. \tag{A.19}$$

Maximum mean value of a given CHSH operator over separable states

Lemma (Rabelo *et al.*, [20]). *For given local observables A_0, A_1, B_0 and B_1, the maximum CHSH value achievable on a quantum Bell test with separable states is*

$$S_{Sep} = \frac{\lambda+\sqrt{8-\lambda^2}}{2}, \tag{A.20}$$

where λ is the smallest eigenvalue of $\mathcal{B}$ such that $\lambda > 2$.

Proof. To evaluate $S_{Sep} = \max_{\rho\in\mathcal{S}} \mathrm{Tr}(\rho\mathcal{B})$, where $\mathcal{S}$ is the set of separable states, first note that, since the trace is linear and $\mathcal{S}$ is a convex set, it suffices to consider the set of pure product states $\mathcal{P}$. Now, using the second corollary of Masanes' lemma, it follows that

$$\begin{aligned} S_{Sep} &= \max_{\{|\phi\rangle\in\mathcal{P}\}} \langle\phi|\mathcal{B}|\phi\rangle \\ &= \max_{\{|\phi\rangle\in\mathcal{P}\}} \langle\phi| \oplus_{i,j} \mathcal{B}_{i,j} |\phi\rangle \\ &= \max_{\{|\phi_{i,j}\rangle\in\mathcal{P}\}} \sum_{i,j} p_{i,j} \langle\phi_{i,j}|\mathcal{B}_{i,j}|\phi_{i,j}\rangle, \end{aligned} \tag{A.21}$$

where $|\phi_{i,j}\rangle = (\Pi_i\otimes\Pi_j)|\phi\rangle/\sqrt{p_{i,j}}$ and $p_{i,j} = \langle\phi|(\Pi_i\otimes\Pi_j)|\phi\rangle$. By convexity, the above expression is upper bounded by the largest mean value among the two-qubit Bell operators $\mathcal{B}_{i,j}$ attained by two-qubit pure product states:

$$\begin{aligned} S_{Sep} &= \max_{\{|\phi_{i,j}\rangle\in\mathcal{P}\}} \sum_{i,j} p_{i,j} \langle\phi_{i,j}|\mathcal{B}_{i,j}|\phi_{i,j}\rangle \\ &\leq \sum_{i,j} p_{i,j} \max_{\{|\phi_{i,j}\rangle\in\mathcal{P}\}} \langle\phi_{i,j}|\mathcal{B}_{i,j}|\phi_{i,j}\rangle \\ &\leq \max_{\{|\phi\rangle\in\mathcal{P},(i,j)\}} \langle\phi|\mathcal{B}_{i,j}|\phi\rangle. \end{aligned} \tag{A.22}$$

According to [111], the spectral decomposition of any two-qubit CHSH operator is, up to local unitaries, $\mathcal{B} = \sum_{i=1}^{4} \alpha_i |\psi_i\rangle \langle\psi_i|$, where the eigenvectors $|\psi_i\rangle$ are Bell states and the eigenvalues are functions of the local observables, with $\alpha_1 = -\alpha_3$, $\alpha_2 = -\alpha_4$, $\alpha_1^2 + \alpha_2^2 = 8$. Let $\alpha_{i,j}$ be the largest eigenvalue of $\mathcal{B}_{i,j}$. Thus,

$$\begin{aligned} S_{Sep} &= \max_{\{|\phi\rangle \in \mathcal{P},(i,j)\}} \langle\phi| \mathcal{B}_{i,j} |\phi\rangle \\ &= \max_{\{|\phi\rangle \in \mathcal{P},(i,j)\}} \alpha_{i,j}[|\langle\phi \mid \psi_1\rangle|^2 - |\langle\phi \mid \psi_3\rangle|^2] \\ &+ \sqrt{8 - \alpha_{i,j}^2}[|\langle\phi \mid \psi_2\rangle|^2 - |\langle\phi \mid \psi_4\rangle|^2]. \end{aligned} \tag{A.23}$$

Without loss of generality, the local unitaries in the spectral decomposition of $\mathcal{B}$ are disconsidered, since they can be absorbed into the states $|\phi\rangle$. The largest overlap between a pure product state and a Bell state is $1/2$; thus, $S_{Sep} = \max_{\{(i,j)\}}(\alpha_{i,j} + \sqrt{8 - \alpha_{i,j}^2})/2$.

Note that $\alpha_{i,j} \geq 2$ for all (i,j). This is because the largest eigenvalue α of $\mathcal{B}$ is given by the positive square root of the largest eigenvalue of $\mathcal{B}^2$, which is lower bounded by 2 [40]. Observe that the above function decreases as α increases. This way, the maximum is attained for the subspace (i,j) such that $\alpha_{i,j}$ is minimum. Then, defining λ as the smallest eigenvalue of $\mathcal{B}$ such that $\lambda \geq 2$, it follows that

$$S_{Sep} = \frac{\lambda + \sqrt{8 - \lambda^2}}{2}. \tag{A.24}$$

This generalizes to all dimensions the results of [135]. □

Bibliography

[1] A. Einstein, B. Podolski, N. Rosen, Phys. Rev. **4**7, 777 (1935).

[2] D. Bohm, Phys. Rev. **85**, 166 (1952).

[3] J. Math. Mech. **17**, 59 (1967).

[4] J. S. Bell, Physics **1**, 195 (1964).

[5] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[6] E. Schrdinger; *Naturwissenschaften* **23**, 807 (1935).

[7] R. F. Werner, Phys. Rev. A **4**0, 4277 (1989).

[8] N. Gisin, Phys. Lett. A, **1**54, 201 (1991).

[9] S. Popescu, D. Rohrlich, Phys. Lett. A **166**, 293 (1992).

[10] S. Popescu, Phys. Rev. Lett. **7**4, 2619 (1995).

[11] A. Peres, Phys. Rev. A **54**, 2685 (1996).

[12] D. Cavalcanti, M. L. Almeida, V. Scarani, A. Acín, Nat. Comm. **2**, 184 (2011).

[13] C. H. Bennett, G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, 175 (1984).

[14] C. H. Bennett, G. Brassard, C. Crápeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. **7**0, 1895 (1993).

[15] A. K. Ekert, Phys. Rev. Lett. **6**7, 661 (1991).

[16] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. **9**8, 230501 (2007).

[17] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, Nature **464**, 1021 (2010).

[18] R. Gallego, N. Brunner, C. Hadley, A. Acín Phys. Rev. Lett. **105**, 230501 (2010).

[19] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, V. Scarani, Phys. Rev. Lett. **1**07 050502 (2011).

[20] R. Rabelo, Y. Z. Law, V. Scarani, Phys. Rev. Lett. **1**09 180401 (2012).

[21] R. Rabelo, "Não localidade quântica: matemática e fundamentos", MSc. dissertation, Universidade Federal de Minas Gerais (2010).

[22] A. Peres, "Quantum theory: concepts and methods", Kluwer Academic Publishers (1995).

[23] R. P. Feynman, R. B. Leighton, M. Sands, "The Feynman lectures on Physics, vol.3", Addison-Wesley publishing company, (1965).

[24] C. Cohen-Tannoudji, B. Diu, F. Lale, "Quantum mechanics", Wiley-Interscience, (2006).

[25] J. von Neumann, "Mathematical foundations of quantum mechanics", Princeton University Press (1955).

[26] M. A. Nielsen, I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge Univ. Press (2000).

[27] S. Pironio, "Aspects of quantum nonlocality", PhD. thesis, Universit Libre de Bruxelles (2004).

[28] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, arXiv:1303.2849 [quant-ph].

[29] J. F. Clauser, M. Horne, Phys. Rev. D **10**, 526 (1974).

[30] http://www.zib.de/Optimization/Software/Porta.

[31] A. Fine, Phys. Rev. Lett. **4**8, 291 (1982).

[32] C. Sliwa, Phys. Lett. A **3**17, 165 (2003).

[33] D. Collins, N. Gisin, J. Phys. A: Math. Gen. **35**, 1775 (2004).

[34] M. Froissard, "Nuovo Cimento B" **64**, 241 (1981).

[35] S. Pironio, J.-D. Bancal, V. Scarani, J. Phys. A: Math. Theor. **4**4, 065303 (2011).

[36] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu, Phys. Rev. Lett. **8**8, 040404 (2002).

[37] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, Phys. Rev. A **7**1, 022101 (2005).

[38] S. Popescu, D. Rohrlich, Found. Phys. **24**, 379, (1994).

[39] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).

[40] L. J. Landau, Phys. Lett. A, **120**, 54 (1987).

[41] J.-A. Larsson, J. Semitecolos, Phys. Rev. A **63**, 022117 (2001).

[42] D. Cavalcanti, N. Brunner, P. Skrzypczyk, A. Salles, V. Scarani, Phys. Rev. A **84**, 022105 (2011).

[43] M. Araújo, M. T. Quintino, D. Cavalcanti, M. França Santos, A. Cabello, M. Terra Cunha, Phys. Rev. A **86**, 030101(R) (2012).

[44] M. T. Quintino, M. Araújo, D. Cavalcanti, M. França Santos, M. Terra Cunha, J. Phys. A: Math. Theor. **45**, 215308 (2012).

[45] N. Sangouard, J. D. Bancal, N. Gisin, W. Rosenfeld, P. Sekatski, M. Weber, H. Weinfurter, Phys. Rev. A **84**, 052122 (2011).

[46] C. Teo, M. Araújo, M. T. Quintino, J. Minár, D. Cavalcanti, V. Scarani, M. Terra Cunha, M. França Santos, Nat. Commun. **4**, 2104 (2013)

[47] S. J. Freedman, J. F. Clauser, Phys. Rev. Lett. **2**8, 938 (1972).

[48] A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. **4**9, 1804 (1982).

[49] Z. Y. Ou, L. Mandel, Phys. Rev. Lett. **6**1, 50 (1988).

[50] Y. H. Shih, C. O. Alley, Phys. Rev. Lett. **6**1, 2921 (1988).

[51] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **8**1, 5039 (1998).

[52] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, D. J. Wineland, Nature **4**09, 791 (2001).

[53] B. G. Christensen, K. T. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, P. G. Kwiat, arXiv:1306.5772 [quant-ph].

[54] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, A. Zeilinger, arXiv:1212.0533 [quant-ph].

[55] D. Cavalcanti, R. Rabelo, V. Scarani, Phys. Rev. Lett. **1**08 040402 (2012).

[56] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Rev. Mod. Phys. **8**1, 865 (2009).

[57] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A **2**23, 1 (1996).

[58] B. M. Terhal, Phys. Lett. A **2**71, 319 (2000).

[59] P. Hyllus, O. Ghüne, D. Bruss, M. Lewenstein, Phys. Rev. A **7**2, 012321 (2005).

[60] A. Peres, Phys. Rev. Lett. **7**6, 1413 (1996).

[61] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989).

[62] A. C. Doherty, P. A. Parrilo, F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).

[63] G. Vidal, J. Mod. Opt. **47**, 335 (2000).

[64] V. Vedral, M.B. Plenio, M.A. Rippin, P. L. Knight, Phys. Rev. Lett. **7**8, 2275 (1997).

[65] M.Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. A **60**, 1888 (1999).

[66] P. M. Hayden, M. Horodecki, B. M. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001).

[67] V. Vedral, M. B. Plenio, Phys. Rev. A **57**, 1619 (1998)

[68] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **8**0, 5239 (1998).

[69] S. Popescu, D. Rohrlich, Phys. Lett. A **169**, 411 (1992)

[70] T. Vertesi, Phys. Rev. A **78**, 032112 (2008).

[71] J. Barrett, Phys. Rev. A, **6**5, 042302 (2002).

[72] M. L. Almeida, S. Pironio, J. Barrett, G. Tóth, A. Acín, Phys. Rev. Lett. **99**, 040403 (2007).

[73] B. M. Terhal, A. C. Doherty, D. Schwab, Phys. Rev. Lett **90**, 157903 (2003).

[74] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).

[75] M. Żukowski, R. Horodecki, M. Horodecki, P. Horodecki, Phys. Rev. A **58**, 1694 (1998).

[76] L. Masanes, Phys. Rev. Lett. **97**, 050503 (2006).

[77] L. Masanes, Y.-C. Liang, A. C. Doherty, Phys. Rev. Lett. **100**, 090403 (2008)

[78] Y.-C. Liang, L. Masanes, D. Rosset, Phys. Rev. A **86**, 052115 (2012).

[79] D. Cavalcanti, N. Brunner, A. Acín, T. Vertési, Phys. Rev. A **87**, 042104 (2013).

[80] I. Devetak, A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[81] M. Junge, C. Palazuelos, D. Pérez-Garcá, I. Villanueva, M. M. Wolf, Phys. Rev. Lett. 104, 170405 (2010).

[82] M. Junge, C. Palazuelos, Comm. Math. Phys. **306** (3), 695-746 (2011).

[83] C. Palazuelos, Phys. Rev. Lett. **109**, 190401 (2012).

[84] K. Zyczkowski, I. Bengtsson, "Geometry of Quantum States", Cambridge (2006).

[85] J. Barrett, L. Hardy, A. Kent, Phys. Rev. Let., **95**, 010503 (2005).

[86] A. Acín, N. Gisin, L. Masanes, Phys. Rev. Lett. **9**7, 120405 (2006).

[87] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, A. Ací, Phys. Rev. A **74**, 042339 (2006).

[88] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scarani, New J. Phys. **11**, 045021 (2009).

[89] L. Masanes, Phys. Rev. Lett. **1**02, 140501 (2009).

[90] E. Hänggi, R. Renner, S. Wolf, in Advances in Cryptology, EUROCRYPT 2010, edited by H. Gilbert (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010), 216.

[91] L. Masanes, S. Pironio, A. Acín, Nat. Commun. **2**, 238 (2011).

[92] R. Colbeck, A. Kent, J. Phys. A: Math. Theor. **44**, 095305 (2011).

[93] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, A. Acín, arXiv:1210.6514 [quant-ph].

[94] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).

[95] K. F. Pál, T. Vértesi, Phys. Rev. A **77**, 042105 (2008).

[96] T. Vértesi, K. F. Pál, Phys. Rev. A **79**, 042106 (2009).

[97] M. Hendrych, R. Gallego, M. Miuda, N. Brunner, A. Acín, J. P. Torres, Nat. Phys. **8**, 588 (2012).

[98] N. Brunner, M. Navascués, T. Vértesi, Phys. Rev. Lett. **110**, 150501 (2013).

[99] G. M. D'Ariano, M. G. A. Paris, M. F. Sacchi, Advances in Imaging and Electron Physics **128**, 205 (2003).

[100] C. E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, V. Scarani, Phys. Rev. A **80**, 062327 (2009).

[101] J.-D. Bancal, N. Gisin, Y.-C. Liang, S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).

[102] D. Mayers, A. Yao, FOCS 98 Proceedings of the Symposium on Foundations of Computer Science, 503 (1998).

[103] D. Mayers, A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[104] F. Magniez, D. Mayers, M. Mosca, H. Ollivier, in: Proceedings of ICALP2006, Part I, M. Bugliesi et al. (Eds.), Lecture Notes in Computer Science **4051**, 72, 2006.

[105] M. McKague, T. H. Yang, V. Scarani, J. Phys. A: Math. Theor. **4**5 455304 (2012).

[106] T. H. Yang, M. Navascués, Phys. Rev. A **8**7, 050102(R) (2013).

[107] M. Navascués, S. Pironio, A. Acín, New Journal of Physics **10**, 073013 (2008).

[108] A. Doherty, Y.-C. Liang, B. Toner, S. Wehner, Proceedings of the 23rd Annual IEEE Conference on Computational Complexity, 199 (2008).

[109] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[110] R. Horodecki, P. Horodecki, M. Horodecki, Phys. Lett. A **2**00, 340 (1995).

[111] V. Scarani, N. Gisin, J. Phys. A: Math. Gen. **34**, 6043 (2001).

[112] S. L. Braunstein, A. Mann, M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

[113] V. Coffman, J. Kundu, W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[114] L. Hardy, Phys. Rev. Lett. **68**, 2981 (1992).

[115] L. Hardy, Phys. Rev. Lett. **71**, 1665 (1993).

[116] D. Greenberger, M. Horne, A. Shimony, A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[117] C. Pagonis, R. Clifton, Phys. Lett. A **168**, 100 (1992).

[118] G. Kar, Phys. Rev. A, **56**, 1023 (1997).

[119] J. Cereceda, Phys. Lett. A **327**, 433 (2004).

[120] D. Boschi, S. Branca, F. De Martini, L. Hardy, Phys. Rev. Lett. **79**, 2755 (1997).

[121] Y.-C. Liang, R. W. Spekkens, H. M. Wiseman, Physics Reports **506**, 1 (2011).

[122] R. Clifton, P. Neiman, Phys. Lett. A **166**, 177 (1992).

[123] S. Kunkri, S. K. Choudhary, Phys. Rev. A **72**, 022348 (2005).

[124] K. Seshdreesan, S. Ghosh, J. Phys. A: Math. Theor. **44** 315305 (2011).

[125] M. Hillery, B. Yurke, D. Stoler, Phys. Rev. A **63**, 062111 (2001).

[126] J. R. Torgerson, D. Branning, C. Monken, L. Mandel, Phys. Lett. A **204**, 323 (1995).

[127] G. Di Giuseppe, F. De Martini, D. Boschi, Phys. Rev. A **56**, 176 (1997).

[128] W. T. M. Irvine, J. F. Hodelin, C. Simon, D. Bouwmeester, Phys. Rev. Lett. **95**, 030401 (2005).

[129] A. Fedrizzi, M. P. Almeida, M. A. Broome, A. G. White, M. Barbieri, Phys. Rev. Lett. **106**, 200402 (2011).

[130] G. Valone, I. Gianani, E. B. Inostroza, C. Saavedra, G. Lima, A. Cabello, P. Mataloni, Phys. Rev. A **83**, 042105 (2011).

[131] D. Braun, M.-S. Choi, Phys. Rev. A **78**, 032114 (2008).

[132] S. Goldstein, Phys. Rev. Lett. **72**, 1951 (1994).

[133] J. F. Sturm, Opt. Meth. Soft. 625 (1999).

[134] J. Löfberg, *YALMIP: A Toolbox for Modeling and Optimization in MATLAB*, In Proceedings of the CACSD Conference, Taipei, Taiwan, (2004).

[135] M. Seevinck, J. Uffink, Phys. Rev. A **76**, 042105 (2007).