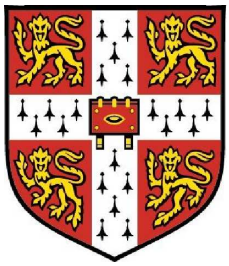
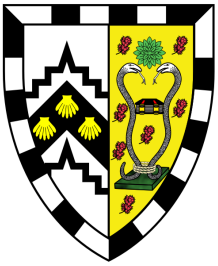
Quantum Information, Bell Inequalities and the No-Signalling Principle

Damián Pitalúa-García

Gonville and Caius College

University of Cambridge

A thesis submitted for the degree of

Doctor of Philosophy

September 2013

Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except where specifically indicated in the text.

The main results presented in chapter 2 were obtained in collaboration with my PhD supervisor, Adrian Kent.

A mis padres, a mi hermana, y a mis abuelos.

Acknowledgements

I am extremely grateful to Adrian Kent for supervising my PhD. His creative, rigorous and passionate approach to physics has influenced my attitude towards research. He always encouraged me to think freely and to pursue my own ideas, and offered me advice and support. I also thank Adrian for inviting me to collaborate in the interesting research project whose results correspond to chapter 2 of this thesis. I enjoyed very much our collaborative work and many interesting and very helpful conversations we had about quantum physics and my research.

I would like to thank all the members of the Centre for Quantum Information and Foundations in the Department of Applied Mathematics and Theoretical Physics for their support during my PhD. I am particularly grateful to Tony Short, Boris Groisman and Nilanjana Datta for several very helpful discussions about my research. I am also grateful to Sabri Al-Safi, Sergii Strelchuk and Min-Hsiu Hsieh for helpful conversations.

I would also like to thank Boris Bukh for helpful discussions, my College tutor Jonathan Evans for his support, and my examiners Boris Groisman and Jonathan Barrett for their careful reading of this thesis and helpful feedback.

I thank all my friends in Cambridge for very enjoyable times, and my friends in Mexico and my family for their encouragement.

I am very grateful to CONACYT México for sponsoring my PhD, to Gobierno de Veracruz for partial support, and to Gonville and Caius College for travel grants.

Abstract

This PhD thesis contains a general introduction and three main chapters. Chapter 2 investigates Bell inequalities that generalize the CHSH and Braunstein-Caves inequalities. Chapter 3 shows a derivation of an upper bound on the success probability of a class of quantum teleportation protocols, denoted as port-based teleportation, from the no-cloning theorem and the no-signalling principle. Chapter 4 introduces the principle of quantum information causality.

Chapter 2 considers the predictions of quantum theory and local hidden variable theories (LHVT) for the correlations obtained by measuring a pair of qubits by projections defined by randomly chosen axes separated by a given angle θ. The predictions of LHVT correspond to binary colourings of the Bloch sphere with antipodal points oppositely coloured. We show a Bell inequality for all θ, which generalizes the CHSH and the Braunstein-Caves inequalities in the sense that the measurement choices are not restricted to be in a finite set, but are constrained only by the angle θ. We motivate and explore the hypothesis that for a continuous range of $\theta > 0$, the maximum correlation (anticorrelation) is obtained by assigning to one qubit the colouring with one hemisphere black and the other white, and assigning the same (reverse) colouring to the other qubit. We describe numerical tests that are consistent with this hypothesis and bound the range of θ.

Chapter 3 shows a derivation of an upper bound on the success probability of port-based teleportation from the no-cloning theorem and the no-signalling principle.

Chapter 4 introduces the principle of quantum information causality, a quantum version of the information causality principle. The quantum information causality principle states the maximum amount of quantum information that a transmitted quantum system can communicate as a function of its dimension, independently of any quantum physical resources previously shared by the communicating parties. These principles reduce to the no-signalling principle if no systems are transmitted. We present a new quantum information task, the quantum information causality game, whose success probability is upper bounded by the new principle, and show that an optimal strategy to perform it combines the quantum teleportation and superdense coding protocols with a task that has classical inputs.

Contents

List of Figures **xv**

1 Introduction **1**

1.1 History of Quantum Information 1

1.2 Quantum Information 5

1.2.1 Quantum Operations 5

1.2.2 The Qubit 8

1.2.3 Entropy 10

1.2.3.1 Classical Entropy 10

1.2.3.2 Quantum Entropy 12

1.2.4 Fundamental Principles 14

1.2.4.1 The No-Cloning Theorem 15

1.2.4.2 The No-Signalling Principle 16

1.2.5 Fundamental Protocols 16

1.2.5.1 Superdense Coding 16

1.2.5.2 Quantum Teleportation 18

1.3 Bell Inequalities and the No-Signalling Principle 21

1.3.1 Bell Inequalities 23

1.3.1.1 The EPR Argument 23

1.3.1.2 Bell's Theorem 25

1.3.1.3 The CHSH Inequality 26

1.3.1.4 The Braunstein-Caves Inequality 28

1.3.1.5 Bell Experiments and Loopholes 30

1.3.2 The No-Signalling Principle 33

1.3.2.1 No-Signalling and the CHSH Inequality 38
1.3.2.2 No-Signalling and Quantum Information 41

2 Bloch Sphere Colourings and Bell Inequalities 45
2.1 Introduction 45
2.2 Bloch Sphere Colourings and Correlation Functions 47
2.3 The Hemispherical Colouring Maximality Hypothesis 52
2.4 Numerical Results 60
2.5 Related Questions for Exploration 64
2.6 Discussion 67

3 Bound on the Success Probability of Port-Based Teleportation from No-Cloning and No-Signalling 77
3.1 Introduction 77
3.1.1 Port-Based Teleportation 78
3.2 The Bound 79
3.3 Summary of the Proof 80
3.4 A More General No-Cloning Theorem 84
3.5 Conditions on the Port States 90
3.6 Implications from Superdense Coding 92
3.7 Discussion 95

4 Quantum Information Causality 99
4.1 Introduction 99
4.1.1 The Holevo Bound 100
4.1.2 Information Causality 101
4.2 Quantum Information Causality 107
4.2.1 Achievability of the Bound 109
4.2.2 The Case of Information Causality 111
4.3 The Quantum Information Causality Game 111
4.4 Upper Bound on the Success Probability in the QIC Game 115
4.4.1 Equivalence of the Two Versions of the Game 117
4.4.2 Reduction to a Covariant Strategy 120
4.4.3 A Useful Bound 122

4.5 Strategies in the QIC Game 123
4.5.1 Teleportation Strategies 124
4.5.2 An Optimal Strategy 128
4.5.3 Nonlocal Strategies 131
4.6 Discussion 132

5 Conclusions **135**

A Details of Numerical Work **139**

B Code for the Computer Program **147**

C Details of the Primed PBT Protocol **155**

D Bound for Nonlocal Strategies in the IC-2 Game **159**

References **165**

List of Figures

1.1 Spacetime diagram showing space-like and time-like separations . 22
1.2 Spacetime diagram of the EPR-Bohm experiment 24
1.3 Spacetime diagram showing that superluminal signalling leads to violation of relativistic causality 34
1.4 Schematic of an instantaneous nonlocal quantum computation . . 43

2.1 Alice's and Bob's measurement axes separated by an angle θ . . . 49
2.2 Diagram of the measurements performed by Alice and Bob that are used in the proof of Lemma 2.2 54
2.3 Diagram of the measurements performed by Alice and Bob that are used in the proof of Theorem 2.1 56
2.4 Some antipodal colouring functions on the sphere 61
2.5 Plots of the correlations for the antipodal colouring functions shown schematically in Figure 2.4, the singlet state quantum correlation, and the bounds given by Theorem 2.1 62
2.6 Plots of correlations for colouring 3_δ 63
2.7 Plots of correlations for colouring 2_Δ 63
2.8 Colourings A_ν 70
2.9 Colourings D_ν 71
2.10 Set of measurements on the sphere 74

3.1 Probabilistic port-based teleportation 82
3.2 A superdense coding protocol without communication 93

4.1 The information causality game 102

4.2 Setting for quantum information causality 108
4.3 Version I of the QIC game 113
4.4 The IC-2 game 125
4.5 Teleportation strategies in the QIC game 126
4.6 Plots of the success probabilities in the QIC game for $m = 1$ achieved with different strategies and the upper bound obtained from quantum information causality 127
4.7 Superdense coding strategies in the IC-2 game 130

B.1 Code for the computer program that defines the integral function and the correlation function $C_2(\theta)$ 148
B.2 Code for the computer program that defines the correlation function $C_3(\theta)$ 149
B.3 Code for the computer program that defines the correlation function $C_4(\theta)$ 150
B.4 Code for the computer program that defines the correlation function $C_{2_\Delta}(\theta)$ 151
B.5 Code for the computer program that defines the correlation function $C_{3_\delta}(\theta)$ 152
B.6 Code for the computer program that outputs the values for the correlation functions plotted in Figures 2.5, 2.6 and 2.7 153

Chapter 1

Introduction

> *"I think I can safely say that nobody understands quantum mechanics."* – Richard Feynman

1.1 History of Quantum Information

Quantum physics originated at the end of the nineteenth century. At that time, there were physical phenomena that could not be explained with the existing physical theories, which now we call *classical physics*. The problem of the *black body radiation* was a cornerstone for the development of *quantum mechanics*, also called *quantum theory*. The energy spectrum that classical physics predicted for the radiation emitted by a *black body*, a perfect absorber and emitter of radiation, in a thermal bath at a constant temperature was different to what was observed experimentally. In 1900, Max Planck discovered that if the black body emitted and absorbed radiation in discrete packets of energy proportional to the radiation frequency then the energy spectrum observed experimentally would be justified theoretically. In 1905, Albert Einstein proposed that not only the electromagnetic radiation was interchanged discretely, but also that it was discrete itself. These ideas developed later into the concept of the *photon*, a particle of light. The emerging theory took its name from the Latin word 'quantus', which means 'how much', to refer to the discreteness of energy discovered by Planck and Einstein.

Nonrelativistic quantum mechanics was developed in the first decades of the

twentieth century mainly by Max Planck, Albert Einstein, Niels Bohr, Werner Heisenberg, Max Born, Louis de Broglie, Erwin Schrödinger, Wolfang Pauli, Paul Dirac and John von Neumann. In 1926, Erwin Schrödinger obtained an equation that described the time evolution of the quantum state. The linearity of Schrödinger's equation implies that quantum systems can be in a linear superposition of different quantum states. When applied to composite systems, *quantum superposition* leads to the property of *quantum entanglement*. Two systems that are entangled present correlations that cannot be explained by classical physics.

In 1935, Einstein, Podolsky and Rosen found an apparent paradox arisen from quantum entanglement [1]. The EPR argument considers a thought experiment in which a pair of particles created in an entangled state are sent to different laboratories that are arbitrarily far-apart. EPR proposed a criterion for the existence of an *element of physical reality* associated to a physical quantity and assumed *local causality*: the elements of physical reality associated to one of the particles cannot be instantaneously altered by an experiment performed on the other distant particle. They concluded that there are elements of reality associated to two physical quantities corresponding to one of the particles that quantum mechanics does not describe simultaneously, and thus that quantum mechanics does not provide a *complete* description of physical reality.

In 1964, John Bell gave a mathematical description for the criterion of physical reality and the assumption of local causality made by EPR [2]. The hypothetical physical theories satisfying these conditions are denoted as *local hidden variable theories* (LHVT). Bell proved that there are statistical prediction of quantum mechanics that cannot be explained by LHVT. Bell's model for LHVT allows the derivation of some inequalities, the *Bell inequalities*, for the correlations between measurement outcomes obtained on distant physical systems. The Bell inequalities, satisfied by LHVT, can be violated by entangled quantum systems. The violation of the Bell inequalities, commonly associated with the term of *nonlocality*, has been verified experimentally. Nevertheless, the Bell experiments performed so far present experimental deficiencies called *loopholes*, which do not allow us to make a definite claim about whether nature violates the EPR criterion of reality and local causality.

The phenomena of quantum superposition, quantum entanglement and quan-

tum nonlocality have important applications to the processing of information. The idea that quantum systems can be used to encode and process information evolved in the last decades of the twentieth century. The mathematical theory of classical information began with a paper by Claude Shannon in 1948 [3], in which the *classical entropy* for random variables was defined. An extension of Shannon's entropy for quantum systems is the *quantum entropy*, originally defined by John von Neumann in 1932 [4]. In 1969, Stephen Wiesner developed two protocols for coding information using quantum mechanics, which were not accepted for publication at that time [5], but which were published in 1983 with the name of *conjugate coding* [6]. The first protocol provides a way to transfer two messages that are encoded in the polarization of light, but only one of them can be received. The second protocol presents the concept of *quantum money*: money encoded in quantum systems that is impossible to counterfeit due to the laws of quantum mechanics. In 1973, Alexander Holevo proved a bound on the amount of classical information that can be communicated by transmitting a quantum system [7]. In 1982, the impossibility of copying unknown quantum states, the *no-cloning theorem*, was proven by William Wootters and Wojciech Zurek [8], and independently by Dennis Dieks [9]. The *stronger no-cloning theorem* was proven by Richard Jozsa [10, 11]. In 1992, Charles Bennett and Stephen Wiesner presented the *superdense coding* protocol, in which a two bit message can be communicated by transmitting only a spin-$\frac{1}{2}$ particle if the communicating parties share quantum entanglement [12]. The *quantum teleportation* protocol was published in 1993 by Charles Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres and William Wootters [13]. In quantum teleportation, quantum entanglement shared by two distant parties allows one party to transfer an unknown quantum state at her location to the other party, by only communicating classical information. In 1995, Benjamin Schumacher presented the idea of storing information in quantum states and compressing the quantum information. Schumacher's theorem states that the minimum rate at which a quantum information source can be compressed is given by its quantum entropy. Moreover, Schumacher named in his paper for the first time the elementary unit of quantum information as the *quantum bit*, or *qubit* [14].

Modern computer science began with a paper published by Alan Turing in

1936 [15]. Turing proposed a model of computation, named a *Turing machine* in his honour. The concept of a *quantum computer*, a computer operating with the laws of quantum mechanics, was first raised by Paul Benioff [16–18] and Richard Feynman [19,20] in the early 1980s. The first formal model of quantum computation was introduced by David Deutsch in 1985 [21]. In 1992, David Deutsch and Richard Jozsa presented an algorithm for quantum computation that is exponentially faster than any algorithm performed on a classical computer [22]. In 1994, Peter Shor obtained a quantum algorithm that finds the prime factors of a composite number in a polynomial time [23], which cannot be achieved by any known classical factoring algorithm. Since the security of many cryptographic systems used today are based on the mathematical difficulty of finding the prime factors of a large composite number, a quantum computer running Shor's algorithm would be able to decrypt such systems.

On the one hand, quantum computers would make the currently used cryptography insecure. On the other hand, quantum systems can be used in new models of cryptography, whose security is guaranteed by the laws of quantum mechanics. *Quantum cryptography* has its roots in the 1960s ideas of Wiesner, which were published until 1983. The term 'quantum cryptography' was used for the first time in 1982, in a work by Charles Bennett, Gilles Brassard, Seth Breidbart and Stephen Wiesner [24]. It was consolidated by Bennett and Brassard in 1984, when they presented the first *quantum key distribution* protocol, the *BB84* protocol [25]. Quantum key distribution allows two parties to generate a random secret string of bits, a *key*, which is used to encode secret messages. In the BB84 protocol, the key is encoded in a series of quantum systems that are prepared from a set of quantum states that are not mutually orthogonal. The impossibility of perfectly distinguishing non-orthogonal quantum states implies the security of the protocol. A different quantum key distribution protocol was proposed by Artur Ekert in 1991 [26]. Ekert's protocol requires that the communicating parties share entangled particles. Its security is guaranteed if a Bell inequality is violated. Jonathan Barrett, Lucien Hardy and Adrian Kent showed in 2005 that quantum key distribution is secure even against eavesdroppers not restricted by the laws of quantum mechanics, as long as the impossibility of sending messages faster than the speed of light is satisfied [27], leading to the

development of *device-independent* quantum key distribution.

1.2 Quantum Information

Quantum information science studies how information can fundamentally be encoded, processed and communicated using quantum systems [5]. Quantum systems are described by *quantum states*. The quantum state allows us to compute the outcome probabilities for the measurement of the physical properties of the described system. Quantum states can be *pure* or *mixed*. Mathematically, a pure state is a vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$. A mixed state is a *density operator*, also called a *density matrix*, which is a positive linear operator $\rho \in \mathcal{D}(\mathcal{H})$ of unit trace, where we define $\mathcal{D}(\mathcal{H})$ to be the set of density operators acting on the Hilbert space $\mathcal{H}$. The dimension of the Hilbert space equals the number of possible distinguishable outcomes in a measurement of the described system. For example, if the described physical system is the polarization of a photon or the spin of an electron, whose measurement gives one of two possible values, the dimension of the associated Hilbert space is two. An infinite dimensional Hilbert space is associated, for example, to the spatial position of a particle or to a field in relativistic quantum theory. In this thesis, we only consider nonrelativistic quantum theory and finite dimensional Hilbert spaces. We are interested in the properties of the quantum state, but not in the particular physical system that is described. For example, if we talk about a quantum state with Hilbert space of dimension two, we do not consider whether it describes the polarization of a photon, the spin of an electron or any other physical system. That is, we only discuss the properties of the quantum information.

1.2.1 Quantum Operations

A general physical operation allowed by quantum theory is called a *quantum operation*. There are three elementary quantum operations, from which a general quantum operation can be implemented [5].

Unitary evolution The time evolution of a quantum state $|\psi(t)\rangle$ is given by

the *Schrödinger equation*:

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \tag{1.1}$$

where $H(t)$ is the corresponding *Hamiltonian* and $h = 2\pi\hbar$ is *Planck's constant*. If the described quantum system is in a quantum state $|\psi(t_0)\rangle$ at the time t_0, its quantum state at the time $t_f > t_0$ is

$$|\psi(t_f)\rangle = \exp\Big(-\frac{i}{\hbar}\int_{t_0}^{t_f} dtH(t)\Big)|\psi(t_0)\rangle. \tag{1.2}$$

Since the Hamiltonian is a *Hermitian* operator, that is $H(t) = H^\dagger(t)$, the operator $U \equiv \exp\Big(-\frac{i}{\hbar}\int_{t_0}^{t_f} dtH(t)\Big)$ is *unitary*: $UU^\dagger = U^\dagger U = I$.

Adding or discarding a system If the original system A is in a state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ and an *ancilla* E in a state $\rho_E \in \mathcal{D}(\mathcal{H}_E)$ is added, the combined system AE is in the state $\rho_A \otimes \rho_E \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$, where $\otimes$ denotes the tensor product. If an original composite system AB is in a state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and the system B is discarded, the state ρ_A of the system A is obtained by taking the partial trace over $\mathcal{H}_B$: $\rho_A = \mathrm{Tr}_B(\rho_{AB}) \in \mathcal{D}(\mathcal{H}_A)$.

Projective measurements A *projective measurement* consists of a set of *projectors* $\{\Pi_j\}_{j=0}^{n-1}$, where n is the number of possible measurement outcomes. The projectors are linear operators that are Hermitian and satisfy $\Pi_j\Pi_k = \delta_{j,k}\Pi_j$ and $\sum_{j=0}^{n-1}\Pi_j = I$. If the system subject to the projective measurement is in the state ρ before the measurement then the outcome k is obtained with probability $P(k) = \mathrm{Tr}(\Pi_k\rho)$. After the outcome k is obtained, the state transforms into $\frac{\Pi_k\rho\Pi_k}{\mathrm{Tr}(\Pi_k\rho)}$.

An arbitrary quantum operation on a system A can be implemented by adding an ancilla E of sufficiently big dimension, applying a unitary operation on the joint system AE, possibly performing a projective measurement, and finally discarding the ancilla. For example, a *generalized measurement* on a system A can be implemented by adding an ancilla E, applying a unitary operation on AE, and then performing a projective measurement on AE.

A generalized measurement of n possible outcomes consists of a set of *measurement operators* $\{M_j\}_{j=0}^{n-1}$, which are linear operators satisfying the *completeness equation*:

$$\sum_{j=0}^{n-1} M_j^\dagger M_j = I. \tag{1.3}$$

If the measured system is in the state ρ before the measurement then the outcome k is obtained with probability $P(k) = \mathrm{Tr}(M_k \rho M_k^\dagger)$. After the outcome k is obtained, the state transforms into $\frac{M_k \rho M_k^\dagger}{\mathrm{Tr}(M_k \rho M_k^\dagger)}$.

It is often useful to analyze the outcome probabilities of a quantum measurement in terms of a *Positive Operator-Valued Measure* (*POVM*). A POVM corresponding to a measurement with n possible outcomes consists of a set of n POVM elements $\{F_j\}_{j=0}^{n-1}$, which are positive operators satisfying $\sum_{j=0}^{n-1} F_j = I$. The probability that a measurement outcome k is obtained when a state ρ is subject to the measurement is $P(k) = \mathrm{Tr}(F_k \rho)$. The POVM elements are related to the measurement operators by $F_j = M_j^\dagger M_j$.

A useful mathematical description of a quantum operation is given by the *operator-sum representation*. The operator sum representation of a quantum operation $\mathcal{E}$ is the following:

$$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger, \tag{1.4}$$

where $\{E_j\}$ is a set of linear operators, the *Kraus operators*, that satisfy

$$\sum_j E_j^\dagger E_j \leq I. \tag{1.5}$$

The more general quantum operations are *non-trace-preserving*, for which the previous equation is satisfied. If $\sum_j E_j^\dagger E_j = I$, the quantum operation is *trace-preserving*. A non-trace-preserving quantum operation corresponds to a process in which information is obtained due to a quantum measurement.

An important quantum operation is the *depolarizing map*. It transforms a state $\rho \in \mathcal{D}(\mathbb{C}^d)$ as follows:

$$\mathcal{E}(\rho) = p\frac{I}{d} + (1-p)\rho, \tag{1.6}$$

where p is the probability that ρ is replaced by the *completely mixed state* $\frac{I}{d}$. The depolarizing map is covariant. A *covariant map* $\mathcal{E}^{\text{cov}}$ is such that

$$\mathcal{E}^{\text{cov}}(U\rho U^\dagger) = U\mathcal{E}^{\text{cov}}(\rho)U^\dagger, \tag{1.7}$$

for any quantum state $\rho \in \mathcal{D}(\mathbb{C}^d)$ and unitary operation $U \in \text{SU}(d)$, where $\text{SU}(d)$ is the special unitary group of degree d.

1.2.2 The Qubit

The elementary unit of quantum information is the *qubit*, or *quantum bit*. The qubit is defined as a quantum system with Hilbert space of dimension two. The qubit is the quantum generalization of a *bit*. A bit can be in one of two possible states: '0' or '1'. A probabilistic bit is described by its probability of being in the state 0, which can be described geometrically by a point on a line of unit length. The mathematical structure of a qubit is much richer than that of a bit. Its quantum state can be visualized geometrically by a point in a sphere, the *Bloch sphere* [5].

The quantum state ρ of a qubit is related to the Bloch sphere through its *Bloch vector* $\vec{r} \in \mathbb{R}^3$, with $\|\vec{r}\| \leq 1$. The relation is

$$\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}), \tag{1.8}$$

where $\vec{\sigma} \equiv (\sigma_x, \sigma_y, \sigma_z)$, I is the identity on $\mathbb{C}^2$ and

$$\sigma_x \equiv \sigma_1 \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y \equiv \sigma_2 \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z \equiv \sigma_3 \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

are the *Pauli matrices*. Pure states define the surface of the sphere: $\|\vec{r}\| = 1$. Mixed states are associated with the interior of the sphere: $\|\vec{r}\| < 1$. The

completely mixed state $\frac{I}{2}$ has Bloch vector zero and corresponds to the centre of the sphere. The north and south poles correspond to the eigenstates of σ_z with eigenvalues 1 and -1, which are denoted as $|0\rangle$ and $|1\rangle$, respectively. Antipodal points on the Bloch sphere define an orthonormal basis. The basis $\{|0\rangle, |1\rangle\}$ is called the *computational basis*. The expansion of a pure state $|\psi\rangle$ of a qubit in this basis is

$$|\psi\rangle = \cos\Big(\frac{\theta}{2}\Big)|0\rangle + e^{i\phi}\sin\Big(\frac{\theta}{2}\Big)|1\rangle, \tag{1.9}$$

where $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$ are the polar and azimuthal angles of the Bloch vector, respectively.

An arbitrary unitary operation on a qubit state can be expressed as follows:

$$U = e^{i\alpha}e^{-i\frac{\beta}{2}\hat{n}\cdot\vec{\sigma}}, \tag{1.10}$$

where $\alpha, \beta \in \mathbb{R}$ and $\hat{n}$ is a unit vector in $\mathbb{R}^3$. Up to the global phase $e^{i\alpha}$, the unitary operation U has the effect of rotating the Bloch vector by an angle β along the axis $\hat{n}$ in the Bloch sphere.

The depolarizing map applied to a qubit state ρ is

$$\mathcal{E}(\rho) = p\frac{I}{2} + (1-p)\rho, \tag{1.11}$$

where p is the probability that ρ is replaced by the completely mixed state. It has the effect of contracting uniformly the Bloch sphere as a function of p. The depolarizing map is the only covariant map acting on a qubit.

A useful identity that is satisfied for any qubit density matrix ρ is the following:

$$\frac{I}{2} = \frac{1}{4}(\rho + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z). \tag{1.12}$$

If we substitute $\frac{I}{2}$, as given by the previous identity, into (1.11), we obtain that the operator-sum representation of the qubit depolarizing map has Kraus operators $E_0 = \sqrt{1-\frac{3p}{4}}I$ and $E_i = \frac{\sqrt{p}}{2}\sigma_i$, for $i = 1, 2, 3$.

A quantum system of dimension d is called a *qudit*, where d is an integer bigger than two. In this thesis, we usually consider sets of n qubits, which form qudits of dimension 2^n. In general, these qubits can be *entangled*. A bipartite

quantum state $\rho \in \mathcal{D}(\mathcal{H})$, with $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, is said to be *entangled* if it cannot be expressed as a convex combination of product states, that is, if it cannot be expressed in the form

$$\rho = \sum_{j=1}^{N} p_j \eta_j \otimes \gamma_j, \tag{1.13}$$

for some probability distribution $\{p_j\}_{j=1}^N$, and states $\{\eta_j\}_{j=1}^N \in \mathcal{D}(\mathcal{H}_A)$ and $\{\gamma_j\}_{j=1}^N \in \mathcal{D}(\mathcal{H}_B)$. On the other hand, a state ρ that can be expressed in the form (1.13) is called *separable*.

1.2.3 Entropy

In this section we briefly discuss a few properties of the entropy for classical random variables and for quantum systems [5].

1.2.3.1 Classical Entropy

Consider a *classical random variable* X that takes the value $x \in \{0, 1, \ldots, d-1\}$ with probability P_x. Shannon [3] defined the entropy of X by

$$H(X) \equiv -\sum_{x=0}^{d-1} P_x \log_2 P_x, \tag{1.14}$$

where $0 \log_2 0 \equiv 0$. Although there can be other definitions of entropy for classical variables, we only discuss the *Shannon entropy* in this thesis, and we refer to it as the *classical entropy*.

The classical entropy is a measure of how much a *classical information source* can be compressed. A classical information source is defined by a set of random variables $X_1, X_2, \ldots, X_N$, whose values $x_1, x_2, \ldots, x_N$ are the outputs of the source. An *independent* and *identically distributed* (i.i.d) information source is one for which $X_j = X$ for $j = 1, 2, \ldots, N$ and whose outputs are independent and identically distributed. *Shannon's noiseless channel coding theorem* [3] states that the minimum number of bits needed to compress reliably the output of an i.i.d information source X per use of the source in the limit $N \to \infty$ is given by the classical entropy $H(X)$.

An important property of the classical entropy is that

$$0 \leq H(X) \leq \log_2 d. \tag{1.15}$$

The entropy is zero if X is deterministic, that is, if $P_x = 1$ for some x. It is maximum if X is totally random, that is, if $P_x = \frac{1}{d}$ for $x = 0, 1, \ldots, d-1$. If X is a variable of n bits, that is, if $d = 2^n$ then $H(X) \leq n$.

A very useful property of the classical entropy is that it is a *concave* function. Consider a set of random variables $\{X_j\}_{j=0}^{l-1}$ and a probability distribution $\{q_j\}_{j=0}^{l-1}$. Let X_j take the value $x \in \{0, 1, \ldots, d-1\}$ with probability $P_x^{(j)}$. Consider a random variable X' that takes the value $x \in \{0, 1, \ldots, d-1\}$ with probability $P'_x \equiv \sum_{j=0}^{l-1} q_j P_x^{(j)}$. The *concavity* property of the classical entropy states that

$$\sum_{j=0}^{l-1} q_j H(X_j) \leq H(X'). \tag{1.16}$$

We can assign a *joint entropy* to a pair of random variables X and Y. Let X and Y take the values $x \in \{0, 1, \ldots, d-1\}$ and $y \in \{0, 1, \ldots, d'-1\}$, respectively. Let $P_{x,y}$ be the probability that $X = x$ and $Y = y$. The *joint entropy* of X and Y is defined as

$$H(XY) \equiv -\sum_{x=0}^{d-1} \sum_{y=0}^{d'-1} P_{x,y} \log_2 P_{x,y}. \tag{1.17}$$

An important inequality satisfied by the classical entropy is *subadditivity*:

$$H(XY) \leq H(X) + H(Y), \tag{1.18}$$

where the probability distributions for X and Y are obtained from the probabilities $P_{x,y}$ as follows: $P_x = \sum_{y=0}^{d'-1} P_{x,y}$ and $P_y = \sum_{x=0}^{d-1} P_{x,y}$. The equality is achieved if and only if X and Y are independent variables, that is, if $P_{x,y} = P_x P_y$ for all $x \in \{0, 1, \ldots, d-1\}$ and $y \in \{0, 1, \ldots, d'-1\}$. Another useful inequality is that

$$H(Y) \leq H(XY), \tag{1.19}$$

where the equality is achieved if and only if X is a function of Y. A similar

inequality is obtained if X and Y are interchanged in (1.19).

The *classical mutual information* of X and Y is defined as

$$H(X:Y) \equiv H(X) + H(Y) - H(XY). \tag{1.20}$$

It is a measure of the information shared by X and Y. From inequalities (1.18) and (1.19), it follows that the classical mutual information satisfies

$$0 \leq H(X:Y) \leq H(X). \tag{1.21}$$

The value of $H(X:Y)$ is zero if X and Y do not share any information. It achieves $H(X:Y) = H(X)$ if all the information about X is contained in Y. Formally, $H(X:Y) = 0$ if and only if X and Y are independent, and $H(X:Y) = H(X)$ if and only if X is a function of Y. Similar results are obtained if X and Y are interchanged.

1.2.3.2 Quantum Entropy

The entropy of a quantum system provides a measure of the uncertainty about its state. The entropy of a quantum state ρ was defined by von Neumann [4], up to a factor of $\ln 2$, as

$$S(\rho) \equiv -\mathrm{Tr}(\rho \log_2 \rho). \tag{1.22}$$

There can be different definitions of entropy for quantum states. In this thesis we only consider the *von Neumann entropy* and we refer to it as the *quantum entropy*.

The quantum entropy is a measure of how much a *quantum information source* can be compressed. A quantum information source is defined by a Hilbert space $\mathcal{H}$ and a density matrix $\rho \in \mathcal{D}(\mathcal{H})$, which corresponds to an ensemble of signal states ρ_i occurring with probability p_i, $\rho \equiv \sum_i p_i \rho_i$. The source is *independent* and *identically distributed* (i.i.d) if N uses of the source produce the ensemble state $\rho^{\otimes N}$, that is, the outputs of different uses of the channel are in a product state. *Schumacher's quantum noiseless channel coding theorem* [14] states that the minimum number of qubits needed to compress reliably the output of an i.i.d quantum information source per use of the source in the limit $N \to \infty$ is given

by $S(\rho)$.

The quantum entropy of a state $\rho \in \mathcal{D}(\mathbb{C}^d)$ equals

$$S(\rho) = -\sum_{j=0}^{d-1} \lambda_j \log_2 \lambda_j, \tag{1.23}$$

where $\{\lambda_j\}_{j=0}^{d-1}$ is the set of eigenvalues of ρ and we define $0 \log_2 0 \equiv 0$. From this expression and (1.14), we see that the quantum entropy of ρ equals the classical entropy of the probability distribution corresponding to its eigenvalues. From (1.15), it follows that

$$0 \leq S(\rho) \leq \log_2 d. \tag{1.24}$$

The entropy of ρ is zero if it only has one nonzero eigenvalue, which equals unity, that is, if ρ is pure. It achieves its maximum value $\log_2 d$ if all its eigenvalues are equal, that is, if ρ is the completely mixed state $\frac{I}{d}$. From (1.24), we see that if ρ is a state of n qubits, which means that $d = 2^n$, we have that $S(\rho) \leq n$.

Similar to the classical entropy, the quantum entropy is concave. Consider a quantum state $\rho' \equiv \sum_{j=0}^{l-1} q_j \rho_j$ for a probability distribution $\{q_j\}_{j=0}^{l-1}$ and quantum states $\{\rho_j\}_{j=0}^{l-1}$. The *concavity* of the quantum entropy states that

$$\sum_{j=0}^{l-1} q_j S(\rho_j) \leq S(\rho'). \tag{1.25}$$

Consider two quantum systems A and B that are in a joint quantum state ρ_{AB}. Let $\rho_A \equiv \mathrm{Tr}_B(\rho_{AB})$ and $\rho_B \equiv \mathrm{Tr}_A(\rho_{AB})$ be the quantum states of A and B, respectively. In the rest of this thesis, we adopt the notation $S(A) \equiv S(\rho_A)$, $S(B) \equiv S(\rho_B)$ and $S(AB) \equiv S(\rho_{AB})$. Two important inequalities for the quantum entropy are *subadditivity* and the *triangle inequality*, also called the *Araki-Lieb inequality*. *Subadditivity* [28] states that

$$S(AB) \leq S(A) + S(B). \tag{1.26}$$

The equality in (1.26) is achieved if and only if A and B are not correlated, that

is, if $\rho_{AB} = \rho_A \otimes \rho_B$. The *triangle inequality* [29] states that

$$|S(B) - S(A)| \leq S(AB). \tag{1.27}$$

Similar to the classical mutual information, the *quantum mutual information* is defined by

$$I(A : B) \equiv S(A) + S(B) - S(AB). \tag{1.28}$$

It is a measure of the total correlations between the quantum systems A and B [30–32]. From (1.26) – (1.28), it follows that

$$0 \leq I(A : B) \leq 2S(A). \tag{1.29}$$

This inequality is satisfied too if we exchange A and B. Notice the factor of 2 that appears in this inequality compared to the analogous inequality (1.21) for the classical mutual information. This factor appears due to the triangle inequality (1.27) for the quantum entropy, which cannot be saturated by classical random variables X and Y, as follows from (1.19), unless one of these is deterministic, say X, in which case the upper bound in (1.29) is achieved trivially: $H(X : Y) = 2H(X) = 0$.

An important property of the quantum mutual information is that it cannot increase by quantum operations that act locally on one of the systems. Consider a quantum operation that acts locally on the system A. Let AB and $A'B$ denote the composite quantum systems before and after a quantum operation is applied on A, respectively. The *data-processing inequality* states that

$$I(A' : B) \leq I(A : B). \tag{1.30}$$

The properties of the quantum entropy discussed in this section are very useful in chapter 4, where we introduce a new principle of quantum information.

1.2.4 Fundamental Principles

Two fundamental principles of quantum information are the *no-cloning theorem* and the *no-signalling principle*.

1.2.4.1 The No-Cloning Theorem

The *no-cloning theorem* states that an unknown quantum state cannot be copied perfectly [8, 9]. This theorem holds even probabilistically [33]. That is, it is impossible to produce a perfect copy of an unknown quantum state with any nonzero success probability. We introduce a more general theorem in section 3.4, from which these results are obtained. The proof follows easily from the unitary evolution and the linearity of quantum theory.

A theorem in the spirit of the no-cloning theorem is the *stronger no-cloning theorem*, which considers the question of how much information about a state $|\psi\rangle$ is necessary to produce a copy of it. The stronger no-cloning theorem states that for a set of pure states $\{|\psi_j\rangle\}_j$, in which no pair of states are orthogonal, and a set of (possibly mixed) states $\{\rho_j\}_j$ of an ancilla, the physical operation $|\psi_j\rangle \otimes \rho_j \to |\psi_j\rangle \otimes |\psi_j\rangle$ is possible if and only if the physical operation $\rho_j \to |\psi_j\rangle$ is possible, that is, the ancilla must have complete information about the state $|\psi_j\rangle$ [10, 11].

Although perfect quantum cloning is impossible, imperfect cloning is not. The first discovered *quantum cloning machine* takes as input an unknown pure state $|\psi\rangle$ of a qubit and gives as output two qubits with equal reduced density matrices ρ such that the fidelity $f \equiv \langle\psi|\rho|\psi\rangle$ equals $\frac{5}{6}$ [34], which is its maximum possible value [35–37]. There exist different classes of quantum cloning machines. The *optimal symmetric universal quantum cloning machines* have been studied in great detail. A quantum cloning machine is *universal* if all states are cloned equally well. It is *symmetric* if it achieves the same fidelity for all the obtained clones. It is *optimal* if the clones have the maximum fidelities allowed by quantum theory [38]. The fidelities of the clones achieved by an optimal symmetric universal quantum cloning machine that takes N pure qudits as inputs and outputs M qudit clones are given by [39, 40]:

$$f = \frac{N}{M} + \frac{(M-N)(N+1)}{M(N+d)}. \tag{1.31}$$

We see that the fidelity reduces to $f = \frac{5}{6}$ for the simplest case $d = 2$, $N = 1$ and $M = 2$.

1.2.4.2 The No-Signalling Principle

The *no-signalling principle* states that communication between two distant parties cannot be performed without the transmission of any physical systems, despite any physical resources that the parties may share. We present a mathematical expression for this principle and discuss it in detail in section 1.3.2. We discuss in section 1.3.2 that quantum theory is consistent with relativistic causality by satisfaction of the no-signalling principle.

1.2.5 Fundamental Protocols

We discuss two fundamental protocols of quantum information theory: *superdense coding* and *quantum teleportation*. These protocols are performed by two distant parties, Alice and Bob. Superdense coding, originally called *4 way coding*, is a protocol in which Alice communicates Bob two bits of classical information by transmitting a single qubit [12]. On the other hand, quantum teleportation allows Alice to transfer an unknown qubit state at her location to Bob's location, by transmitting two bits of classical information without the need to transmit any quantum systems [13]. In the general case, these protocols consider a qudit and a classical message of d^2 possible values.

1.2.5.1 Superdense Coding

Superdense coding [12] is a protocol in which Alice communicates Bob $2\log_2 d$ bits of classical information, or more precisely, a message of d^2 possible values, by sending him a qudit. We first describe the protocol in the case of a qubit, $d = 2$.

Alice and Bob need to share a pair of qubits a, at Alice's location, and b, at Bob's location, in a maximally entangled state. Up to local unitary operations, the maximally entangled state is the *singlet state*: $|\Psi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$. Alice has a two bit message (x_0, x_1) that she wants to communicate Bob. Thus, Alice applies the unitary operation σ_{x_0,x_1} on her qubit a, where $\sigma_{0,0} \equiv I$ is the identity acting on $\mathbb{C}^2$ and $\sigma_{0,1} \equiv \sigma_1$, $\sigma_{1,0} \equiv \sigma_2$ and $\sigma_{1,1} \equiv \sigma_3$ are the Pauli matrices. The shared entangled state transforms into $(\sigma_{x_0,x_1} \otimes I)|\Psi^-\rangle_{ab}$. Alice's

operation generates one of four mutually orthogonal states, the *Bell states*:

$$\begin{aligned} |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle), \\ |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle). \end{aligned} \tag{1.32}$$

The transformations are obtained in the following way:

$$\begin{aligned} (\sigma_{0,0} \otimes I)|\Psi^{-}\rangle_{ab} &= |\Psi^{-}\rangle_{ab}, \\ (\sigma_{0,1} \otimes I)|\Psi^{-}\rangle_{ab} &= -|\Phi^{-}\rangle_{ab}, \\ (\sigma_{1,0} \otimes I)|\Psi^{-}\rangle_{ab} &= i|\Phi^{+}\rangle_{ab}, \\ (\sigma_{1,1} \otimes I)|\Psi^{-}\rangle_{ab} &= |\Psi^{+}\rangle_{ab}. \end{aligned} \tag{1.33}$$

Then, Alice sends Bob the qubit a. Bob measures the two qubit system ab in the Bell basis. Bob's measurement outcome indicates Alice's message (x_0, x_1).

Consider now the case in which Alice and Bob have qudits a and b, respectively, in a maximally entangled state $|\Psi\rangle_{ab}$. In the schmidt basis $\{|l\rangle\}_{l=0}^{d-1}$, the expression for $|\Psi\rangle_{ab}$ is $|\Psi\rangle_{ab} = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle_a |l\rangle_b$. Alice wants to communicate Bob a classical message (j, k) of d^2 possible values, with $j, k \in \{0, 1, \ldots, d-1\}$. Thus, Alice applies the following unitary operation on her system a:

$$U_{j,k} = \sum_{l=0}^{d-1} e^{\frac{i2\pi lj}{d}} |l\rangle\langle (l+k) \bmod d|. \tag{1.34}$$

The state $|\Psi\rangle_{ab}$ is transformed into $(U_{j,k} \otimes I)|\Psi\rangle_{ab} = |\phi_{j,k}\rangle_{ab}$. The transformed state is

$$|\phi_{j,k}\rangle_{ab} = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{\frac{i2\pi lj}{d}} |l\rangle_a |(l+k) \bmod d\rangle_b. \tag{1.35}$$

Alice sends Bob her system a. Since the states $\{|\phi_{j,k}\rangle\}_{j,k=0}^{d-1}$ form an orthonormal basis of $\mathbb{C}^d \otimes \mathbb{C}^d$, by measuring the joint system ab in this basis, Bob obtains Alice's message (j, k) perfectly.

1.2.5.2 Quantum Teleportation

Quantum teleportation [13] provides a way for Alice to transfer an unknown quantum state at her location to Bob's location, which can be arbitrarily far and possibly unknown to her, without the need to transmit any quantum systems. We first discuss the quantum teleportation protocol for a qubit state.

Alice has a qubit a in an unknown quantum state that she wants to teleport to Bob's location. For convenience, we consider that a is in a pure state $|\psi\rangle_a$. Due to the linearity of quantum theory, quantum teleportation works too if a is in a mixed state, possibly in an entangled state with another system. The physical resource that makes quantum teleportation possible is quantum entanglement. Alice and Bob need to share a pair of qubits A, at Alice's location, and B, at Bob's location, in a maximally entangled state in order to complete quantum teleportation faithfully. Thus, consider that Alice and Bob share a singlet state $|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$. Alice measures their qubits in the Bell basis $\{|\Psi^\pm\rangle, |\Phi^\pm\rangle\}$. The initial state of the three qubits system can be expressed by

$$\begin{aligned} |\psi\rangle_a|\Psi^-\rangle_{AB} &= -\frac{1}{2}|\Psi^-\rangle_{aA} \otimes |\psi\rangle_B - \frac{1}{2}|\Psi^+\rangle_{aA} \otimes \sigma_z|\psi\rangle_B + \frac{1}{2}|\Phi^-\rangle_{aA} \otimes \sigma_x|\psi\rangle_B \\ &\quad - \frac{i}{2}|\Phi^+\rangle_{aA} \otimes \sigma_y|\psi\rangle_B, \end{aligned} \tag{1.36}$$

for any state $|\psi\rangle \in \mathbb{C}^2$. We see that for any measurement outcome obtained by Alice, Bob's qubit projects into the state $|\psi\rangle$, up to a possible Pauli error σ_x, σ_y or σ_z. Bob obtains the teleported state $|\psi\rangle$ perfectly after applying the corresponding Pauli unitary operation that corrects the error. To do so, Bob needs to receive a two bit message that indicates Alice's measurement result.

Quantum teleportation is consistent with the no-cloning theorem. From Equation (1.36), we see that the state of Alice's qubits projects into one of the four Bell states. Thus, no copies of $|\psi\rangle$ are produced during quantum teleportation. In principle, it is not necessary that Alice knows Bob's location, because she can broadcast her measurement result to all possible regions of space where Bob might be. On the other hand, sending the system a directly does not allow Alice to transfer its state to an unknown location of Bob, because according to the no-cloning theorem, the unknown quantum state $|\psi\rangle$ cannot be copied, hence, Alice

can only transmit a single copy of it and thus is forced to know Bob's location.

Quantum teleportation is consistent with the no-signalling principle. From Equation (1.36), we see that Alice's measurement outcome is totally random. It follows that, before receiving any message from Alice, Bob's qubit is in the mixed state

$$\rho_B = \frac{1}{4}(|\psi\rangle\langle\psi| + \sigma_x|\psi\rangle\langle\psi|\sigma_x + \sigma_y|\psi\rangle\langle\psi|\sigma_y + \sigma_z|\psi\rangle\langle\psi|\sigma_z), \tag{1.37}$$

which is the completely mixed state $\frac{I}{2}$, as seen from the identity (1.12). Thus, Bob cannot obtain any information about the state $|\psi\rangle$ before receiving a message from Alice, as stated by the no-signalling principle. Moreover, the no-signalling principle implies that faithful teleportation of an unknown qubit state cannot be accomplished if Alice sends Bob less than two bits of classical information, as shown below [13].

Suppose that a message of c bits is sufficient to complete faithful teleportation of an unknown qubit state, with c possibly smaller than two. Using the superdense coding protocol [12], we show that the no-signalling principle implies that $c = 2$. Let Alice and Bob share a singlet $|\Psi^-\rangle_{ab}$ that they use to perform superdense coding and some resource state $|\xi\rangle_{AB}$ that they use for teleportation. Alice has the system aA and Bob has the system bB. We do not impose any conditions on the state $|\xi\rangle_{AB}$. Alice is given a random two bit message (x_0, x_1) that she encodes in her qubit a by applying the unitary operation σ_{x_0,x_1} on it, where $\sigma_{0,0} \equiv I$, $\sigma_{0,1} \equiv \sigma_1$, $\sigma_{1,0} \equiv \sigma_2$ and $\sigma_{1,1} \equiv \sigma_3$. In the superdense coding protocol, Alice then sends Bob her qubit a and Bob learns the message (x_0, x_1) after measuring the pair ab in the Bell basis. Consider instead, that Alice does not send Bob her qubit a, but that she teleports its state to Bob's qubit B. However, Alice does not send Bob the c-bits message y that would allow Bob to complete the teleportation. Bob guesses the value of y with probability 2^{-c}, in which case, after performing the teleportation correction operation and the Bell measurement, Bob learns the two bit message (x_0, x_1). Hence, Bob learns the value of (x_0, x_1) with probability 2^{-c}. Since there is not communication in this protocol, the no-signalling principle implies that Bob can only obtain the two bit random message (x_0, x_1) with the probability of making a random guess. Thus, it must be that $2^{-c} = \frac{1}{4}$, which means that $c = 2$.

Now we discuss the teleportation of a quantum state of dimension bigger than two. Teleportation of a state of n qubits can be performed by applying the teleportation protocol described above for each of the n qubits. Teleportation of an arbitrary qudit state $|\psi\rangle_a$ can be performed as follows. Alice and Bob share a maximally entangled state $|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle_A |l\rangle_B$, where $\{|l\rangle\}_{l=0}^{d-1}$ is the Schmidt basis. Alice measures her pair of qudits aA in the basis defined by the set of orthonormal states

$$|\phi_{j,k}\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{\frac{i2\pi lj}{d}} |l\rangle |(l+k) \bmod d\rangle. \tag{1.38}$$

Alice obtains the measurement outcome (j, k) and sends it to Bob. Then, Bob applies the following unitary operation on B:

$$U_{j,k} = \sum_{l=0}^{d-1} e^{\frac{i2\pi lj}{d}} |l\rangle\langle (l+k) \bmod d|. \tag{1.39}$$

After Bob's operation, the state of his system B transforms into the state $|\psi\rangle$. Similar to the qubit case, the superdense coding protocol and the no-signalling principle can be used to show that faithful teleportation of an unknown quantum state of dimension d requires a message of $2 \log_2 d$ bits from Alice to Bob [13].

From Equations (1.34), (1.35), (1.38) and (1.39), we notice that the measurement applied by Alice and the unitary correction operations applied by Bob in the quantum teleportation protocol are the same as the decoding measurement applied by Bob and the encoding unitary operations applied by Alice in the superdense coding protocol, respectively. In this sense, quantum teleportation can be considered as the inverse of superdense coding. In section 4.5, we present two novel quantum information protocols that combine quantum teleportation and superdense coding, and show that they satisfy a similar inverse relation.

In chapter 3, we discuss a different type of teleportation protocol, denoted as *port-based teleportation*. We use the original quantum teleportation protocol described in this section, together with the superdense coding protocol, the no-cloning theorem and the no-signalling principle to show an upper bound on the success probability of port-based teleportation.

1.3 Bell Inequalities and the No-Signalling Principle

Causality is a fundamental physical principle, which can be understood as stating that if P is an event occurring before another event F, P can be a cause of F, but it cannot be a consequence of F. In other words, events in the future are consequences of events in the past or in the present, but events in the past cannot be consequences of events in the future. The previous statement seems obvious according to our human experience of time. Nevertheless, giving a precise definition of causality is a subtle problem. Although we do not attempt to define causality in a precise way, we discuss briefly the question of causality in the frameworks of special relativity and quantum mechanics.

According to relativity, space and time are not separate entities, but a single physical concept called *spacetime*. Physical events occurring in different reference frames in spacetime are observed differently. That is, physical quantities like distance, time length, speed and energy are relative to observers in difference reference frames. However, there is a physical quantity that remains constant in all reference frames, the *speed of light* in the vacuum, which has a value of 2.998 x 10^8 meters per second, and is the maximum speed that any physical system can have in any reference frame.

The speed of light allows us to make a precise statement of which events are in the future and which are in the past of a given event. Consider the spacetime diagram in Figure 1.1. The physical events A, B, C and D are observed in two different inertial reference frames, which displace from each other at a constant speed. The spatial and time coordinates are x and t for the unprimed frame, and x' and t' for the primed frame. The speed of light in the vacuum is denoted by c. The dashed lines represent two light beams in the vacuum that reach A and continue their way in opposite directions. These lines define a two-dimensional slice of two four-dimensional cones, the *light cones* of A. Events inside the upper cone are in the future of A and events in the lower cone are in the past of A. This is independent of the reference frame, because the speed of light is the same in any reference frame. We see that the distance and time lengths between the events observed in the unprimed frame are different in the primed frame, but in

both frames C and D are in the past and in the future of A, respectively. On the other hand, B is neither in the past nor in the future of A. We say that C, A and D are *time-like* separated, while A and B are *space-like* separated. Time-like separated events are causally connected, but space-like separated events are not. Thus, a relativistic notion of causality is that a physical event A can be a cause of a physical event D, only if A and D are time-like separated and D is in the future of A. This means in particular that if A and B are space-like separated events then B cannot be caused by A, and vice versa. In this section we describe how quantum mechanics shakes this notion of causality through the violation of the Bell inequalities, but still remains consistent with it by satisfaction of the no-signalling principle.

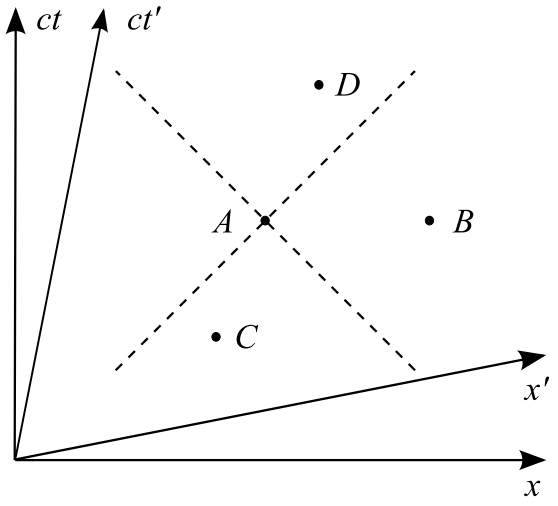


Figure 1.1: Spacetime diagram for physical events A, B, C and D, which are observed in two different inertial reference frames that displace away from each other at a constant speed. The spatial and time coordinates are x and t in one frame and x' and t' in the other frame, respectively. The speed of light in the vacuum is denoted by c. The dashed lines define a two-dimensional slice of the four-dimensional light cones of A. The events C, A and D are time-like separated, while A and B are space-like separated. The events C and D are in the past and in the future of A, respectively.

1.3.1 Bell Inequalities

1.3.1.1 The EPR Argument

In their seminal paper [1], Einstein, Podolsky and Rosen claimed that quantum mechanics is not a complete theory. Their argument is based on an implicit physical assumption based on relativistic causality and a defined criterion of physical reality. These assumptions are the following.

Local causality. *A physical event A cannot have any influence on another physical event B, if A and B are space-like separated.*

The EPR criterion of reality. *If the value of a physical quantity can be predicted with certainty without disturbing the system then there exists an element of physical reality associated to this physical quantity.*

We consider Bohm's [41] version of the EPR thought experiment, whose spacetime diagram is given in Figure 1.2. A pair of qubits is prepared in the singlet state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big)$.[1] The qubits are sent to two distant laboratories, one controlled by Alice and the other one controlled by Bob. Alice randomly chooses a measurement $A \in \{0, 1\}$ from a set of two elements. Similarly, Bob randomly chooses a measurement $B \in \{0, 1\}$. Alice and Bob perform a projective measurements on their qubits in a basis corresponding to the Bloch vectors $\vec{a}_A$ and $\vec{b}_B$, respectively. Alice obtains an outcome a and Bob obtains an outcome b. The measurement outcomes are assigned numerical values $a = \pm 1$ and $b = \pm 1$, if the qubits project into the states with Bloch vectors $\pm\vec{a}_A$ and $\pm\vec{b}_B$, respectively. A crucial property of the experiment is that the spacetime region in which Alice chooses her measurement A is space-like separated from the spacetime region in which Bob obtains his outcome b, and vice versa.

A property of the singlet state is that if both qubits are measured in the same basis, the outcomes are opposite. This means that if Alice measures her qubit in the basis corresponding to the Bloch vector $\vec{a}_A$ and obtains outcome a then, if Bob measures his particle in the same basis, $\vec{b}_B = \vec{a}_A$, Bob's outcome

[1] The physical quantities considered in the EPR original argument are the momentum and position of a particle, whereas the quantity considered in Bohm's version is the spin of a spin-$\frac{1}{2}$ particle, which is a particular type of qubit system.

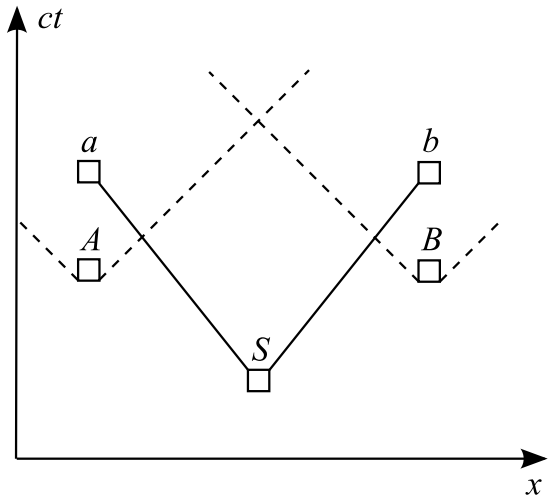


Figure 1.2: Spacetime diagram of the EPR-Bohm experiment. The boxes represent spacetime regions in which a pair of qubits is created in the singlet state (S) and sent to Alice's and Bob's distant laboratories, Alice randomly chooses her measurement (A), Alice applies the measurement on her qubit and obtains a measurement outcome (a), Bob randomly chooses his measurement (B), and Bob applies the measurement on his qubit and obtains a measurement outcome (b). The dashed lines represent the two-dimensional slices of the light cones for the regions corresponding to the measurement choices. The regions A and b are space-like separated. Similarly, B and a are space-like separated.

is $b = -a$ with probability equal to unity. Since Alice's and Bob's experiments are space-like separated, the assumption of local causality implies that Alice's experiment on her qubit cannot in any way disturb the qubit at Bob's location, and vice versa. Thus, local causality and the EPR criterion of reality imply the existence of an element of physical reality associated to Bob's qubit measurement $\vec{b}_B = \vec{a}_A$. This argument holds for any measurement basis $\vec{a}_A$ chosen by Alice, and $\vec{b}_B = \vec{a}_A$ by Bob. Thus, EPR argued that there are elements of physical reality associated to any measurement $\vec{b}_B$ that Bob can perform on his qubit. However, quantum mechanics does not describe all possible qubit measurement values simultaneously. For example, if Bob's measurement corresponds to $\vec{b}_B = \hat{z}$, the state of his qubit projects into one of the orthogonal states $|0\rangle$ or $|1\rangle$. Hence, Bob obtains complete knowledge about his qubit state in this basis, but his qubit is then in an equal superposition of the orthogonal states $|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ and

$|-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$, which means that Bob does not have any knowledge about his qubit state in the basis corresponding to $\vec{b}_B = \hat{x}$. Therefore, EPR concluded that quantum mechanics cannot be a complete theory, because there are physical quantities with elements of physical reality that quantum mechanics does not describe simultaneously.

The EPR assumptions of local causality and physical reality seem as sensible conditions for a physical theory. Nevertheless, these conditions are not necessarily satisfied by nature. In the following sections we describe how hypothetical theories based on the EPR criterion of reality and local causality can be tested experimentally.

1.3.1.2 Bell's Theorem

Bell [2] provided a mathematical description for *local hidden variable theories* (LHVT), which are hypothetical physical theories based on the EPR assumptions of local causality and physical reality. Bell's formalism allows us to test these conditions experimentally.

Consider the EPR-Bohm experiment described in the previous section. According to deterministic LHVT, the outcomes a and b are determined respectively by the measurement choices A and B and by hidden variables λ shared by both qubits, in the following way:

$$a = a(A, \lambda) \in \{1, -1\}, \qquad b = b(B, \lambda) \in \{1, -1\}. \tag{1.40}$$

We can also consider probabilistic LHVT, which determine the outcomes a and b with some probability of the form

$$P(a, b|A, B, \lambda) = P(a|A, \lambda)P(b|B, \lambda). \tag{1.41}$$

An LHVT also assigns a probability distribution $\rho(\lambda)$, independent of A and B, to the hidden variables, satisfying positivity and normalization:

$$\rho(\lambda) \geq 0, \qquad \int_\Lambda d\lambda \rho(\lambda) = 1, \tag{1.42}$$

where Λ is the set of hidden variables.

The LHVT defined above aim to include general theories satisfying local causality and the EPR criterion of reality. The outcome at one laboratory is independent of the measurement choice made at the other laboratory, if the experiments are performed at space-like separations, as required by local causality. The measured properties have elements of physical reality, hence, the outcomes are predetermined, at least probabilistically, by the values of the hidden variables λ.

We define the correlation $C(A, B)$ as the average value of the product of Alice's and Bob's outcomes in experiments in which the measurements A and B are chosen. For a deterministic LHVT we have

$$C(A, B) = \int_{\Lambda} d\lambda \rho(\lambda) a(A, \lambda) b(B, \lambda). \tag{1.43}$$

A probabilistic LHVT predicts

$$C(A, B) = \sum_{a,b \in \{1,-1\}} ab \int_{\Lambda} d\lambda \rho(\lambda) P(a|A, \lambda) P(b|B, \lambda). \tag{1.44}$$

There are quantum correlations obtained in the EPR-Bohm experiment that cannot be described by the general form (1.44) predicted by LHVT. Thus, we can state Bell's theorem as follows.

Bell's Theorem. *There exist predictions of quantum mechanics that are inconsistent with the predictions of local hidden variable theories.*

Bell's theorem is most easily shown by the quantum violation of some inequalities, the *Bell inequalities*, which are satisfied by LHVT. An important Bell inequality is the CHSH inequality.

1.3.1.3 The CHSH Inequality

The correlations described by LHVT in the EPR-Bohm experiment satisfy the *CHSH inequality* [42]:

$$|I_2| \equiv \left| C(0,0) + C(1,1) + C(1,0) - C(0,1) \right| \leq 2\,. \tag{1.45}$$

We first show this inequality for deterministic LHVT. We have that

$$\begin{aligned}
|I_2| &= \left|\int_\Lambda d\lambda\rho(\lambda)\big[a(0,\lambda)b(0,\lambda)+a(1,\lambda)b(1,\lambda)+a(1,\lambda)b(0,\lambda)-a(0,\lambda)b(1,\lambda)\big]\right| \\
&\leq \int_\Lambda d\lambda\rho(\lambda)\Big|a(0,\lambda)\big[b(0,\lambda)-b(1,\lambda)\big]+a(1,\lambda)\big[b(1,\lambda)+b(0,\lambda)\big]\Big| \\
&\leq \int_\Lambda d\lambda\rho(\lambda)\Big[\big|a(0,\lambda)\big|\big|b(0,\lambda)-b(1,\lambda)\big|+\big|a(1,\lambda)\big|\big|b(1,\lambda)+b(0,\lambda)\big|\Big] \\
&= \int_\Lambda d\lambda\rho(\lambda)\Big[\big|b(0,\lambda)-b(1,\lambda)\big|+\big|b(1,\lambda)+b(0,\lambda)\big|\Big] \\
&\leq 2, \qquad (1.46)
\end{aligned}$$

where in the first line we used (1.43) and (1.45); in the second and third lines we arranged terms and used the properties of the modulus function; in the fourth line we used that $|a(0,\lambda)| = |a(1,\lambda)| = 1$, as follows from (1.40); and in the last line we used that the value of one of the terms is zero, while the other one is 2, as obtained from (1.40).

Now we show the CHSH inequality for probabilistic LHVT [43]. From (1.44), it follows straightforwardly that

$$C(A,B) = \int_\Lambda d\lambda\rho(\lambda)\bar{a}(A,\lambda)\bar{b}(B,\lambda), \qquad (1.47)$$

where $\bar{a}(A,\lambda)$ and $\bar{b}(B,\lambda)$ are averaged values defined by

$$\bar{a}(A,\lambda) \equiv P(1|A,\lambda) - P(-1|A,\lambda), \qquad \bar{b}(B,\lambda) \equiv P(1|B,\lambda) - P(-1|B,\lambda). \quad (1.48)$$

Thus, replacing $a(A,\lambda)$ and $b(B,\lambda)$ in (1.46) by their averaged values $\bar{a}(A,\lambda)$ and $\bar{b}(B,\lambda)$, we obtain with the same procedure the corresponding first four lines of (1.46), with the equality sign replaced by $\leq$ in the fourth line due to the inequalities

$$|\bar{a}(A,\lambda)| \leq 1, \qquad |\bar{b}(B,\lambda)| \leq 1. \qquad (1.49)$$

Thus, we have

$$|I_2| \leq \int_\Lambda d\lambda\rho(\lambda)\Big[\big|\bar{b}(0,\lambda)-\bar{b}(1,\lambda)\big|+\big|\bar{b}(1,\lambda)+\bar{b}(0,\lambda)\big|\Big]. \qquad (1.50)$$

It is easy to see from (1.49) and (1.50) that

$$|I_2| \leq \int_\Lambda d\lambda \rho(\lambda) 2. \tag{1.51}$$

Finally, it follows from (1.42) that $|I_2| \leq 2$, which is the CHSH inequality (1.45).

There exist quantum states and quantum measurements for which the quantum correlations violate the CHSH inequality, up to the value $2\sqrt{2}$, as given by the Cirel'son [44] bound

$$\left|I_2^{\mathrm{Q}}\right| \leq 2\sqrt{2}, \tag{1.52}$$

where the label Q indicates that the correlations in (1.45) are quantum. Consider the singlet state quantum correlation

$$Q(\theta) = -\cos\theta, \tag{1.53}$$

where $\cos\theta = \vec{a}_A \cdot \vec{b}_B$. Let $\vec{a}_A = \cos\left(\frac{A\pi}{2}\right)\hat{z} + \sin\left(\frac{A\pi}{2}\right)\hat{x}$ and $\vec{b}_B = \cos\left(\frac{B\pi}{2} + \frac{\pi}{4}\right)\hat{z} + \sin\left(\frac{B\pi}{2} + \frac{\pi}{4}\right)\hat{x}$, for $A, B \in \{0, 1\}$. We see that $\cos\theta = \frac{1}{\sqrt{2}}$ for the pairs $(A = 0, B = 0)$, $(A = 1, B = 1)$ and $(A = 1, B = 0)$, and $\cos\theta = -\frac{1}{\sqrt{2}}$ for $(A = 0, B = 1)$. Thus, from (1.53), each term in (1.45) contributes with a value of $-\frac{1}{\sqrt{2}}$. Hence, the Cirel'son bound (1.52) is achieved by this set of measurements on the singlet state.

1.3.1.4 The Braunstein-Caves Inequality

Consider now a version of the EPR-Bohm experiment in which Alice's and Bob's measurement choices belong to a set of N possible elements: $A, B \in \{0, 1, \ldots, N-1\}$. In this case, the correlations predicted by LHVT satisfy the *Braunstein-Caves inequality* [45]:

$$|I_N| \equiv \left| \sum_{k=0}^{N-1} C(k,k) + \sum_{k=0}^{N-2} C(k+1,k) - C(0,N-1) \right| \leq 2N - 2. \tag{1.54}$$

This inequality is valid for probabilistic and deterministic LHVT. We present a proof similar to (1.46) for deterministic LHVT:

$$\begin{aligned}
|I_N| &= \left| \int_\Lambda d\lambda \rho(\lambda) \left[\sum_{k=0}^{N-1} a(k,\lambda) b(k,\lambda) + \sum_{k=0}^{N-2} a(k+1,\lambda) b(k,\lambda) - a(0,\lambda) b(N-1,\lambda) \right] \right| \\
&\leq \int_\Lambda d\lambda \rho(\lambda) \left| a(0,\lambda) \big[b(0,\lambda) - b(N-1,\lambda) \big] + \sum_{k=1}^{N-1} a(k,\lambda) \big[b(k,\lambda) + b(k-1,\lambda) \big] \right| \\
&\leq \int_\Lambda d\lambda \rho(\lambda) \left[\big| a(0,\lambda) \big| \big| b(0,\lambda) - b(N-1,\lambda) \big| + \sum_{k=1}^{N-1} \big| a(k,\lambda) \big| \big| b(k,\lambda) + b(k-1,\lambda) \big| \right] \\
&= \int_\Lambda d\lambda \rho(\lambda) \left[\big| b(0,\lambda) - b(N-1,\lambda) \big| + \sum_{k=1}^{N-1} \big| b(k,\lambda) + b(k-1,\lambda) \big| \right] \\
&\leq 2N-2, \qquad (1.55)
\end{aligned}$$

where in the first line we used (1.43) and (1.54); in the second and third lines we arranged terms and used the properties of the modulus function; in the fourth line we used that $|a(A,\lambda)| = 1$, as follows from (1.40); and in the last line we used that at least one of the terms in the fourth line is zero, while the other $N-1$ are not bigger than 2, as follows from (1.40), for example, all the right hand side terms contribute with a value of 2 if and only if all the terms $b(k,\lambda)$ are equal for $k = 0, 1, \ldots, N-1$, which implies that $b(0,\lambda) - b(N-1,\lambda) = 0$.

We see that the CHSH inequality (1.45) is a special case of the Braunstein-Caves inequality (1.54) with $N = 2$. There exist quantum states and measurements for which the quantum correlations violate the Braunstein-Caves inequality, up to the bound [46]:

$$\big| I_N^{\mathrm{Q}} \big| \leq 2N \cos\Big(\frac{\pi}{2N} \Big), \qquad (1.56)$$

where the label Q indicates that the correlations in (1.54) are quantum. For example, if Alice's and Bob's qubits are in the singlet state and their measurements are given by the Bloch vectors $\vec{a}_A = \cos\big(\frac{A\pi}{N}\big)\hat{z} + \sin\big(\frac{A\pi}{N}\big)\hat{x}$ and $\vec{b}_B = \cos\big(\frac{B\pi}{N} + \frac{\pi}{2N}\big)\hat{z} + \sin\big(\frac{B\pi}{N} + \frac{\pi}{2N}\big)\hat{x}$, for $A, B \in \{0, 1, \ldots, N-1\}$, it is straightforward to obtain from (1.53) and (1.54) that the equality is achieved in (1.56).

In chapter 2, we introduce a Bell inequality that generalizes the CHSH and Braunstein-Caves inequalities in the following sense. Instead of restricting Alice's

and Bob's measurement choices to a finite set, we allow them to choose any qubit projective measurements defined by Bloch vectors $\vec{a}$ and $\vec{b}$. However, we constrain these vectors to be separated by a fixed angle θ, hence, $\cos\theta = \vec{a} \cdot \vec{b}$.

1.3.1.5 Bell Experiments and Loopholes

The prediction of quantum mechanics that the Bell inequalities are violated has been verified experimentally. Particularly, the violation of the CHSH inequality has been observed in several experiments [47–55].[1] Ideally, this would rule out any possible description of the experimental results in terms of local hidden variable models. However, the Bell experiments performed so far have had deficiencies called *loopholes*, which allow us to describe the experiments in terms of local hidden variable models that exploit such loopholes. There are three main loopholes: the *locality* loophole [58, 59], the *detector efficiency* loophole [60] and the *collapse locality* loophole [61].

In the locality loophole, the event in which a measurement choice is made at Alice's laboratory and the event in which an outcome is obtained at Bob's laboratory are not space-like separated. Thus, if the locality loophole is not closed, the experimental results can be described by a local hidden variable model in which a signal travelling not faster than light from Alice's to Bob's laboratory that indicates the measurement choice at Alice's location influences the outcome obtained at Bob's location, and vice versa. The locality loophole remained open during the first experimental violations of the Bell inequalities, because the measurements were kept fixed during a whole run of the experiment [47, 48]. In a further experiment, the measurements were chosen by a pseudo-random genera-

[1] To be more precise, a different version of the CHSH inequality (1.45) deduced in the same paper by Clauser, Horne, Shimony and Holt [42], and investigated further by Clauser and Horne [56], was tested in experiments [47, 49]. Such a version of the CHSH inequality is particularly suitable for an experimental set up with photons and polarizers in which only the outcomes $a = 1$ and $b = 1$ can be recorded, these corresponding to photons passing through polarizers at Alice's and Bob's laboratories, respectively. The outcomes $a = -1$ and $b = -1$ cannot be detected because these correspond to photons being blocked by the polarizers. This difficulty was removed in other experiments [48, 50–54] in which both possible outcomes $a = \pm 1$ and $b = \pm 1$ were measured, for example by using two-channel polarizers instead of ordinary polarizers in experiments with photons. Thus, these later experiments tested version (1.45) of the CHSH inequality. The experiment [55] tested a different version [57] of the CH inequality [56].

tor [49]. Although this was an improvement, the locality loophole was not closed completely, because the generator worked at a fixed sinusoidal frequency and thus was not truly random. In two later experiments, the measurements were selected according to the outcome of a quantum measurement, using a beam splitter to measure the polarization of a photon. In one experiment, the photons were separated by 400 m across the Innsbruck University science campus [51]. In the other experiment, the photons were sent from Geneva to the villages of Bellevue and Bernex, which are separated by 10.9 km [50, 62]. It is claimed that these experiments closed the locality loophole, because according to quantum mechanics, the outcome of a measurement of the polarization of a photon, which was used to choose what measurements to perform in the Bell experiment, is a totally random event,[1] which cannot be determined before the measurement is performed. Nevertheless, we must say that there is still the logical possibility that the outcomes of a quantum measurement are predetermined by a hidden variables theory, in which case the outcomes of a quantum measurement are not truly random events and hence the locality loophole is still open in this case. Moreover, it is logically possible that any apparently random event, given for example by a quantum measurement outcome or a human "free" choice, is predetermined by a hidden variables theory [58]. According to this possibility, closing the locality loophole is an impossible task, because any measurement choice made at Alice's laboratory is predetermined, and thus a signal travelling not faster than light from Alice's to Bob's location, indicating this predetermined choice, can influence the measurement outcome at Bob's laboratory.

In the detector efficiency loophole, also called the detection loophole, the detector efficiencies are small enough that LHV models can describe the observed correlations. The experimental result of a projective measurement on a qubit consists in a detection of the qubit system after it has passed through a measurement process. For example, if the qubit consists in the polarization of a photon, the photon goes through a beam splitter, whose orientation defines the performed measurement, which divides the photon trajectory into two possible paths ending each at a photon detector. The measurement outcome is recorded according

[1] We are considering here that the measured photon is initially prepared in an equal superposition of the orthogonal polarizations being measured.

to which detector is activated. Ideally, all pairs of entangled photons that are sent to the corresponding laboratories should activate a detection. However, the detection efficiency achieved in the experiments is not perfect. Therefore, it is a common practice to assume that the statistics of the detected particles are the same as the statistics of all the created particles; this is the *fair sampling assumption*. However, if the detector efficiencies are small enough, the experimentally observed correlations can be reproduced by LHV models in which the detection statistics are affected by the hidden variables [60]. A minimum detection efficiency of $2(\sqrt{2}-1) = 0.828$ [63] is required to close this loophole in the EPR-Bohm experiment, in which the pair of measured qubits are in a singlet state. The detection loophole can be closed with a smaller detection efficiency, with a minimum value of $\frac{2}{3}$, if the quantum state is optimized, interestingly to a non-maximally entangled state [57]. Some experiments have closed the detector efficiency loophole [52, 53, 55], but have left the locality loophole open. On the other hand, the Innsbruck and the Geneva experiments, which closed the locality loophole, left the detection loophole open, because their detector efficiencies were not big enough; the detector efficiency was only 0.05 in the Innsbruck experiment. In fact, no Bell experiment performed so far has been able to close both the detector efficiency and the locality loopholes. Given that the locality loophole has only been closed with photons and that recent experiments [55] with photons achieved to close the detection loophole, it is reasonable to expect that both the detection and the locality loopholes will be closed in the near future in a Bell experiment with photons.

The collapse locality loophole is based on the idea that the *collapse* of the quantum state, also called *state vector reduction* or collapse of the wave function, in a quantum measurement is a well defined physical process. If a measurement event is not instantaneous, but takes a finite time due to the physical collapse of the quantum state, then there can be a signal, travelling not faster than light, departing from Alice's laboratory indicating her measurement choice that arrives to Bob's laboratory after a particle has entered his measurement apparatus, but before its quantum state collapse is completed, and vice versa. In this case, the measurements could seem to be space-like separated if state vector reduction were not considered, but would in fact be time-like separated if the collapse of the

quantum state were a physical process that takes a finite time to be completed. In order to close the collapse locality loophole, it is necessary to have a theory for the state vector reduction. One suggestion is that gravity induces the collapse of the quantum state [64–66]. According to gravity induced collapse models, the sate vector reduction is completed when a superposition state of significantly different configurations of massive objects is achieved. The violation of a Bell inequality was observed in an experiment [54, 67] that closed the collapse locality loophole, assuming these collapse models. The collapse locality loophole remains open for other models of state vector reduction. Independently of the collapse model under consideration, it is argued that a collapse should not last longer than the time that takes for a human brain to register a measurement result, which is of the order of 0.1 seconds [61]. Thus, a Bell experiment in which Alice's and Bob's laboratories are separated by 0.1 light seconds would be able to close the collapse locality loophole completely. This distance is four orders of magnitude bigger than the biggest separation between the laboratories achieved by the Bell experiments performed so far, which is 18 km [54].

1.3.2 The No-Signalling Principle

In the previous sections we have seen that according to relativity, local causality is a sensible assumption for a physical theory. However, local hidden variable theories, which aim to include all hypothetical physical theories satisfying EPR's criterion of reality and local causality predict the satisfaction of Bell inequalities, which can be violated by quantum mechanics, and whose violation has been verified experimentally. In this section we show that quantum mechanics is still consistent with relativity by satisfaction of the no-signalling principle, which is a stronger version of the following principle:

No-Superluminal Signalling (NSLS). *Information cannot be communicated at a speed higher than the speed of light in the vacuum.*

According to relativity theory, no-superluminal signalling is a necessary condition for satisfaction of causality. If superluminal signalling were possible, causality would be violated, as illustrated in Figure 1.3 [68].

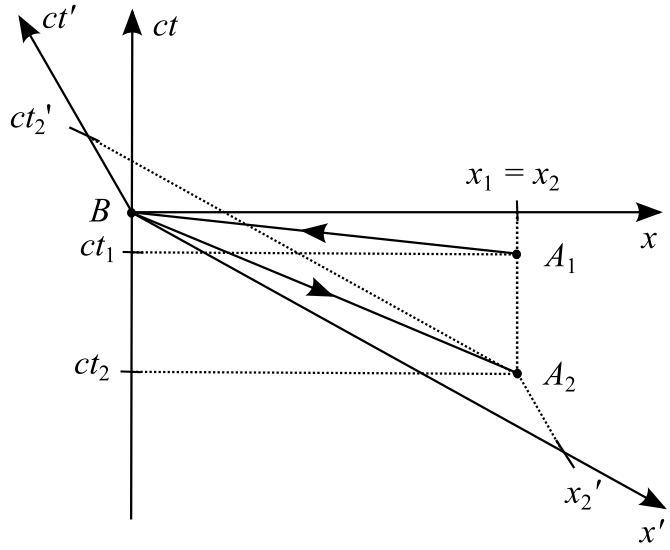


Figure 1.3: Spacetime diagram showing that superluminal signalling leads to violation of relativistic causality. Consider that Alice and Bob are at distant locations and that they have devices that allow them to send messages to each other at a speed $w > c$, where c is the speed of light in the vacuum. Alice is moving at a constant speed v away from Bob, with $0 < v < c$. Alice (Bob) is at rest in the unprimed (primed) reference frame. The events $A_1 = (x_1, ct_1)$, $B = (0, 0)$ and $A_2 = (x_2, ct_2)$ correspond to Alice sending Bob a message at speed w, Bob receiving Alice's message and sending Alice a message at speed w, in his rest frame, and Alice receiving Bob's message, respectively. Applying the corresponding Lorentz transformations, it is straightforward to show that for v big enough, but still satisfying $v < c$, we have that $t_2 < t_1$, that is, Alice receives Bob's message before she has sent hers to Bob. This is a violation of causality, because the effect, Alice receiving a reply from Bob, precedes the cause, Alice sending a message to Bob. Logical contradictions can arise. For example, if Alice's message indicates what is happening in her present and Bob's message is just a copy of Alice's message, Alice learns from Bob's message what will happen in her future; then, Alice can take appropriate actions to change her future, which means that the message she receives from Bob should be different.

Quantum mechanics satisfies the following principle, which is a stronger version of no-superluminal signalling.

The No-Signalling Principle (NS). *A party, Alice, cannot communicate any information to another distant party, Bob, if Alice does not transmit any physical systems to Bob.*

An interesting question is, if Alice does send Bob a physical system, how much information can the transmitted system fundamentally communicate? This question is discussed in chapter 4, in which an extension of the no-signalling principle, quantum information causality, is presented.

Satisfaction of NS implies satisfaction of NSLS. This is seen as follows. According to NS, Alice can communicate information to a distant party, Bob, only if she sends him a physical system. Therefore, since according to relativity, no physical system can travel faster than light, satisfaction of NS implies that Alice cannot communicate any information to Bob at a speed higher than the speed of light, which is NSLS. However, satisfaction of NSLS does not necessarily imply satisfaction of NS. Suppose that Alice and Bob have devices that allow them to communicate at a speed not higher than the speed of light, but these devices do not require the transmission of any physical systems. In this case NSLS is satisfied but NS is violated.

The no-signalling principle can be stated mathematically in terms of some conditions on probability distributions. Consider the general situation in which Alice and Bob try to communicate by using some devices without the transmission of any physical systems. Alice has a message A that she wants to communicate Bob. Similarly, Bob has a message B that she wants to communicate Alice. Alice and Bob choose their messages from sets $\mathcal{A}$ and $\mathcal{B}$, respectively. Alice's and Bob's devices output respective values $r \in \mathcal{R}$ and $s \in \mathcal{S}$. These devices are usually called *correlation boxes*. The correlation boxes are defined by their outcome probabilities $P(r, s|A, B)$. Alice and Bob can use their boxes several times; or they can use them only once, but they have access to several pairs of identical boxes. The boxes satisfy the no-signalling principle if Alice cannot infer Bob's message from her outcome probabilities, and similarly for Bob. This means that Alice's (Bob's) outcome probabilities are independent of Bob's (Alice's) inputs.

These *no-signalling conditions* are

$$\begin{aligned}\sum_{s\in\mathcal{S}} P(r,s|A,B) &= \sum_{s\in\mathcal{S}} P(r,s|A,B') \equiv P(r|A), \quad \forall B,B'\in\mathcal{B},\ r\in\mathcal{R},\ A\in\mathcal{A},\\ \sum_{r\in\mathcal{R}} P(r,s|A,B) &= \sum_{r\in\mathcal{R}} P(r,s|A',B) \equiv P(s|B), \quad \forall A,A'\in\mathcal{A},\ s\in\mathcal{S},\ B\in\mathcal{B}.\end{aligned} \tag{1.57}$$

A *quantum box* corresponds to the probability distribution $P(r,s|A,B)$ of a quantum measurement. In this case, the inputs correspond to measurements implemented on a quantum state and the outputs correspond to the measurement outcomes. Quantum mechanics satisfies the no-signalling principle, as we show below [69].

Consider a quantum system composed of two subsystems, '1' and '2', at different locations in a quantum state with density matrix $\rho_{12}\in\mathcal{D}(\mathcal{H}_1\otimes\mathcal{H}_2)$. Alice has system 1 and Bob has system 2. Alice and Bob apply measurements labelled by $A\in\mathcal{A}$ and $B\in\mathcal{B}$, respectively. Alice's (Bob's) measurement A (B) consists of a set of measurement operators M_r^A (M_s^B) acting on $\mathcal{H}_1$ ($\mathcal{H}_2$), where $r\in\mathcal{R}$ ($s\in\mathcal{S}$) is Alice's (Bob's) outcome. The outcome probabilities are given by

$$P(r,s|A,B) = \mathrm{Tr}\Big(\big(M_r^A\otimes M_s^B\big)\rho_{12}\big(M_r^A\otimes M_s^B\big)^\dagger\Big). \tag{1.58}$$

These satisfy the no-signalling conditions (1.57), as we show:

$$\begin{aligned}\sum_{s\in\mathcal{S}} P(r,s|A,B) &= \sum_{s\in\mathcal{S}} \mathrm{Tr}\Big(\big(M_r^A\otimes M_s^B\big)\rho_{12}\big(M_r^A\otimes M_s^B\big)^\dagger\Big)\\ &= \sum_{s\in\mathcal{S}} \mathrm{Tr}\Big(\Big(\big(M_r^{A\dagger}M_r^A\big)\otimes\big(M_s^{B\dagger}M_s^B\big)\Big)\rho_{12}\Big)\\ &= \mathrm{Tr}\Big(\Big(\big(M_r^{A\dagger}M_r^A\big)\otimes\sum_{s\in\mathcal{S}}\big(M_s^{B\dagger}M_s^B\big)\Big)\rho_{12}\Big)\\ &= \mathrm{Tr}\Big(\Big(\big(M_r^{A\dagger}M_r^A\big)\otimes I_2\Big)\ \rho_{12}\Big),\end{aligned} \tag{1.59}$$

where in the second line we used the cyclicity of the trace, in the third line we used the linearity of the trace, in the fourth line we used the completeness equation

(1.3), and I_2 denotes the identity acting on $\mathcal{H}_2$. Thus, we see that the right hand side of the previous expression is independent of B, as required by (1.57). In a similar way we obtain that

$$\sum_{r\in\mathcal{R}} P(r,s|A,B) = \mathrm{Tr}\bigg(\Big(I_1 \otimes \big(M_s^{B\dagger} M_s^B\big)\Big)\ \rho_{12}\bigg), \tag{1.60}$$

where I_1 denotes the identity acting on $\mathcal{H}_1$. Thus, the right hand side of the previous expression is independent of A, as required. The expressions (1.59) and (1.60) can be stated in the simpler form

$$\begin{aligned} P(r|A) &= \mathrm{Tr}\big(M_r^A \rho_1 M_r^{A\dagger}\big), \\ P(s|B) &= \mathrm{Tr}\big(M_s^B \rho_2 M_s^{B\dagger}\big), \end{aligned} \tag{1.61}$$

where we have used the cyclicity of the trace and the definitions (1.57), $\rho_1 \equiv \mathrm{Tr}_2(\rho_{12})$, and $\rho_2 \equiv \mathrm{Tr}_1(\rho_{12})$.

An application of the no-signalling principle that is useful in chapters 3 and 4 considers the following situation. Alice and Bob are at different locations and share an arbitrary quantum state. Alice is given a random message from a set of N elements. Alice and Bob perform an arbitrary quantum strategy using their quantum state, but without the transmission of any physical systems, with the goal that Bob guesses the message given to Alice. According to the no-signalling principle, since Alice does not send Bob any physical systems, Bob cannot obtain any information about Alice's message. Since the message given to Alice is chosen randomly from a set of N elements, that is, with a probability $\frac{1}{N}$, the no-signalling principle implies that Bob can only guess it with probability $\frac{1}{N}$. This can be shown using the no-signalling conditions (1.57), as follows.

A general quantum strategy performed by Alice and Bob in which no physical systems are transmitted consists of quantum measurements $A \in \mathcal{A}$ and $B \in \mathcal{B}$ performed by Alice and Bob, respectively, on a shared entangled state. Alice and Bob obtain respective outcomes $r \in \mathcal{R}$ and $s \in \mathcal{S}$. Alice's measurement choice A encodes the received message, hence, $|\mathcal{A}| = N$. Bob's outcome s corresponds to his guess of Alice's message A, hence, the elements of $\mathcal{S}$ are in one to one correspondence with the elements of $\mathcal{A}$. Therefore, without loss of generality, we

assume that $\mathcal{A} = \mathcal{S}$. Thus, the probability that Bob outputs the correct message is

$$P_{\text{guess}} = \sum_{x \in \mathcal{A}} P(s = x|B, A = x)P(A = x). \tag{1.62}$$

The no-signalling conditions (1.57) state that Bob's outcome probabilities are independent of Alice's measurement. Therefore, $P(s = x|B, A = x) = P(s = x|B)$ for all $x \in \mathcal{A}$ and $B \in \mathcal{B}$, which from (1.62) implies that

$$\begin{aligned} P_{\text{guess}} &= \sum_{x \in \mathcal{A}} P(s = x|B)P(A = x) \\ &= \frac{1}{N} \sum_{x \in \mathcal{A}} P(s = x|B) \\ &= \frac{1}{N}, \end{aligned} \tag{1.63}$$

where in the second line we used that the message given to Alice is random and in the third line we used the normalization of probabilities.

In the following sections we discuss some implications of the no-signalling principle for the violation of the CHSH inequality (section 1.3.2.1) and for some quantum information tasks (section 1.3.2.2).

1.3.2.1 No-Signalling and the CHSH Inequality

An interesting question to ask is, why does not quantum mechanics violate the CHSH inequality up to the maximum possible algebraic value of 4? An interesting hypothesis is that the no-signalling principle restricts the maximum violation of the CHSH inequality up to the Cirel'son bound. This was shown to be false because there exist theoretical correlation systems, the *PR boxes*, which violate the CHSH inequality up to the value of 4 and still satisfy the no-signalling principle [70]. It was shown later that an extension of the no-signalling principle, the information causality principle [71], does imply the Cirel'son bound, as discussed in chapter 4. A different approach to this question is given in [72].

In order to present the PR boxes, it is convenient to translate the EPR-Bohm experiment into an informational task, usually called the *CHSH game*. Alice and Bob are at different locations and share a pair of correlated boxes defined by their

joint outcome probabilities $P(r,s|A,B)$. Alice (Bob) randomly chooses a value $A \in \mathcal{A}$ ($B \in \mathcal{B}$) and inputs this into her (his) box, which then outputs a value $r \in \mathcal{R}$ ($s \in \mathcal{S}$), with $\mathcal{A} = \mathcal{B} = \mathcal{R} = \mathcal{S} = \{0,1\}$. The game's goal is that their outputs satisfy $r \oplus s = AB$, where $\oplus$ denotes sum modulo 2. Thus, we define the success probability in the CHSH game by

$$P_{\text{CHSH}} \equiv P(r \oplus s = AB). \tag{1.64}$$

We show below that the CHSH inequality and the Cirel'son bound impose bounds on P_{CHSH} when the boxes are described by LHVT and by quantum mechanics, respectively. To do so, we associate the EPR-Bohm experiment and the CHSH game according to the following relations:

$$r \equiv \frac{1-a}{2}, \qquad\qquad s \equiv \frac{1-b}{2}. \tag{1.65}$$

We show at the end of this section that the CHSH quantity I_2 and the success probability P_{CHSH} satisfy the relation

$$P_{\text{CHSH}} = \frac{1}{2} + \frac{I_2}{8}. \tag{1.66}$$

Using the relation (1.66), the CHSH inequality (1.45) and the Cirel'son bound (1.52), it follows that the success probabilities $P^{\text{L}}_{\text{CHSH}}$ and $P^{\text{Q}}_{\text{CHSH}}$ achieved by LHV correlations and quantum correlations in the CHSH game, respectively, satisfy the following inequalities:

$$\frac{1}{4} \leq \quad P^{\text{L}}_{\text{CHSH}} \quad \leq \frac{3}{4}, \tag{1.67}$$

$$\frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \leq \quad P^{\text{Q}}_{\text{CHSH}} \quad \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right). \tag{1.68}$$

The *PR box* [70] is defined by the following outcome probabilities $P(r,s|A,B)$:

$$\begin{aligned} P(0,0|0,0) &= P(1,1|0,0) = P(0,0|0,1) = P(1,1|0,1) = P(0,0|1,0) \\ &= P(1,1|1,0) = P(0,1|1,1) = P(1,0|1,1) = \frac{1}{2}, \end{aligned} \tag{1.69}$$

with all other outcome probabilities equal to zero. Is is easy to see that the PR box achieves $P_{\text{CHSH}} = 1$. The PR box satisfies the no-signalling conditions (1.57):

$$\begin{aligned} \sum_{s=0}^{1} P(r,s|A,0) &= \sum_{s=0}^{1} P(r,s|A,1) \equiv P(r|A), \\ \sum_{r=0}^{1} P(r,s|0,B) &= \sum_{r=0}^{1} P(r,s|1,B) \equiv P(s|B), \end{aligned} \tag{1.70}$$

for $r, s, A, B \in \{0, 1\}$.

Similarly, if we relabel $r \to r \oplus 1$, we obtain a non-signalling probability distribution for which $P_{\text{CHSH}} = 0$. Thus, the no-signalling principle does not impose any restrictions on the success probability in the CHSH game or in the maximum violation of the CHSH inequality.

We complete this section by showing (1.66). First, a general average correlation in terms of the probabilities of the outcomes $a, b \in \{1, -1\}$, when measurements A and B are chosen, is

$$C(A,B) \equiv \sum_{a,b\in\{1,-1\}} abP(a,b|A,B). \tag{1.71}$$

Second, using the change of variables (1.65), the correlation is

$$C(A,B) \equiv \sum_{r,s\in\{0,1\}} (-1)^{r\oplus s} P(r,s|A,B). \tag{1.72}$$

Third, after relabelling $A \to A \oplus 1$, the CHSH quantity (1.45) is

$$I_2 \equiv \sum_{A,B\in\{0,1\}} (-1)^{AB} C(A,B). \tag{1.73}$$

We notice that the CHSH inequality (1.45) is still satisfied because we have only changed the measurement labels. From (1.72) and (1.73), the CHSH quantity is

$$I_2 \equiv \sum_{A,B,r,s\in\{0,1\}} (-1)^{r\oplus s\oplus AB} P(r,s|A,B). \tag{1.74}$$

Finally, noting that by definition of the CHSH game, the measurements are chosen randomly, $P(A,B) = \frac{1}{4}$, we have

$$\begin{aligned} \frac{I_2}{4} &= \sum_{A,B,r,s\in\{0,1\}} (-1)^{r\oplus s\oplus AB} P(r,s|A,B)P(A,B). \\ &= P(r\oplus s = AB) - P(r\oplus s \neq AB) \\ &= 2P_{\text{CHSH}} - 1, \end{aligned} \tag{1.75}$$

where in the third line we used the normalization of probabilities and the definition (1.64). Thus, the relation (1.66) follows.

1.3.2.2 No-Signalling and Quantum Information

The no-signalling principle has important implications for quantum information processing tasks. The no-cloning theorem was first noticed after a publication claiming a procedure for superluminal communication between distant parties with access to a hypothetical machine that could produce perfect copies of an unknown quantum state [38]. Since superluminal communication is not possible by any quantum process, the assumption of a perfect quantum cloning machine is false. The no-cloning theorem was shown after such a claim for superluminal communication. In fact, the maximum fidelity $f = \frac{5}{6}$ achieved by a cloning machine of qubit states, as mentioned in section 1.2.4.1, can be deduced from the no-signalling principle [37]. There are other important implications of the no-signalling principle for quantum information tasks. The security of quantum key distribution for eavesdroppers not restricted by quantum mechanics is obtained from the violation of a Bell inequality and satisfaction of the no-signalling principle [27]. The maximum guessing probability in quantum state discrimination can be derived from the no-signalling principle [73]. We discuss below a few other quantum information tasks that are constrained by the no-signalling principle.

An interesting extension of the no-cloning theorem to relativistic quantum mechanics is the *no-summoning theorem* [74], which guarantees the security of a quantum relativistic protocol for bit commitment [75] and has application to other quantum information tasks [76]. Consider the following task called *summoning*. Alice gives Bob a quantum state ρ at a point P in space-time. The state ρ is known

by Alice but unknown by Bob. Alice and Bob agree in advance that Alice will ask the state back from Bob at a space-time point Q that is time-like separated from P and that Alice will choose from some set Ω with some probability distribution p_Q. Bob succeeds in this task if he gives Alice a copy of ρ at the spacetime point Q. Consider the example in one spatial dimension in which $P = (0, 0)$, $\Omega = \{Q_0, Q_1\}$, $Q_i = (x_i, ct)$ and $p_{Q_i} = \frac{1}{2}$ for $i = 0, 1$, with $x_0 = -ct$, $x_1 = ct$ and $t > 0$. The no-summoning theorem states that Bob cannot succeed with probability equal to unity. The proof follows straightforwardly from the no-signalling principle and the no-cloning theorem. A general quantum strategy performed by Bob includes a quantum measurement on the received state ρ together with some ancillary system, whose outcome is sent at the speed of light to space-time points Q_i and is used to obtain a quantum state ρ_i at point Q_i, for $i = 0, 1$. If Alice announces that she wants the state ρ back at the spacetime point Q_i, Bob succeeds in the task if $\rho_i = \rho$. From the no-signalling principle, the state ρ_0 is independent of whether or not Alice chooses to ask the state back at Q_1, and similarly for ρ_1. Thus, the only way for Bob to succeed for both of Alice's possible asked points Q_0 and Q_1 is that $\rho_0 = \rho_1 = \rho$, but this is impossible according to the no-cloning theorem.

Other important quantum information tasks restricted by the no-signalling principle are *instantaneous nonlocal quantum computation* (INLQC) and *instantaneous nonlocal measurements* (INLM) [77–85]. In an INLQC, a distributed input quantum state $|\psi\rangle \in \mathcal{H}$ is transformed into $U|\psi\rangle$ up to local errors that are corrected after a single round of communication by the parties sharing the state $|\psi\rangle$, where U is a given nonlocal unitary acting on $\mathcal{H}$ (see Figure 1.4). The no-signalling principle requires that this task is completed with at least one round of communication. The word *instantaneous* means that, in principle, Alice's and Bob's local operations on $|\psi\rangle$ can be performed in an arbitrarily short time.

An INLM is the measurement of a nonlocal variable O on a distributed quantum state $|\psi\rangle \in \mathcal{H}$ among distant parties that is completed after a single round of communication among the parties sharing the state $|\psi\rangle$. Consider the bipartite case in which $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. One party, Alice, has the system A and the other party, Bob, has the system B. A nonlocal variable O consists of a Hermitian operator acting on $\mathcal{H}$ that cannot be written as $O_A \otimes O_B$, with O_A and O_B acting

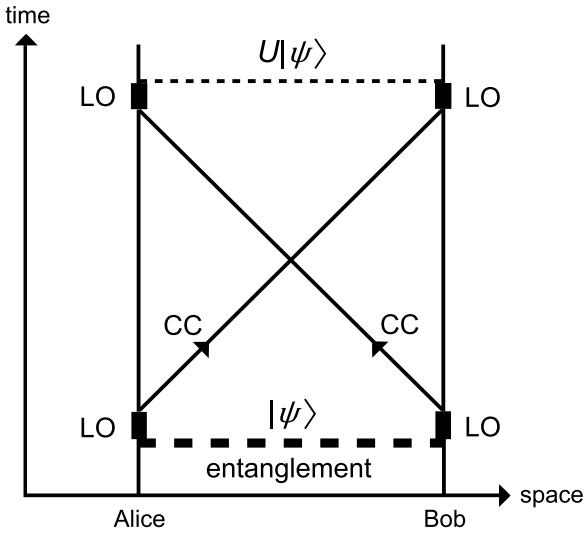


Figure 1.4: In an instantaneous nonlocal quantum computation, a given nonlocal unitary U is applied to a distributed quantum state $|\psi\rangle$ after a single round of classical communication (CC) between the parties (Alice and Bob) sharing the state. The protocol consists of local operations (LO), which include measurements, on $|\psi\rangle$ and shared entanglement, communication of the measurement results and further local operations.

on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. The measurement of the variable O gives as a result the eigenvalue of O in the state $|\psi\rangle$, with a probability distribution given by the Born rule if $|\psi\rangle$ is in a superposition of eigenstates of O. In general, the INLM consists of local operations performed by Alice and Bob, and communication between them or to a third party who learns the measurement outcome.

The no-signalling principle has implications for the nonlocal measurement process. According to the no-signalling principle, the nonlocal measurement requires at least one round of communication among the parties. As in an INLQC, the word *instantaneous* in an INLM means that, in principle, the local operations applied on $|\psi\rangle$ can be performed in an arbitrarily short time. The nonlocal measurement is conceptually easy to implement if two rounds of communication are allowed: Bob sends his part of $|\psi\rangle$ to Alice through a quantum channel or via quantum teleportation, then Alice measures the variable O in the state $|\psi\rangle$ localized at her site, and communicates the outcome to Bob. The no-signalling principle implies too that in an INLM, if the quantum state $|\psi\rangle$ is in an eigen-

state of the measured variable O, the quantum state cannot in general remain unchanged after the measurement is completed, that is, the measurement is of a *verification* (also called *demolition*) type and not of a *von-Neumann* (also called *non-demolition*) type [81–83].

An INLM can be implemented with an INLQC as follows. The unitary operation U mapping the eigenstates of the nonlocal variable to the computational basis is instantaneously applied to $|\psi\rangle$ up to local uncontrollable errors. This refers to the step in the INLQC corresponding to the local operations implemented by the parties before they perform classical communication (see Figure 1.4). Then, each party measures the transformed state in the computational basis and communicate their outcomes to the other parties. The result of the nonlocal measurement, which indicates the eigenstate of O in which $|\psi\rangle$ was previous to the nonlocal measurement, is computed from the local measurement outcomes communicated by the parties.

INLQC is possible if enough entanglement is previously distributed to the participating parties. A recursive scheme based on standard teleportation implements INLQC with an amount of entanglement growing double exponentially with the number of qubits n of the input state $|\psi\rangle$ [82, 84]. However, another scheme based on a different type of quantum teleportation protocol, denoted as port-based teleportation, implements INLQC with an amount of entanglement growing only exponentially with n [85].

INLQC has application to other distributed quantum information tasks. INLQC allows an eavesdropper to break the security of position-based quantum cryptography (PBQC) and some quantum tagging schemes [86–92]. Quantum tagging [86–89, 93] and PBQC [91, 92] are cryptographic tasks that rely on quantum information processing and relativistic constraints with the goals of verifying the location of an object and providing secure communication with a party at a given location, respectively.

In chapter 3, we derive another implication of the no-signalling principle for an important quantum information task. The maximum success probability of port-based teleportation is deduced from the no-signalling principle and a version of the no-cloning theorem.

Chapter 2

Bloch Sphere Colourings and Bell Inequalities

2.1 Introduction

As discussed in detail in section 1.3.1, the assumptions of local causality and the criterion of physical reality made by Einstein, Podolsky and Rosen [1] in their argument that quantum mechanics is an incomplete theory, led Bell [2] to introduce a mathematical description for hypothetical physical theories based on these assumptions. These local hidden variable theories (LHVT) make predictions on experiments performed at space-like separations that are inconsistent with the quantum predictions. Quantum mechanics predicts the violation of Bell inequalities, which are satisfied by LHVT. One of the Bell inequalities that has been investigated the most, both theoretically and experimentally, is the CHSH inequality [42]. The CHSH inequality considers Bohm's version [41] of the EPR thought experiment.

In the EPR-Bohm experiment, a pair of qubits is created in the singlet state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big)$ and then sent to distant laboratories. One of these laboratories is controlled by Alice and the other one by Bob. Alice (Bob) randomly chooses one of two possible measurements to perform on her (his) qubit, which we denote by $A \in \{0,1\}$ ($B \in \{0,1\}$). These are projective measurements performed by Alice (Bob) on bases defined by the Bloch vectors $\vec{a}_A$ $\big(\vec{b}_B\big)$. We

denote Alice's (Bob's) outcome as $a \in \{-1, 1\}$ ($b \in \{-1, 1\}$). An important condition is that the events at which Alice (Bob) chooses her (his) measurement and Bob (Alice) obtains his (her) outcome are space-like separated (see Figure 1.2 in section 1.3.1).

According to deterministic LHVT, Alice's (Bob's) outcome is predetermined by the value of a hidden variable λ and in general depends on her (his) measurement choice, but does not depend on Bob's (Alice's) measurement choice. Thus, according to deterministic LHVT, we have

$$a = a(A, \lambda), \qquad b = b(B, \lambda). \tag{2.1}$$

Additionally, LHVT assume the existence of a probability distribution $\rho(\lambda)$ that does not have any dependence on the measurement choices and that satisfy

$$\rho(\lambda) \geq 0, \qquad \int_{\Lambda} d\lambda \rho(\lambda) = 1, \tag{2.2}$$

where Λ is the set of hidden variables. We restrict to consider deterministic LHVT in this chapter, because probabilistic LHVT can be described by the same equations if we extend the definitions of the hidden variables for probabilistic measurement outcomes. The prediction of LHVT for the average product of Alice's and Bob's outcomes, when their measurement choices are A and B, is

$$C(A, B) = \int_{\Lambda} d\lambda \rho(\lambda) a(A, \lambda) b(B, \lambda). \tag{2.3}$$

The LHV correlations $C(A, B)$ satisfy the CHSH inequality [42]:

$$|I_2| \equiv \big|C(0,0) + C(1,1) + C(1,0) - C(0,1)\big| \leq 2\,. \tag{2.4}$$

However, the correlations predicted by quantum mechanics for the singlet state are

$$Q(\theta) = -\cos\theta, \tag{2.5}$$

where $\cos\theta = \vec{a}_A \cdot \vec{b}_B$, which can violate the CHSH inequality for appropriate sets of axes $\vec{a}_A$ and $\vec{b}_B$, up to the value $2\sqrt{2}$ given by Cirel'son's bound [44].

The quantum prediction that the CHSH inequality is violated has been verified in several experiments [47–55]. As discussed in section 1.3.1.5, there exist loopholes in the Bell experiments performed so far, which do not allow us to completely rule out descriptions of the experimental results in terms of LHVT.

An extension of the EPR-Bohm experiment in which Alice and Bob choose their measurements from sets of $N \geq 2$ elements leads to the Braunstein-Caves inequality [45]:

$$|I_N| \equiv \left| \sum_{k=0}^{N-1} C(k,k) + \sum_{k=0}^{N-2} C(k+1,k) - C(0,N-1) \right| \leq 2N-2. \tag{2.6}$$

The Braunstein-Caves inequality is satisfied by LHVT, but can be violated by quantum mechanics, up to the value $2N\cos\left(\frac{\pi}{2N}\right)$ [46]. We see that the Braunstein-Caves inequality generalizes the CHSH inequality for $N \geq 2$.

In this chapter, we explore Bell inequalities that generalize the CHSH and Braunstein-Caves inequalities, in the following sense. Alice's and Bob's choices for their projective measurements are not restricted to be in a finite set, but can take any values $\vec{a}$ and $\vec{b}$ on the Bloch sphere $\mathbb{S}^2$, with the condition that $\vec{a}$ and $\vec{b}$ are separated by a fixed angle θ so that $\vec{a}\cdot\vec{b} = \cos\theta$. Apart from this condition, the measurement axes $\vec{a}$ and $\vec{b}$ are chosen randomly. The results of this chapter correspond to work done in collaboration with Adrian Kent and has been published in [94].

2.2 Bloch Sphere Colourings and Correlation Functions

We explore LHVT in which Alice's and Bob's qubit projective measurement results are given by $a(\vec{a},\lambda)$ and $b\big(\vec{b},\lambda\big)$, respectively; where λ is a local hidden variable common to both qubits. For fixed λ, we can describe the functions a and b by two binary (black and white) colourings of spheres, associated to a and b, respectively, where black (white) represents the outcome '1' ('-1'). Different sphere colourings are associated with different values of λ. We investigate the LHV predictions by analyzing the corresponding sphere colourings. Thus, we

drop the λ-dependence and include a label x that indicates a particular pair of colouring functions $a_x(\vec{a})$ and $b_x(\vec{b})$.

A measurement along axis $\vec{a}$ with outcome 1 (-1) is equivalent to a measurement along axis $-\vec{a}$ with outcome -1 (1), and so a and b satisfy the *antipodal* property:

$$a_x(\vec{a}) = -a_x(-\vec{a}), \qquad b_x\big(\vec{b}\big) = -b_x\big(-\vec{b}\big), \tag{2.7}$$

for all $\vec{a}, \vec{b} \in \mathbb{S}^2$. We define $\mathcal{X}$ as the set of all colourings x satisfying the antipodal property.

The correlation for outcomes of measurements about randomly chosen axes separated by θ for the pair of colouring functions labelled by x is

$$C_x(\theta) = \frac{1}{8\pi^2} \int_{\mathbb{S}^2} dA a_x(\vec{a}) \int_0^{2\pi} d\omega b_x\big(\vec{b}\big), \tag{2.8}$$

where dA is the area element of the sphere corresponding to Alice's axis $\vec{a}$ and ω is an angle in the range $[0, 2\pi]$ along the circle described by Bob's axis $\vec{b}$ with an angle θ respective to $\vec{a}$ (see Figure 2.1). A general correlation is of the form

$$C(\theta) = \int_{\mathcal{X}} dx \mu(x) C_x(\theta), \tag{2.9}$$

where $\mu(x)$ is a probability distribution over $\mathcal{X}$.

Let (ϵ, ϕ) be the spherical coordinates of $\vec{a}$ and (α, β) be those of $\vec{b}$; where $\epsilon, \alpha \in [0, \pi]$ are angles from the north pole and $\phi, \beta \in [0, 2\pi]$ are azimuthal angles. The spherical coordinates (α, β) for a point $\vec{b}$ with angular coordinate ω on the circle around the axis $\vec{a}$ are:

$$\alpha = \arccos(\cos\theta\cos\epsilon - \sin\theta\sin\epsilon\cos\omega), \tag{2.10}$$

$$\beta = \left[\phi + k_\omega \arccos\Big(\frac{\cos\epsilon\sin\theta\cos\omega + \sin\epsilon\cos\theta}{\sin\alpha}\Big)\right] \bmod 2\pi, \tag{2.11}$$

where $k_\omega = 1$ if $0 \leq \omega \leq \pi$ and $k_\omega = -1$ if $\pi < \omega \leq 2\pi$. Notice that β is undefined for $\alpha \in \{0, \pi\}$.

Equations (2.10) and (2.11) can be obtained by applying three consecutive rotations around the z, y and z axes, given by $R_z(\phi)R_y(\epsilon)R_z(\omega)$, on the vectors

$\vec{a}' = \hat{z}$ and $\vec{b}' = \sin\theta\hat{x} + \cos\theta\hat{z}$, which satisfy $\vec{a}' \cdot \vec{b}' = \cos\theta$. After applying the first two rotations, the rotated vector $\vec{b}'' = R_y(\epsilon)R_z(\omega)\vec{b}'$ has the form $\vec{b}'' = \sin\alpha\cos\beta''\hat{x} + \sin\alpha\sin\beta''\hat{y} + \cos\alpha\hat{z}$. Then, we see that α is obtained from the z coordinate and β from the x coordinate by $\beta = \phi + \beta'' \bmod 2\pi$, which give Equations (2.10) and (2.11).

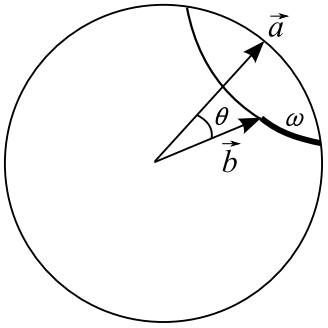


Figure 2.1: Alice's and Bob's measurement axes $\vec{a}$ and $\vec{b}$ form an angle θ. The spherical coordinates of $\vec{a}$ and $\vec{b}$ are (ϵ, ϕ) and (α, β), respectively, related by (2.10) and (2.11). Equation (2.8) computes the correlation $C_x(\theta)$ by (i) integrating the colouring function $b_x(\vec{b}\,)$ over the circle on the sphere generated by $\vec{b}$ (parameterized by the angle ω in (2.10) and (2.11)) and (ii) integrating the colouring function $a_x(\vec{a})$ over the sphere generated by $\vec{a}$. Equation (2.9) computes a general correlation $C(\theta)$ by integrating over the probability distribution $\mu(x)$ of the colourings satisfying the antipodal property, Equation (2.7).

A simple colouring of the spheres satisfying the antipodal property is one in which, for one sphere, one hemisphere is completely black and the other one is completely white, and the colouring is reversed for the other sphere. We define this to be *colouring 1*, with

$$a_1(\epsilon, \phi) = -b_1(\epsilon, \phi) = \begin{cases} 1 & \text{if } \epsilon \in \left[0, \frac{\pi}{2}\right], \\ -1 & \text{if } \epsilon \in \left(\frac{\pi}{2}, \pi\right], \end{cases} \tag{2.12}$$

for all $\phi \in [0, 2\pi]$; where we have used the spherical coordinates for vector $\vec{a}$, as introduced above.

If all colourings $x \in \mathcal{X}$ satisfy $Q_{\rho_{\mathrm{L}}}(\theta) < C^{\mathrm{L}}(\theta) \leq C_x(\theta)$ or $C_x(\theta) \leq C^{\mathrm{U}}(\theta) < Q_{\rho_{\mathrm{U}}}(\theta)$ for quantum correlations $Q_{\rho_{\mathrm{L}}}(\theta)$ and $Q_{\rho_{\mathrm{U}}}(\theta)$ obtained with particular two qubit states ρ_{U} and ρ_{L}, and some identifiable lower and upper bounds, $C^{\mathrm{L}}(\theta)$

and $C^{\mathrm{U}}(\theta)$, respectively, then a general LHV correlation $C(\theta)$ must satisfy the same inequalities. We aim here to explore this possibility via intuitive arguments and numerical and analytic results. We focus on the case $\rho_{\mathrm{L}} = |\Psi^-\rangle\langle\Psi^-|$, for which $Q_{\rho_{\mathrm{L}}}(\theta) \equiv Q(\theta) = -\cos\theta$, which is the maximum quantum anticorrelation for a given angle θ (see section 2.5 for details). We begin with some general observations.

First, we consider colouring functions $x \in \mathcal{X}$ for which the probability that Alice and Bob obtain opposite outcomes when they choose the same measurement, averaged uniformly over all measurement choices, is

$$P(a_x = -b_x|\theta = 0) = 1 - \gamma. \tag{2.13}$$

In general, $0 \leq \gamma \leq 1$. We first consider small values of γ and seek Bell inequalities distinguishing the singlet state quantum correlations from LHV correlations for which opposite outcomes are observed with probability $1 - \gamma$ when the same measurement axis is chosen by Alice and Bob. Experimentally, we can verify the violation of such Bell inequalities if the performed tests include some frequency of tests for opposite outcomes for the same axis chosen randomly, and independently for each test, by Alice and Bob. These tests of opposite outcomes allow statistical bounds on γ, which imply statistical tests for the violation of the γ-dependent Bell inequalities.

In the limiting case $\gamma = 0$, we have

$$a_x\left(\vec{a}\right) = -b_x\left(\vec{a}\right), \tag{2.14}$$

for all $\vec{a} \in \mathbb{S}^2$. This case is very interesting theoretically because we expect to prove stronger results for this case. We present some numerical results for this case in section 2.4.

Second, for any pair of colourings $x \in \mathcal{X}$ and $\theta \in [0, \pi]$, we have $C_x(\pi - \theta) = -C_x(\theta)$. This can be seen as follows. For a fixed $\vec{a}$, the circle with angle $\theta = \theta'$ around the axis $\vec{a}$, defined by the angle ω in (2.8) contains a point $\vec{b}$ that is antipodal to a point on the circle with angle $\theta = \pi - \theta'$ around $\vec{a}$. Since the colouring is antipodal, we have that the value of the integral $\int_0^{2\pi} d\omega b_x\left(\vec{b}\right)$ in (2.8)

for $\theta = \theta'$ is the negative of the corresponding integral for $\theta = \pi - \theta'$. It follows that $C_x(\pi - \theta') = -C_x(\theta')$. Therefore, in the rest of this chapter, we restrict to consider correlations for the range $\theta \in \left[0, \frac{\pi}{2}\right]$, unless otherwise stated. From the previous argument, we have $C_x\left(\frac{\pi}{2}\right) = -C_x\left(\frac{\pi}{2}\right)$, which implies that $C_x\left(\frac{\pi}{2}\right) = 0$. We also have that $C_x(0) = 1 - 2P(a_x = -b_x|\theta = 0)$, hence, from (2.13) we have that the LHVT we consider give

$$C_x(0) = -1 + 2\gamma. \tag{2.15}$$

The correlations for LHVT satisfying (2.8) and (2.13) in the case $\gamma = 0$ thus coincide with the singlet state quantum correlations for $\theta = 0$ and $\theta = \frac{\pi}{2}$, where $Q(0) = C_x(0) = -1$ and $Q\left(\frac{\pi}{2}\right) = C_x\left(\frac{\pi}{2}\right) = 0$.

Third, consider colouring 1, defined by (2.12). We have

$$C_1(\theta) = -\left(1 - \frac{2\theta}{\pi}\right), \tag{2.16}$$

for $\theta \in \left[0, \frac{\pi}{2}\right]$. This is easily seen as follows. For any two different points on the spheres defining colouring 1, $\vec{a}$ in one sphere and $\vec{b}$ in the oppositely coloured one, an arc of angle π of the great circle passing through $\vec{a}$ and $\vec{b}$ is completely black and the other arc of angle π is completely white. Thus, given that the pair of vectors $\vec{a}$ and $\vec{b}$ are chosen randomly, subject to the constraint of angle separation θ, the probability that both $\vec{a}$ and $\vec{b}$ are in oppositely coloured regions is $P(a_1 = -b_1|\theta) = \frac{\pi-\theta}{\pi} = 1 - \frac{\theta}{\pi}$. Thus, the correlation $C_1(\theta) = 1 - 2P(a_1 = -b_1|\theta)$ is given by Equation (2.16). We see that $C_1(\theta)$ linearly interpolates between the values at $C_1(0) = -1$, which is common to all colourings with $\gamma = 0$, and $C_1\left(\frac{\pi}{2}\right) = 0$, which is common to all colourings $x \in \mathcal{X}$, and we have $0 > C_1(\theta) > Q(\theta)$ for $\theta \in \left(0, \frac{\pi}{2}\right)$.

In the following sections, we motivate and explore the hypothesis that colouring 1 gives the maximum LHV anticorrelation for a continuous range of $\theta > 0$.

2.3 The Hemispherical Colouring Maximality Hypothesis

In this section, we motivate and state *strong* and *weak* forms of the *hemispherical colouring maximality hypothesis* that, for a continuous range of $\theta > 0$, the maximum LHV anticorrelation is obtained by colouring 1, defined by (2.12).

We first consider the following lemmas.

Lemma 2.1. *For any colouring $x \in \mathcal{X}$ satisfying (2.13) and any $\theta \in \left(0, \frac{2\pi}{3}\right]$, we have $-1 + \frac{2}{3}\gamma \leq C_x(\theta) \leq \frac{1}{3} + \frac{2}{3}\gamma$.*

Proof. From the CHSH inequality,

$$\left|C(0,0) + C(1,1) + C(1,0) - C(0,1)\right| \leq 2\,,$$

in the case in which the measurements $A = 0$, $A = 1$ and $B = 0$ correspond to projections on states with Bloch vectors separated from each other by the same angle $\theta \in \left(0, \frac{2\pi}{3}\right]$, Bob's measurement $B = 1$ is the same as Alice's measurement $A = 0$ and the outcomes are described by LHVT satisfying (2.8), we obtain after averaging over random rotations of the Bloch sphere that

$$|3C_x(\theta) - C_x(0)| \leq 2.$$

Then, the result follows from (2.15):

$$C_x(0) = -1 + 2\gamma,$$

which holds for all $x \in \mathcal{X}$ satisfying (2.13). □

Remark 2.1. Unsurprisingly, since small γ implies near-perfect anticorrelation at $\theta = 0$, we see that for $\theta \in \left(0, \frac{2\pi}{3}\right]$ and γ small there are no colourings with very strong correlations. However, strong anticorrelations are possible for small θ. We are interested in bounding these.

Lemma 2.2. *For any colouring $x \in \mathcal{X}$ satisfying (2.13), any integer $N > 2$ and any $\theta \in \left[\frac{\pi}{N}, \frac{\pi}{N-1}\right)$, we have $C_x(\theta) \geq C_1\left(\frac{\pi}{N}\right) - 2\gamma$.*

Proof. From the Braunstein-Caves inequality (2.6), we have that

$$\left|\sum_{k=0}^{N-1} C(k,k) + \sum_{k=0}^{N-1} C(k+1,k)\right| \leq 2N-2,$$

with the convention that measurement choice N is measurement choice 0 with reversed outcomes. We consider the case in which Alice's and Bob's measurements k are the same, for $k = 0, 1, \ldots, N-1$ and $N > 2$, and their outcomes are described by LHVT satisfying (2.8) and (2.13), which then also satisfy (2.15). If we take measurement k to be of the projection onto the state $|\xi_k\rangle$ so that the states $\{|\xi_k\rangle\}_{k=0}^{N-1}$ are along a great circle on the Bloch sphere with a separation angle $\theta = \frac{\pi}{N}$ between $|\xi_k\rangle$ and $|\xi_{k+1}\rangle$ for $k = 0, 1, \ldots, N-2$, for example $|\xi_k\rangle = \cos\left(\frac{k\pi}{2N}\right)|0\rangle + \sin\left(\frac{k\pi}{2N}\right)|1\rangle$, and average over random rotations of the Bloch sphere, this gives

$$\left|NC_x(0) + NC_x(\theta)\right| \leq 2N-2\,.$$

Thus, from (2.15):

$$C_x(0) = -1 + 2\gamma,$$

it follows that

$$C_x(\theta) \geq -1 + \frac{2}{N} - 2\gamma.$$

Since $C_1\left(\frac{\pi}{N}\right) = -1 + \frac{2}{N}$, as follows from (2.16), we have

$$C_x(\theta) \geq C_1\left(\frac{\pi}{N}\right) - 2\gamma.$$

Similarly, if we take the states $\{|\xi_k\rangle\}_{k=0}^{N-1}$ to be along a zigzag path crossing a great circle on the Bloch sphere with a separation angle $\theta > \frac{\pi}{N}$ between $|\xi_k\rangle$ and $|\xi_{k+1}\rangle$ for $k = 0, 1, \ldots, N-2$, in such a way that the angle separation between $|\xi_{N-1}\rangle$ and the state with Bloch vector antiparallel to that one of $|\xi_0\rangle$ is also θ (see Figure 2.2), we obtain after averaging over random rotations of the Bloch sphere that $C_x(\theta) \geq -1 + \frac{2}{N} - 2\gamma = C_1\left(\frac{\pi}{N}\right) - 2\gamma$. □

Remark 2.2. In other words, for small θ, $C_1(\theta)$ is very close to the maximal possible anticorrelation for LHVT when $\gamma \ll \theta$.

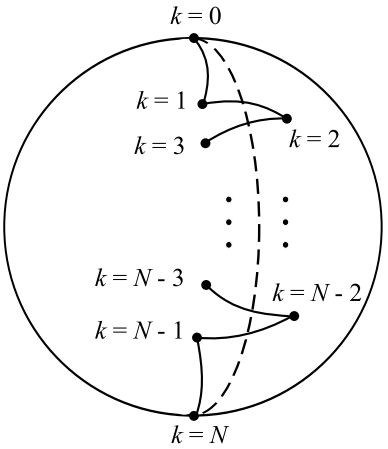


Figure 2.2: Diagram of the measurements performed by Alice and Bob that are used in the proof of Lemma 2.2. Alice's and Bob's measurements k are the same, for $k = 0, 1, \ldots, N-1$ and $N > 2$; these are projections onto the states $|\xi_k\rangle$ and correspond to points in the Bloch sphere with label k. These points form a zigzag path crossing the dashed great circle. The state $|\xi_N\rangle$ is antipodal to $|\xi_0\rangle$ and represents the measurement $k = 0$ with reversed outcomes. The solid lines represent arcs of great circles with the same angle $\theta > \frac{\pi}{N}$ that connect adjacent points. If $\theta = \frac{\pi}{N}$, all these points are on the same great circle.

Geometric intuitions also suggest bounds on $C_x(\theta)$ that are maximised by colouring 1 for small θ. Consider *simple colourings*, in which a set of (not necessarily connected) piecewise differentiable curves of finite total length separate black and white regions, with points lying on these curves having either colour. Intuition suggests that, for small θ and simple colourings with $\gamma = 0$, the quantity $1 + C_x(\theta)$, which measures the deviation from pure anticorrelation, should be bounded by a quantity roughly proportional to the length of the boundary between the black and white areas of the sphere colouring $x \in \mathcal{X}$. Since colouring 1 has the smallest such boundary (the equator), this might suggest that $C_x(\theta) \geq C_1(\theta)$, for small θ and for all simple colourings $x \in \mathcal{X}$ with $\gamma = 0$. Intuition also suggests that any non-simple colouring will produce less anticorrelation than the optimal simple colouring, because regions in which black and white colours alternate with arbitrarily small separation tend to wash out anticorrelation. These intuitions are discussed further in section 2.6.

These various observations motivate us to explore what we call the *Weak*

Hemispherical Colouring Maximality Hypothesis (*WHCMH*).

WHCMH. *There exists an angle* $\theta^w_{max} \in \left(0, \frac{\pi}{2}\right)$ *such that for every colouring* $x \in \mathcal{X}$ *with* $\gamma = 0$ *and every angle* $\theta \in [0, \theta^w_{max}]$, $C_x(\theta) \geq C_1(\theta)$.

The WHCMH considers models with perfect anticorrelation for $\theta = 0$, because we are interested in distinguishing LHV models from the quantum singlet state, which produces perfect anticorrelations for $\theta = 0$. Of course, there is a symmetry in the space of LHV models given by exchanging the colours of one qubit's sphere, which maps $\gamma \to 1 - \gamma$ and $C_x(\theta) \to -C_x(\theta)$. The WHCMH thus also implies that $C_x(\theta) \leq -C_1(\theta)$ for all colourings $x \in \mathcal{X}$ with $\gamma = 1$ and $\theta \in [0, \theta^{\mathrm{w}}_{\mathrm{max}}]$.

It is also interesting to investigate stronger versions of the WHCMH and related questions. For instance, is it the case that for every angle $\theta \in \left(\theta^{\mathrm{w}}_{\mathrm{max}}, \frac{\pi}{2}\right)$ there exists a colouring $x' \in \mathcal{X}$ with $\gamma = 0$ such that $C_{x'}(\theta) < C_1(\theta)$? And does this hypothesis still hold true (not necessarily for the same $\theta^{\mathrm{w}}_{\mathrm{max}}$) if we consider general local hidden variable models corresponding to independently chosen colourings for the two qubits, not constrained by any choice of the correlation parameter γ?

The following theorem and lemmas give some relevant bounds.

Theorem 2.1. *For any colouring* $x \in \mathcal{X}$, *any integer* $N \geq 2$ *and any* $\theta \in \left[\frac{\pi}{2N}, \frac{\pi}{2(N-1)}\right)$, *we have* $C_1\left(\frac{\pi}{2N}\right) \leq C_x(\theta) \leq -C_1\left(\frac{\pi}{2N}\right)$.

Proof. Consider the Braunstein-Caves inequality (2.6):

$$\left|\sum_{k=0}^{N-1} C(k,k) + \sum_{k=0}^{N-1} C(k+1,k)\right| \leq 2N - 2,$$

with the convention that measurement choice N is measurement choice 0 with reversed outcomes, in the case in which Alice's and Bob's measurements' outcomes are described by LHVT satisfying (2.8). Let Alice's and Bob's measurements k to correspond to the projections onto the states $|\xi_k\rangle$ and $|\chi_k\rangle$, respectively, for $k = 0, 1, \ldots, N-1$ and $N \geq 2$. Let the angle along the great circle in the Bloch sphere passing through the states $|\xi_k\rangle$ and $|\chi_k\rangle$ be θ, for $k = 0, 1, \ldots, N-1$. Similarly, let the angle along the great circle passing through $|\chi_k\rangle$ and $|\xi_{k+1}\rangle$ be θ for $k = 0, 1, \ldots, N-1$, with the convention that the state $|\xi_N\rangle$ has Bloch vector antiparallel to that one of $|\xi_0\rangle$. If $\theta = \frac{\pi}{2N}$, all these states are on the same great

circle beginning at $|\xi_0\rangle$ and ending at $|\xi_N\rangle$. If $\theta > \frac{\pi}{2N}$, the states can be accommodated on a zigzag path crossing the great circle that goes from $|\xi_0\rangle$ to $|\xi_N\rangle$ (see Figure 2.3). Thus, from the Braunstein-Caves inequality, after averaging over random rotations of the Bloch sphere, we have

$$-1 + \frac{1}{N} \leq C_x(\theta) \leq 1 - \frac{1}{N}.$$

Since $C_1\big(\frac{\pi}{2N}\big) = -1 + \frac{1}{N}$, as follows from (2.16), we have

$$C_1\Big(\frac{\pi}{2N}\Big) \leq C_x(\theta) \leq -C_1\Big(\frac{\pi}{2N}\Big),$$

for $\theta \geq \frac{\pi}{2N}$. □

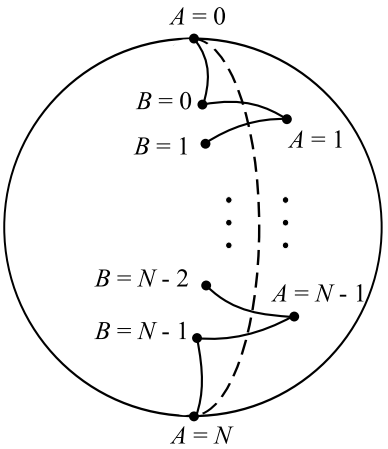


Figure 2.3: Diagram of the measurements performed by Alice and Bob that are used in the proof of Theorem 2.1. Alice's and Bob's measurements A and B are projections onto the states $|\xi_A\rangle$ and $|\chi_B\rangle$ and correspond to points in the Bloch sphere with labels A and B, respectively, for $A, B \in \{0, 1, \ldots, N-1\}$ and $N \geq 2$. These points form a zigzag path crossing the dashed great circle. The state $|\xi_N\rangle$ is antipodal to $|\xi_0\rangle$ and represents Alice's measurement $A = 0$ with reversed outcomes. The solid lines represent arcs of great circles with the same angle $\theta > \frac{\pi}{2N}$ that connect adjacent points. If $\theta = \frac{\pi}{2N}$, all these points are on the same great circle.

Remark 2.3. In particular, for small θ, $-C_1(\theta)$ and $C_1(\theta)$ are very close to the maximal possible correlation and anticorrelation for any LHVT, respectively.

Lemma 2.3. *If any colouring $x \in \mathcal{X}$ obeys $C_x(\theta) < C_1(\theta)$ $\Big(C_x(\theta) > -C_1(\theta)\Big)$ for some $\theta \in \big(\frac{\pi}{M+1}, \frac{\pi}{M}\big]$ and an integer $M \geq 2$ then there are angles $\theta_j \equiv \frac{\pi}{M+1-j} - \theta$ with $j = 1, 2, \ldots, M-1$, which satisfy $0 \leq \theta_j < \theta$ if $j < \frac{M}{2} + 1$, and $\frac{\pi}{2} > \theta_j > \theta$ if $j \geq \frac{M}{2} + 1$, such that $C_x(\theta_j) > C_1(\theta_j)$ $\Big(C_x(\theta_j) < -C_1(\theta_j)\Big)$.*

Proof. Consider a colouring $x \in \mathcal{X}$ and an angle $\theta \in \big(\frac{\pi}{M+1}, \frac{\pi}{M}\big]$ for an integer $M \geq 2$ such that $C_x(\theta) < C_1(\theta)$ or $C_x(\theta) > -C_1(\theta)$. From Theorem 2.1 and the fact that $C_x\big(\frac{\pi}{2}\big) = C_1\big(\frac{\pi}{2}\big) = 0$, it must be that $\theta \neq \frac{\pi}{M}$ if M is even. We define the angles $\theta_j \equiv \frac{\pi}{M+1-j} - \theta$ with $j = 1, 2, \ldots, M-1$. Considering the cases M even and M odd, and using that $\theta \neq \frac{\pi}{M}$ if M is even, it is straightforward to obtain that $0 \leq \theta_j < \theta$ if $j < \frac{M}{2} + 1$ and $\frac{\pi}{2} > \theta_j > \theta$ if $j \geq \frac{M}{2} + 1$. Now consider the Braunstein-Caves inequality (2.6):

$$\left| \sum_{k=0}^{N-1} C(k,k) + \sum_{k=0}^{N-1} C(k+1,k) \right| \leq 2N - 2,$$

with the convention that measurement choice N is measurement choice 0 with reversed outcomes, in the case in which Alice's and Bob's measurements' outcomes are described by LHVT satisfying (2.8). Let Alice's and Bob's measurements k to correspond to the projections onto the states $|\xi_k\rangle$ and $|\chi_k\rangle$, respectively, for $k = 0, 1, \ldots, N-1$ and $N \equiv M+1-j$. Since $1 \leq j \leq M-1$, we have $2 \leq N \leq M$. Let all these states be on the great circle in the Bloch sphere that passes through the states $|\xi_0\rangle$ and $|\xi_N\rangle$, with the convention that the state $|\xi_N\rangle$ has Bloch vector antiparallel to that one of $|\xi_0\rangle$. Let the angles between $|\xi_k\rangle$ and $|\chi_k\rangle$, and between $|\chi_k\rangle$ and $|\xi_{k+1}\rangle$ along this great circle be θ and θ_j, respectively. For example, $|\xi_k\rangle = \cos\big(\frac{k\pi}{2N}\big)|0\rangle + \sin\big(\frac{k\pi}{2N}\big)|1\rangle$ and $|\chi_k\rangle = \cos\big(\frac{k\pi}{2N} + \frac{\theta}{2}\big)|0\rangle + \sin\big(\frac{k\pi}{2N} + \frac{\theta}{2}\big)|1\rangle$, for $k = 0, 1, \ldots, N-1$. From the Braunstein-Caves inequality, after averaging over random rotations of the Bloch sphere, we obtain

$$-1 + \frac{1}{N} \leq \frac{1}{2}\big(C_x(\theta) + C_x(\theta_j)\big) \leq 1 - \frac{1}{N}.$$

Since the average angle $\bar{\theta}_j \equiv \frac{1}{2}(\theta + \theta_j)$ satisfies $\bar{\theta}_j = \frac{\pi}{2(M+1-j)} = \frac{\pi}{2N}$ and $C_1(\frac{\pi}{2N}) =$

$-1+\frac{1}{N}$, as follows from (2.16), we have

$$C_1\big(\bar{\theta}_j\big) \leq \frac{1}{2}\big(C_x(\theta)+C_x(\theta_j)\big) \leq -C_1\big(\bar{\theta}_j\big).$$

Since $C_1(\theta)$ is a linear function of θ, it follows that

$$C_x(\theta_j) > C_1(\theta_j),$$

if $C_x(\theta) < C_1(\theta)$. Similarly,

$$C_x(\theta_j) < -C_1(\theta_j),$$

if $C_x(\theta) > -C_1(\theta)$. □

Remark 2.4. In this sense (at least), the anticorrelations defined by C_1 and the correlations defined by $-C_1$ cannot be dominated by any other colourings.

Lemma 2.4. *For any colouring $x \in \mathcal{X}$ and any $\theta \in \big(0, \frac{\pi}{3}\big)$, we have $Q(\theta) < C_x(\theta) < -Q(\theta)$.*

Proof. Let $x \in \mathcal{X}$ be any colouring and $\theta \in \big(0, \frac{\pi}{3}\big)$. We first consider the case $\theta \in \big[\frac{\pi}{4}, \frac{\pi}{3}\big)$. From Theorem 2.1, we have

$$C_1\Big(\frac{\pi}{4}\Big) \leq C_x(\theta) \leq -C_1\Big(\frac{\pi}{4}\Big).$$

The quantum correlation for the singlet state is $Q(\theta) = -\cos\theta$. Since $Q(\theta)$ is a strictly increasing function of θ, we have $Q(\theta) < Q\big(\frac{\pi}{3}\big) = -\frac{1}{2} = C_1\big(\frac{\pi}{4}\big)$ for $\theta < \frac{\pi}{3}$, where the second equality follows from (2.16). Therefore,

$$Q(\theta) < C_x(\theta) < -Q(\theta),$$

for $\theta \in \big[\frac{\pi}{4}, \frac{\pi}{3}\big)$. Similarly, it is easy to see that $Q(\theta) < C_x(\theta) < -Q(\theta)$ for $\theta \in \big[\frac{\pi}{6}, \frac{\pi}{4}\big)$.

Now we consider the case $\theta \in \big(0, \frac{\pi}{6}\big)$. We define $N = \lceil \frac{\pi}{2\theta} \rceil$. It follows that

$\theta \in \left[\frac{\pi}{2N}, \frac{\pi}{2(N-1)}\right)$ for an integer $N \geq 4$. From Theorem 2.1 and (2.16), we have

$$-1 + \frac{1}{N} \leq C_x(\theta) \leq 1 - \frac{1}{N}.$$

From the Taylor series $Q(\theta) = -1 + \frac{\theta^2}{2} - \frac{\theta^4}{4!} + \frac{\theta^6}{6!} - \cdots$, it is easy to see that $Q(\theta) < -1 + \frac{\theta^2}{2}$ for $0 < \theta < \sqrt{30}$. Thus, we have

$$Q\left(\frac{\pi}{2(N-1)}\right) < -1 + \frac{1}{2}\left(\frac{\pi}{2(N-1)}\right)^2.$$

Since $N^2 > \left(\frac{\pi^2}{8} + 2\right)N - 1$, it follows that $(N-1)^2 > \frac{\pi^2}{8}N$, which implies that

$$-1 + \frac{1}{2}\left(\frac{\pi}{2(N-1)}\right)^2 < -1 + \frac{1}{N}.$$

It follows that

$$Q\left(\frac{\pi}{2(N-1)}\right) < C_x(\theta).$$

Since $Q(\theta)$ is a strictly increasing function of θ and $\theta < \frac{\pi}{2(N-1)}$, we have

$$Q(\theta) < Q\left(\frac{\pi}{2(N-1)}\right).$$

Thus, we have

$$Q(\theta) < C_x(\theta).$$

Similarly, we have

$$C_x(\theta) < -Q(\theta).$$

□

Remark 2.5. This inequality separates all possible LHV correlations $C_x(\theta)$ from the singlet state quantum correlations $Q(\theta)$ for all $\theta \in \left(0, \frac{\pi}{3}\right)$.

The previous observations motivate the *Strong Hemispherical Colouring Maximality Hypothesis* (*SHCMH*).

SHCMH. *There exists an angle* $\theta^s_{max} \in \left(0, \frac{\pi}{2}\right)$ *such that for every colouring* $x \in \mathcal{X}$ *and every angle* $\theta \in [0, \theta^s_{max}]$, $C_1(\theta) \leq C_x(\theta) \leq -C_1(\theta)$.

Note that the SHCMH applies to all colourings, without any assumption of perfect anticorrelation for $\theta = 0$. If the SHCMH is true then so is the WHCMH. In this case, we have that $\theta^{\mathrm{s}}_{\max} \leq \theta^{\mathrm{w}}_{\max}$. Thus, an upper bound on $\theta^{\mathrm{w}}_{\max}$ implies an upper bound on $\theta^{\mathrm{s}}_{\max}$.

2.4 Numerical Results

We investigated the WHCMH numerically by computing the correlation $C_x(\theta)$ for various colouring functions that satisfy the antipodal property (2.7), the condition (2.14), and that have azimuthal symmetry. These colourings, which are illustrated in Figure 2.4, are defined as

$$a_x(\epsilon) \equiv \begin{cases} 1 & \text{if } \epsilon \in \mathcal{E}_x, \\ -1 & \text{if } \epsilon \in [0,\pi]/\mathcal{E}_x, \end{cases} \tag{2.17}$$

where $\epsilon \in [0,\pi]$ is the polar angle in the sphere and

$$\begin{aligned}
\mathcal{E}_1 &\equiv \left[0, \frac{\pi}{2}\right], \\
\mathcal{E}_2 &\equiv \left[0, \frac{\pi}{4}\right] \bigcup \left[\frac{\pi}{2}, \frac{3\pi}{4}\right], \\
\mathcal{E}_3 &\equiv \bigcup_{k=0}^{2} \left[k\frac{\pi}{3}, (2k+1)\frac{\pi}{6}\right], \\
\mathcal{E}_4 &\equiv \bigcup_{k=0}^{3} \left[k\frac{\pi}{4}, (2k+1)\frac{\pi}{8}\right], \\
\mathcal{E}_{2_\Delta} &\equiv \left[0, \frac{\pi}{4} - \Delta\right] \bigcup \left[\frac{\pi}{2}, \frac{3\pi}{4} + \Delta\right], \\
\mathcal{E}_{3_\delta} &\equiv \left[0, \frac{\pi}{6} + \delta\right] \bigcup \left[\frac{\pi}{3}, \frac{\pi}{2}\right] \bigcup \left[\frac{2\pi}{3}, \frac{5\pi}{6} - \delta\right],
\end{aligned}$$

with $0 \leq \Delta \leq \frac{\pi}{12}$ and $-\frac{\pi}{18} \leq \delta \leq \frac{\pi}{24}$. Notice that colourings 2_Δ and 3_δ reduce to colourings 2 and 3 if $\Delta = 0$ and $\delta = 0$, respectively.

Equation (2.10) was used to compute the double integral in (2.8). Equation (2.11) was not necessary because the colourings we considered have azimuthal

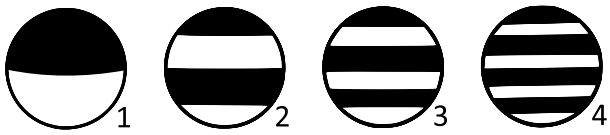


Figure 2.4: Some antipodal colouring functions a_x on the sphere defined by (2.17). Their correlations $C_x(\theta)$, computed with Equation (2.8), subject to the constraint (2.14), are plotted in Figure 2.5.

symmetry. The integral with respect to the angle ω was performed analytically. Thus, the correlations $C_x(\theta)$ were reduced to a sum of terms that include single integrals with respect to the polar angle ϵ; the obtained expressions are given in Appendix A. The single integrals with respect to ϵ were computed numerically with a computer program, whose code is given in Appendix B.

Our results are plotted in Figure 2.5; they are consistent with the WHCMH. They also show that $\theta^{\mathrm{w}}_{\max} < \frac{\pi}{2}$, because they show that there exists a colouring x with $C_x(\theta) < C_1(\theta)$ for some angles $\theta \in \left(0, \frac{\pi}{2}\right)$, namely colouring 3 for angles $\theta \in \left[0.405\pi, \frac{\pi}{2}\right)$. They also show that there exist colourings x with $C_x(\theta) > -C_1(\theta)$ for some angles $\theta \in \left(0, \frac{\pi}{2}\right)$, namely colouring 2 for angles $\theta \in \left[0.375\pi, \frac{\pi}{2}\right)$ and colouring 4 for $\theta \in \left[0.422\pi, \frac{\pi}{2}\right)$. Another interesting result is that there exist colourings that produce correlations $C_x(\theta) < Q(\theta)$ for θ close to $\frac{\pi}{2}$: colouring 3 for angles $\theta \in \left[0.467\pi, \frac{\pi}{2}\right)$. It is interesting to find other colourings whose correlations satisfy $C_x(\theta) < C_1(\theta)$, $C_x(\theta) > -C_1(\theta)$ and $C_x(\theta) < Q(\theta)$ for angles θ closer to zero. For this purpose, we consider colourings 2_Δ and 3_δ, which are defined in (2.17) and consist in small variations of colourings 2 and 3 in terms of the parameters Δ and δ, respectively. Colourings 2_Δ and 3_δ reduce to colourings 2 and 3 if $\Delta = 0$ and $\delta = 0$, respectively. For values of δ in the range $\left[-\frac{\pi}{18}, \frac{\pi}{24}\right]$, we obtained that the smallest angle θ for which $C_{3_\delta}(\theta) < C_1(\theta)$ is achieved for $\delta = -0.038\pi$, in which case we have that $C_{3_{-0.038\pi}}(\theta) < C_1(\theta)$ for $\theta \in \left[0.386\pi, \frac{\pi}{2}\right)$. We also obtained that the smallest angle θ for which $C_{3_\delta}(\theta) < Q(\theta)$ is achieved for $\delta = -0.046\pi$, in which case we have that $C_{3_{-0.046\pi}}(\theta) < Q(\theta)$ for $\theta \in [0.431\pi, \frac{\pi}{2})$ (see Figure 2.6). For values of Δ in the range $\left[0, \frac{\pi}{12}\right]$, we obtained that the smallest angle θ for which $C_{2_\Delta}(\theta) > -C_1(\theta)$ is achieved for $\Delta = 0.035\pi$, in which case we have that $C_{2_{0.035\pi}}(\theta) > -C_1(\theta)$ for $\theta \in \left[0.345\pi, \frac{\pi}{2}\right)$ (see Figure 2.7).

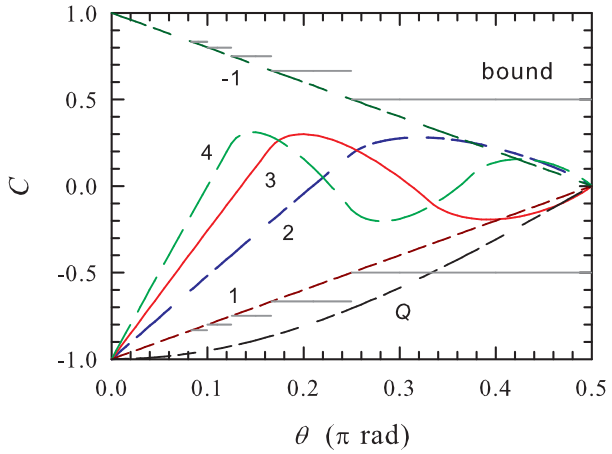


Figure 2.5: Correlations computed with Equation (2.8), subject to the constraint (2.14), for the colouring functions a_x shown schematically in Figure 2.4 and defined by (2.17). The correlations for colouring 2, 3 and 4 are blue dot-dashed, red solid and green dashed curves, respectively. The black dot-dash-dotted curve represents the singlet state quantum correlation $Q(\theta)$. The dark red dotted and dark green dash-dotted curves show respectively the colouring 1 correlation, $C_1(\theta)$, and anticorrelation, $-C_1(\theta)$. The gray solid straight lines show the bounds given by Theorem 2.1, for $\theta \geq \frac{\pi}{12}$.

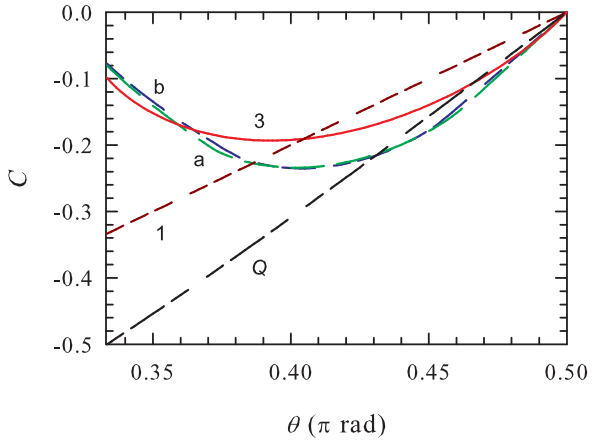


Figure 2.6: Correlations obtained for colouring 3_δ, defined in (2.17), for $\delta = -0.038\pi$ (a, green dashed curve) and $\delta = -0.046\pi$ (b, blue dot-dashed curve); for colourings 3, 1 and the singlet state quantum correlation $Q(\theta)$ (red solid, dark red dotted and black dot-dash-dotted curves, respectively).

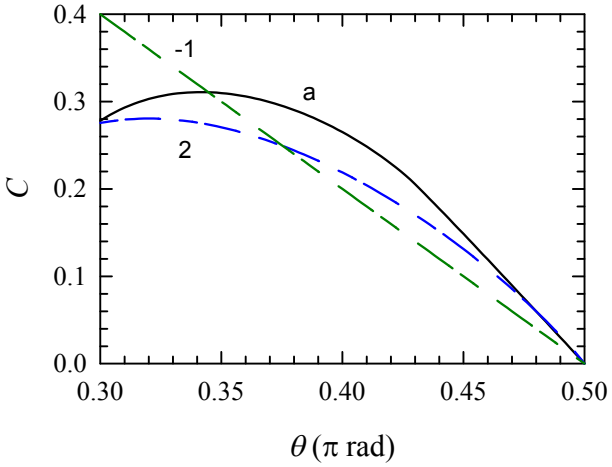


Figure 2.7: Correlations obtained for colouring 2_Δ, defined in (2.17), for $\Delta = 0.035\pi$ (a, black solid curve) and for colouring 2 (blue dot-dashed curve). The colouring 1 anticorrelation is plotted too (-1, dark green dash-dotted curve).

Our numerical results imply the bound $\theta^{\mathrm{w}}_{\max} \leq 0.386\pi$. They also imply that $\theta^{\mathrm{s}}_{\max} \leq 0.345\pi$, because $C_{2_{0.035\pi}}(\theta) > -C_1(\theta)$ for $\theta \in \left(0.345\pi, \frac{\pi}{2}\right)$, and $C_1(\theta) \leq C_x(\theta) \leq -C_1(\theta)$ for $x = 2, 3, 4, 2_\Delta, 3_\delta$ and $\theta \in [0, 0.345\pi]$. Notice that the weaker upper bound $\theta^{\mathrm{s}}_{\max} \leq 0.375\pi$ is given in our publication [94] because colouring 2_Δ is not considered there.

In order to confirm analytically the numerical observation that there exist colouring functions $x \in \mathcal{X}$ such that $C_x(\theta) < Q(\theta)$ for θ close to $\frac{\pi}{2}$, we computed $C_3\left(\frac{\pi}{2} - \tau\right)$ for $0 \leq \tau \ll 1$ to order $\mathcal{O}(\tau^2)$. The computation is presented in Appendix A. We obtain

$$C_3\left(\frac{\pi}{2} - \tau\right) = -1.5\tau + \mathcal{O}(\tau^2). \tag{2.18}$$

On the other hand, the singlet state quantum correlation gives $Q\left(\frac{\pi}{2} - \tau\right) = -\cos\left(\frac{\pi}{2} - \tau\right) = -\tau + \mathcal{O}(\tau^3)$. Thus, we see that for τ small enough, indeed $C_3\left(\frac{\pi}{2} - \tau\right) < Q\left(\frac{\pi}{2} - \tau\right)$.

2.5 Related Questions for Exploration

An interesting question is, for an arbitrary two qubit state ρ and qubit projective measurements performed by Alice and Bob corresponding to random Bloch vectors separated by an angle θ, what are the maximum values of the quantum correlations and anticorrelations $Q_\rho(\theta)$, and which states achieve them?

We show that the maximum quantum anticorrelations and correlations are $Q_\rho(\theta) = -\cos\theta$, achieved by the singlet state $\rho = |\Psi^-\rangle\langle\Psi^-|$, and $Q_\rho(\theta) = \frac{1}{3}\cos\theta$, achieved by the other Bell states, $\rho = |\Phi^\pm\rangle\langle\Phi^\pm|$ and $\rho = |\Psi^+\rangle\langle\Psi^+|$, respectively.[1]

[1]Notice that correlations equal to $\cos\theta$ would be achieved with the singlet state, and correlations equal to $-\frac{1}{3}\cos\theta$ would be obtained with the other Bell states, if one of the parties always flips their outcomes. This strategy corresponds only to relabeling the measurement outcomes and is not included in our analysis.

At first sight, it could be surprising that the singlet state achieves the maximum quantum anticorrelation, while the other Bell states do not. The fact that any Bell state can violate the CHSH and Braunstein-Caves inequalities to the maximum value allowed by quantum mechanics, for an appropriate set of measurement choices, would suggest that the maximum quantum anticorrelations and correlations considered here could be achieved by the four Bell states too. However, a fundamental difference between the singlet and the other Bell states is that the singlet expressed in a given basis is the same in any other basis, while this property does not

This result follows because, as we show below, we have

$$-\cos\theta \leq Q_\rho(\theta) \leq \frac{1}{3}\cos\theta. \tag{2.19}$$

Another related question that we do not explore further here is, for a fixed given angle θ separating Alice's and Bob's measurement axes, what are the maximum correlations and anticorrelations, if in addition to the two qubit state ρ, Alice and Bob have other resources? For example, Alice and Bob could have an arbitrary entangled state on which they perform arbitrary local quantum operations and measurements. In a different scenario, Alice and Bob could have some amount of classical or quantum communication. Another possibility is for Alice and Bob to share arbitrary non-signalling resources, not necessarily quantum, with no communication allowed. It is interesting to note that in this case, the no-signalling principle does not restrict the value of the correlations, because $C = 1$ is achieved for all θ by a generalization of the PR-box [70], which is given by the following non-signalling outcome probabilities: $P\big(1,1|\vec{a},\vec{b}\big) = P\big(-1,-1|\vec{a},\vec{b}\big) = \frac{1}{2}$, $P\big(1,-1|\vec{a},\vec{b}\big) = P\big(-1,1|\vec{a},\vec{b}\big) = 0$ for all $\vec{a},\vec{b} \in \mathbb{S}^2$. Similarly, $C = -1$ is achieved by the non-signalling outcome proabilities $P\big(1,-1|\vec{a},\vec{b}\,\big) = P\big(-1,1|\vec{a},\vec{b}\,\big) = \frac{1}{2}$, $P\big(1,1|\vec{a},\vec{b}\,\big) = P\big(-1,-1|\vec{a},\vec{b}\,\big) = 0$ for all $\vec{a},\vec{b} \in \mathbb{S}^2$. Different variations of the task described above with continuous parameters can be investigated.

Some interesting related questions involving nonlocal games with continuous inputs have been considered in [95]. In particular, in the third game considered in [95], Alice and Bob are given uniformly distributed Bloch sphere vectors, $\vec{r}_A$ and $\vec{r}_B$, and aim to maximise the probability of producing outputs that are opposite if $\vec{r}_A \cdot \vec{r}_B \geq 0$ or equal if $\vec{r}_A \cdot \vec{r}_B < 0$. It is suggested in [95] that the LHV strategy defined by opposite hemispherical colourings is optimal, though no argument is given. It is also suggested that the quantum strategy given by sharing a singlet and carrying out measurements corresponding to the input vectors is optimal, based on evidence from semi-definite programming. Equation (2.19) shows that this is the case for all θ, and so in particular for the average advantage in the

hold for the other Bell states. Since the (anti) correlations we consider here are obtained after averaging over all possible projective measurements on the Bloch sphere, given the constraint of the angle separation θ between Alice's and Bob's measurement axes, the anticorrelation achieved by the singlet is higher than the anticorrelation achieved by the other Bell states.

game considered, if Alice and Bob are restricted to outputs defined by projective measurements on a shared pair of qubits. Our results given by Lemma 2.4 also prove that there is a quantum advantage for all θ in the range $0 < \theta < \frac{\pi}{3}$, and hence for many versions of this game defined by a variety of probability distributions for the inputs.

We complete this section by showing (2.19). First, we compute the average outcome probabilities when Alice and Bob apply local projective measurements on a two qubit state ρ, for measurement bases defined by Bloch vectors separated by an angle θ. The average is taken over random rotations of these vectors in the Bloch sphere, subject to the angle separation θ. Then, we compute the quantum correlations.

Consider a fixed pair of pure qubit states $|0\rangle$ and $|\chi\rangle = \cos\big(\frac{\theta}{2}\big)|0\rangle + \sin\big(\frac{\theta}{2}\big)|1\rangle$ for Alice's and Bob's measurements corresponding to outcomes '1', respectively. A general state for Bob's measurement separated by an angle θ with respect to a fixed state $|0\rangle$ for Alice's measurement is obtained by applying the unitary $R_z(\omega)$ that corresponds to a rotation of an angle $\omega \in [0, 2\pi]$ around the z axis in the Bloch sphere, which only adds a phase to the state $|0\rangle$. Then, after applying $R_z(\omega)$, a general pure product state $|\xi_{\vec{a}}\rangle \otimes |\chi_{\vec{b}}\rangle$ of two qubits with Bloch vectors separated by an angle θ is obtained by applying the unitary $R_z(\phi)R_y(\epsilon)$ that rotates the Bloch sphere around the y axis by an angle $\epsilon \in [0, \pi]$ and then around the z axis by an angle $\phi \in [0, 2\pi]$. Thus, we have $|\xi_{\vec{a}}\rangle \otimes |\chi_{\vec{b}}\rangle = U_{\phi,\epsilon,\omega}|0\rangle \otimes U_{\phi,\epsilon,\omega}|\chi\rangle$, with $U_{\phi,\epsilon,\omega} = R_z(\phi)R_y(\epsilon)R_z(\omega)$. This is a general unitary acting on a qubit, up to a global phase. Therefore, we can parameterize this unitary by the Haar measure μ on SU(2), hence, we have $|\xi_{\vec{a}}\rangle \otimes |\chi_{\vec{b}}\rangle = U_\mu|0\rangle \otimes U_\mu|\chi\rangle$. After taking the average, the probability that both Alice and Bob obtain the outcome '1' is

$$\begin{aligned} P(1,1|\theta) &= \int d\mu \mathrm{Tr}\Big(\rho\big(|\xi_{\vec{a}}\rangle\langle\xi_{\vec{a}}| \otimes |\chi_{\vec{b}}\rangle\langle\chi_{\vec{b}}|\big)\Big) \\ &= \int d\mu \mathrm{Tr}\Big(\rho\big(U_\mu \otimes U_\mu\big)\big(|0\rangle\langle 0| \otimes |\chi\rangle\langle\chi|\big)\big(U_\mu^\dagger \otimes U_\mu^\dagger\big)\Big) \\ &= \mathrm{Tr}\Big(\int d\mu \big(U_\mu^\dagger \otimes U_\mu^\dagger\big)\rho\big(U_\mu \otimes U_\mu\big)\big(|0\rangle\langle 0| \otimes |\chi\rangle\langle\chi|\big)\Big) \\ &= \mathrm{Tr}\Big(\tilde{\rho}\big(|0\rangle\langle 0| \otimes |\chi\rangle\langle\chi|\big)\Big), \end{aligned} \tag{2.20}$$

where in the third line we used the linearity and the cyclicity of the trace and in the fourth line we used the definition $\tilde{\rho} \equiv \int d\mu \big(U_\mu^\dagger \otimes U_\mu^\dagger\big)\rho\big(U_\mu \otimes U_\mu\big)$. The state $\tilde{\rho}$ is invariant under a unitary transformation $U \otimes U$, for any $U \in \mathrm{SU}(2)$. The only states with this symmetry are the Werner states [96], which for the two qubit case have the general form

$$\tilde{\rho} = r|\Psi^-\rangle\langle\Psi^-| + \frac{1-r}{3}\big(|\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|\big), \tag{2.21}$$

with $0 \leq r \leq 1$. Thus, from (2.20) and (2.21), we obtain

$$P(1,1|\theta) = \frac{1-r}{3} + \frac{4r-1}{6}\sin^2\Big(\frac{\theta}{2}\Big). \tag{2.22}$$

Since the projectors corresponding to Alice and Bob obtaining outcomes '-1' are obtained by a unitary transformation of the form $U \otimes U$ on $|0\rangle \otimes |\chi\rangle$, with $U \in \mathrm{SU}(2)$, then from (2.20) we see that after integrating over the Haar measure on SU(2), we obtain $P(-1,-1|\theta) = P(1,1|\theta)$.

Thus, the average quantum correlation is $Q_\rho(\theta) = 4P(1,1|\theta) - 1$, which from (2.22) gives

$$Q_\rho(\theta) = -\Big(\frac{4r-1}{3}\Big)\cos\theta. \tag{2.23}$$

Then, Equation (2.19) follows because $0 \leq r \leq 1$.

2.6 Discussion

In this chapter, we have investigated Bell inequalities for a pair of qubits in which projective measurements are chosen randomly from the Bloch sphere, with the constraint that the measurement axes are fixed by a given separation angle θ. We have obtained Bell inequalities for $\theta \in \big[0, \frac{\pi}{2}\big]$, given by Theorem 2.1. These inequalities allow us to distinguish any LHV correlations from the singlet state quantum correlations for angles $\theta \in \big(0, \frac{\pi}{3}\big)$, as stated by Lemma 2.4. Nevertheless, we have introduced a hypothesis, the SHCMH, which if were proven true would imply that our Bell inequalities are not optimal.

The Strong Hemispherical Colouring Maximality Hypothesis (SHCMH) states that colouring 1, in which for one sphere, one hemisphere is totally black and the

other hemisphere is totally white, and the colours are opposite for the other sphere, gives the maximum correlation and anticorrelation for $\theta \in [0, \theta^{\mathrm{s}}_{\mathrm{max}}]$. A weak version of this hypothesis, the WHCMH, restricts to colourings in which the spheres are coloured oppositely and states that, for these colourings, colouring 1 gives the maximum anticorrelation for $\theta \in [0, \theta^{\mathrm{w}}_{\mathrm{max}}]$.

We have explored these hypotheses numerically for some simple colourings (see Figure 2.4). Our numerical results are consistent with these hypotheses for $\theta^{\mathrm{w}}_{\mathrm{max}} \leq 0.386\pi$ and $\theta^{\mathrm{s}}_{\mathrm{max}} \leq 0.345\pi$. Notice that a smaller upper bound, $\theta^{\mathrm{s}}_{\mathrm{max}} \leq 0.375\pi$, is given in our publication [94], because colouring 2_Δ is not considered there.

It would be interesting to explore these hypotheses numerically for other colourings. We have restricted to compute the correlations for a few simple colourings. As discussed in detail in Appendix B, the main reason for this was to obtain sufficiently high precision, of the order of 10^{-5}, for the plotted values so that the given precision in the bounds $\theta^{\mathrm{w}}_{\mathrm{max}} \leq 0.386\pi$ and $\theta^{\mathrm{s}}_{\mathrm{max}} \leq 0.345\pi$ is guaranteed. We expect that more involved colourings can be investigated with adequate numerical techniques. We describe some colourings that we consider interesting to investigate. Before doing so, we discuss some geometric intuitions that motivate our interest in such colourings.

As introduced in section 2.3, a geometric intuition supporting the WHCMH is that, for colourings with oppositely coloured spheres and small values of θ, the anticorrelation seems to decrease proportionally to the boundary between black and white regions. Since colouring 1 has the shortest boundary, the equator, according to the previous intuition, the colouring 1 anticorrelation should be optimal for this class of colourings and for small values of θ. This intuition can be challenged by colourings defined by some parameter ν such that $C_\nu(\theta_\nu) < C_1(\theta_\nu)$ for some $\theta_\nu \in \left(0, \frac{\pi}{2}\right)$, while $C_\nu(\theta) > C_1(\theta)$ for $0 < \theta << \theta_\nu$. If a set of colourings satisfying these properties can be found for which the angle θ_ν can be made arbitrarily small then the above geometric intuition is clearly satisfied, but the WHCMH is false, which implies that the SHCMH is false too.

Further analysis of the previous intuitions is made by distinguishing the one-dimensional case of antipodal colourings for a pair of circles. In this case, the analogue of colouring 1 is a colouring in which, for one circle, one half-circle is

black and the other one is white, and the colours are opposite for the other circle. The correlations for this colouring are given by the function $\tilde{C}_1(\theta) = -1 + \frac{2\theta}{\pi}$, where the tilde is used to distinguish the one-dimensional case. We can find antipodal colourings of the circle that violate the one-dimensional analogue of the WHCMH, that is, for any arbitrarily small θ there exists a colouring A such that $\tilde{C}_{\mathrm{A}}(\theta) < \tilde{C}_1(\theta)$. Consider the set of colourings A_ν, for odd positive integers ν, defined by the colouring functions $a_{\mathrm{A}_\nu}(\phi) = -b_{\mathrm{A}_\nu}(\phi) = (-1)^{\left\lfloor \frac{\nu\phi}{\pi} \right\rfloor}$, where $\phi \in [0, 2\pi]$ is the angular coordinate in the circle. The correlations for these colourings satisfy $\tilde{C}_{\mathrm{A}_\nu}(\theta) = -1 + \frac{2\nu\theta}{\pi}$ for $\theta \in \left[0, \frac{\pi}{\nu}\right]$ and $\tilde{C}_{\mathrm{A}_\nu}(\theta) = 3 - \frac{2\nu\theta}{\pi}$ for $\theta \in \left[\frac{\pi}{\nu}, \frac{2\pi}{\nu}\right]$. Thus, by defining $\theta_{\mathrm{A}_\nu} \equiv \frac{2\pi}{\nu}$, we have that $\tilde{C}_{\mathrm{A}_\nu}(\theta) > \tilde{C}_1(\theta)$ for $\theta \in \left(0, \frac{2\pi}{1+\nu}\right)$, where $\frac{2\pi}{1+\nu} < \theta_{\mathrm{A}_\nu}$, and that $\tilde{C}_1(\theta_{\mathrm{A}_\nu}) > \tilde{C}_{\mathrm{A}_\nu}(\theta_{\mathrm{A}_\nu}) = -1$. Therefore, the set of colourings A_ν are in agreement with the geometrical intuitions given above, in the sense that $\tilde{C}_{\mathrm{A}_\nu}(\theta) > \tilde{C}_1(\theta)$ for $0 < \theta << \theta_{\mathrm{A}_\nu}$. However, the analogue of colouring 1 in one dimension does not give the maximum anticorrelation for any range of $\theta > 0$, because for any arbitrarily small $\varepsilon > 0$ we can find a positive angle $\theta_{\mathrm{A}_\nu} < \varepsilon$ for which $\tilde{C}_{\mathrm{A}_\nu}(\theta_{\mathrm{A}_\nu}) < \tilde{C}_1(\theta_{\mathrm{A}_\nu})$.

For the one-dimensional case, the high degree of symmetry for the colourings A_ν allows them to achieve perfect anticorrelation at the angles θ_{A_ν}. However, in the two-dimensional case, which we have investigated in this chapter, colourings that have similar symmetry properties along some directions are less symmetric along other directions. For example, consider a natural extension of the one-dimensional colourings A_ν to the two-dimensional case, defined by the colouring functions $a_{\mathrm{A}_\nu}(\epsilon, \phi) = -b_{\mathrm{A}_\nu}(\epsilon, \phi) = (-1)^{\left\lfloor \frac{\nu\phi}{\pi} \right\rfloor}$ for $\epsilon \in [0, \pi]$ and $\phi \in [0, 2\pi]$, where ϵ and ϕ are the polar and the azimuthal angles in the sphere, respectively (see Figure 2.8). These colourings are antipodal for odd positive integers ν. Notice that colouring A_1 is colouring 1, apart from a rotation of the spheres of an angle $\frac{\pi}{2}$ around an axis in the equatorial plane, which does not change the correlations. As in the one-dimensional case, we define $\theta_{\mathrm{A}_\nu} \equiv \frac{2\pi}{\nu}$. Perfect anticorrelations are achieved at angles $\theta = \theta_{\mathrm{A}_\nu}$ if we consider measurement axes constrained to be along the equator, but this property is lost for measurement axes along other great circles. Due to the periodic variations of the colourings A_ν, we expect the correlations $C_{\mathrm{A}_\nu}(\theta)$ for these colourings to oscillate between local maximums and minimums at intervals with values close to $\frac{\theta_{\mathrm{A}_\nu}}{2}$.

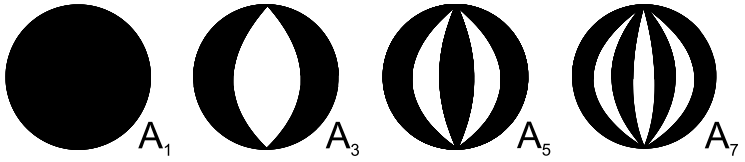


Figure 2.8: Colourings A_ν. These colourings are defined by the colouring functions $a_{\mathrm{A}_\nu}(\epsilon,\phi) = -b_{\mathrm{A}_\nu}(\epsilon,\phi) = (-1)^{\left\lfloor \frac{\nu\phi}{\pi} \right\rfloor}$ for $\epsilon \in [0,\pi]$ and $\phi \in [0,2\pi]$, where ϵ and ϕ are the polar and the azimuthal angles in the sphere, respectively. The figure illustrates the range of angles $\phi \in [0,\pi]$ for one of the pair of spheres. These colourings are antipodal for ν odd. Colouring A_1 is the same as colouring 1, apart from a rotation of the spheres, which does not change the correlations.

Another set of simple colourings is the set B_ν, defined by the colouring functions $a_{\mathrm{B}_\nu}(\epsilon,\phi) = -b_{\mathrm{B}_\nu}(\epsilon,\phi) = (-1)^{\left\lfloor \frac{2\nu\epsilon}{\pi} \right\rfloor}$ for $\epsilon \in [0,\pi)$ and $a_{\mathrm{B}_\nu}(\pi,\phi) = -b_{\mathrm{B}_\nu}(\pi,\phi) = -1$, for $\phi \in [0,2\pi]$ and integers $\nu \geq 1$. For $\nu = 1,2,3,4$, these colourings correspond to the colourings illustrated in Figure 2.4, whose correlations are plotted in Figure 2.5. Similar to the colourings A_ν, we expect the correlations for these colourings to oscillate between local maximums and minimums at periodic intervals, close to the value $\frac{\pi}{2\nu}$ in this case. These intuitions are confirmed to some extent, as observed in Figure 2.5, in particular for big ν and small θ. For example, the first local maximum of $C_4(\theta)$ is very close to $\theta = \frac{\pi}{8}$.

It would be interesting to investigate numerically colourings A_ν, colourings B_ν that we have not explored here, and variations of these, for example, in the lines of colourings 2_Δ and 3_δ defined by (2.17). However, we do not expect these colourings to reduce drastically the upper bounds $\theta^{\mathrm{w}}_{\max} \leq 0.386\pi$ and $\theta^{\mathrm{s}}_{\max} \leq 0.345\pi$, for the reasons previously mentioned. The different class of colourings D_ν, illustrated in Figure 2.9, seems more promising in producing correlations $C_{\mathrm{D}_\nu}(\theta) < C_1(\theta)$ for smaller values of θ.

Our intuition about the colourings D_ν is that for angles θ_{D_ν}, whose order of magnitude is schematized in Figure 2.9, $C_{\mathrm{D}_\nu}(\theta_{\mathrm{D}_\nu})$ is a local minimum. We expect that $C_{\mathrm{D}_\nu}(\theta_{\mathrm{D}_\nu}) < C_1(\theta_{\mathrm{D}_\nu})$ for some values of ν. This intuition is based on the observation from Figure 2.9 that for circles with angles close to θ_{D_ν} there seems to be a considerably big area for which the centre of these circles, in one sphere, and points on these circles, in the oppositely coloured sphere, are

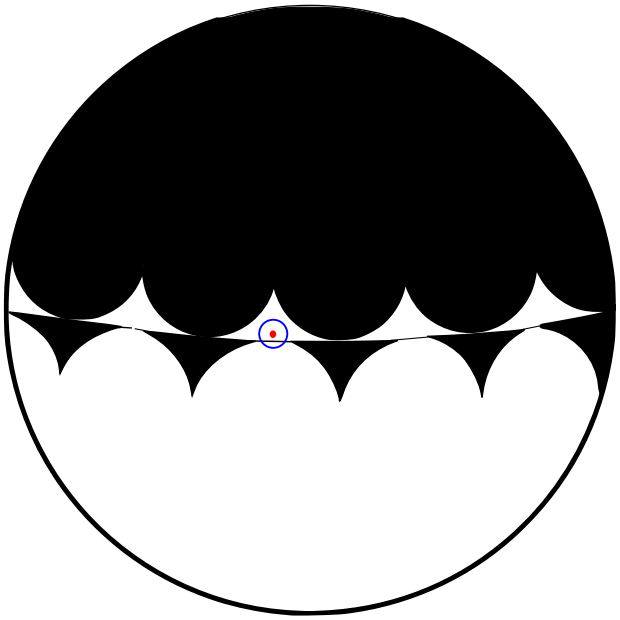


Figure 2.9: Colourings D_ν. The colouring for one sphere is illustrated in the figure. The other sphere is coloured oppositely. The equator is touched on a single point by circular curves that define the boundary between black and white regions. These curves correspond to identical half-circles that repeat periodically at azimuthal angles with intervals of $\frac{2\pi}{\nu}$, for odd positive integers ν. That is, an odd number ν of these half-circles go around the equator circumference (the figure illustrates the case $\nu = 9$). The colouring is antipodal. It is observed that the white region of the southern hemisphere is obtained by reflecting the black region of the northern hemisphere through the equatorial plane and then rotating the obtained region by an azimuthal angle equal to $\frac{\pi}{\nu}$. The small blue circle and the red centre point represent Alice's and Bob's measurement axes separated by an angle of the order of magnitude of θ_{D_ν}, for which we expect that $C_{\mathrm{D}_\nu}(\theta_{\mathrm{D}_\nu})$ is a local minimum.

anticorrelated. Curves different to half-circles defining the boundary between black and white regions could be considered in order to maximize the quantity $-C_{\mathrm{D}_\nu}(\theta_{\mathrm{D}_\nu}) + C_1(\theta_{\mathrm{D}_\nu})$. We expect bigger anticorrelations to be achieved with convex curves compared to concave curves, in the northern hemisphere. The circular curves can be defined explicitly using (2.10) and (2.11). If the colourings D_ν were such that θ_{D_ν} is a strictly decreasing function of ν with $\lim_{\nu\to\infty}\theta_{\mathrm{D}_\nu} = 0$, as suggested by Figure 2.9, and $C_{\mathrm{D}_\nu}(\theta_{\mathrm{D}_\nu}) < C_1(\theta_{\mathrm{D}_\nu})$ for all ν big enough, the WHCMH and the SHCMH would be false. It is perhaps more reasonable to expect that $C_{\mathrm{D}_\nu}(\theta_{\mathrm{D}_\nu}) < C_1(\theta_{\mathrm{D}_\nu})$ for some values of ν, but not for ν arbitrarily big. It would be interesting to investigate these colourings numerically and to find formal analytic arguments that support or discard these geometric intuitions.

Further analytic investigation of the correlations produced by antipodal colourings could give Bell inequalities stronger than those stated in Theorem 2.1. A possible research direction is to consider sets of measurement choices that are along curves on the sphere more complicated than those illustrated in Figure 2.3, which were used to prove Theorem 2.1. Consider the set of measurement choices corresponding to projections on states with Bloch vectors $\vec{a}_i^{(j)}$, performed by Alice, and $\vec{b}_k^{(l)}$, performed by Bob, that are illustrated in Figure 2.10. The points $\vec{a}_i^{(j)}$, $\vec{b}_k^{(l)}$ on the unit spheres are defined so that any pair of adjacent points is separated by the same angle $\theta_{N,M,L} \in \left(0, \frac{\pi}{2}\right)$ and that two series of points $\vec{a}_i^{(j)}$ are antipodal. Consider integers $N \geq 2$, $M \geq 2$ and $L = 0, 1, \ldots, \left\lceil \frac{M-3}{2} \right\rceil$. Let the spherical coordinates for these points be $\vec{a}_i^{(j)} = (\epsilon_i, \phi_j)$, $\vec{b}_k^{(l)} = (\alpha_k, \beta_l)$, where $\epsilon_i, \alpha_k \in [0, \pi]$ are polar angles and $\phi_j = 2j\Gamma \bmod 2\pi$, $\beta_l = (2l+1)\Gamma \bmod 2\pi$ are azimuthal angles with $\Gamma \equiv \frac{(2L+1)\pi}{2M}$ for $i = 0, 1, \ldots, N$, $j = 0, 1, \ldots, M$, $k = 0, 1, \ldots, N-1$, $l = 0, 1, \ldots, M-1$, such that $\epsilon_{i+1} > \epsilon_i$ for $i = 0, 1, \ldots, N-1$, $\alpha_{k+1} > \alpha_k$ for $k = 0, 1, \ldots, N-2$, $\epsilon_0 = 0$ and $\epsilon_N = \pi$; the four angles along the great circles passing between $\vec{b}_k^{(l)}$ and the four points $\vec{a}_i^{(j)}$ with $(i = k, j = l), (i = k+1, j = l), (i = k, j = l+1), (i = k+1, j = l+1)$ for $k = 0, 1, \ldots, N-1$, $l = 0, 1, \ldots, M-1$ are equal and are defined as $\theta_{N,M,L}$. Since $\epsilon_0 = 0$, all points $\vec{a}_0^{(j)}$ are the same and correspond to the north pole; we define them as $\vec{a}_0$. Similarly, since $\epsilon_N = \pi$, all points $\vec{a}_N^{(j)}$ are the same and correspond to the south pole; we define them as $\vec{a}_N$. It follows that

$$\epsilon_{N-i} = \pi - \epsilon_i, \qquad \alpha_{N-1-k} = \pi - \alpha_k, \tag{2.24}$$

for $i = 0, 1, \ldots, N$ and $k = 0, 1, \ldots, N-1$. Let the measurement outcomes be described by an LHVT defined by an antipodal colouring $x \in \mathcal{X}$. For simplicity, we define $a_0 \equiv a_x(\vec{a}_0)$, $a_N \equiv a_x(\vec{a}_N)$, $a_i^{(j)} \equiv a_x(\vec{a}_i^{(j)})$ for $i = 1, 2, \ldots, N-1$, $j = 0, 1, \ldots, M$, and $b_k^{(l)} \equiv b_x(\vec{b}_k^{(l)})$ for $k = 0, 1, \ldots, N-1$, $l = 0, 1, \ldots, M-1$. We consider the products $a_i^{(j)} b_k^{(l)}$ for all pairs of vectors $\vec{a}_i^{(j)}$ and $\vec{b}_k^{(l)}$ separated by an angle $\theta_{N,M,L}$. The correlation is

$$C = \frac{1}{(4N-2)M} \sum_{l=0}^{M-1} \left[\sum_{k=1}^{N-2} b_k^{(l)} \left(a_k^{(l)} + a_k^{(l+1)} + a_{k+1}^{(l)} + a_{k+1}^{(l+1)} \right) + b_0^{(l)} \left(a_0 + a_1^{(l)} + a_1^{(l+1)} \right) + b_{N-1}^{(l)} \left(a_N + a_{N-1}^{(l)} + a_{N-1}^{(l+1)} \right) \right]. \tag{2.25}$$

From (2.24) and the definition of $\vec{a}_i^{(j)}$, we have that $\vec{a}_N$ is antipodal to $\vec{a}_0$ and $\vec{a}_{N-i}^{(M)}$ is antipodal to $\vec{a}_i^{(0)}$, for $i = 1, 2, \ldots, N-1$. Thus, since the colouring x satisfies the antipodal property, we have $a_N = -a_0$ and $a_{N-i}^{(M)} = -a_i^{(0)}$, for $i = 1, 2, \ldots, N-1$. Hence, after arranging terms, we have

$$\begin{aligned} C = \frac{1}{(4N-2)M} \Bigg\{ & \sum_{l=0}^{M-2} \left[b_0^{(l)} \left(a_0 + a_1^{(l)} + a_1^{(l+1)} \right) + \sum_{k=1}^{N-2} b_k^{(l)} \left(a_k^{(l)} + a_k^{(l+1)} + a_{k+1}^{(l)} + a_{k+1}^{(l+1)} \right) \right. \\ & \left. + b_{N-1}^{(l)} \left(-a_0 + a_{N-1}^{(l)} + a_{N-1}^{(l+1)} \right) \right] + b_0^{(M-1)} \left(a_0 + a_1^{(M-1)} - a_{N-1}^{(0)} \right) \\ & + \sum_{k=1}^{N-2} b_k^{(M-1)} \left(a_k^{(M-1)} - a_{N-k}^{(0)} + a_{k+1}^{(M-1)} - a_{N-k-1}^{(0)} \right) \\ & + b_{N-1}^{(M-1)} \left(-a_0 + a_{N-1}^{(M-1)} - a_1^{(0)} \right) \Bigg\}. \end{aligned} \tag{2.26}$$

We expect that a bound $C \geq B_{N,M}$ can be found from the previous expression. If so, after averaging over random rotations of the Bloch sphere, this would imply a bound $C_x(\theta_{N,M,L}) \geq B_{N,M}$ for all antipodal colourings x, which would also imply the bound $C_x(\theta_{N,M,L}) \leq -B_{N,M}$ by reversing the colouring of one sphere. We expect such bounds to be tighter than the bounds given by Theorem 2.1, for appropriate values of N, M and L.

A different analytic approach to prove Bell inequalities stronger than those

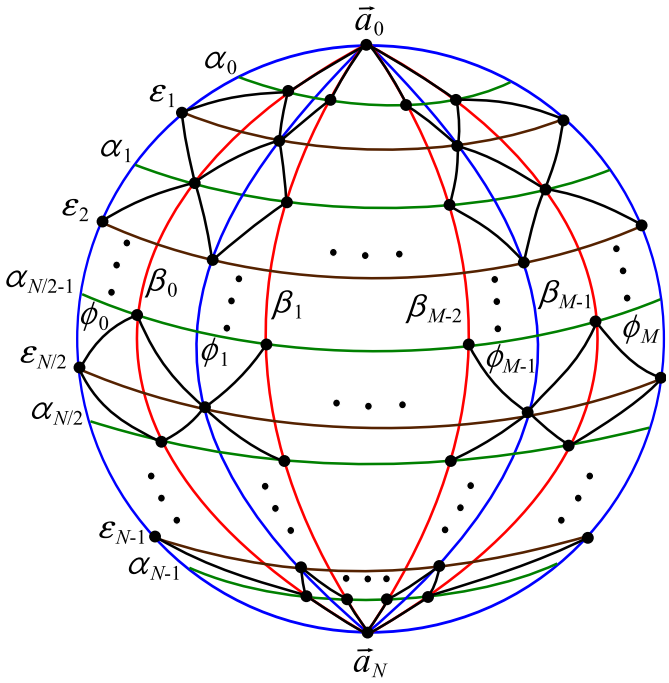


Figure 2.10: Diagram of points $\vec{a}_i^{(j)}$, $\vec{b}_k^{(l)}$ in the unit sphere that define angles $\theta_{N,M,L}$ for integers $N \geq 2$, $M \geq 2$ and $L = 0, 1, \ldots, \left\lceil \frac{M-3}{2} \right\rceil$. The figure represents the case N even and $L = 0$. The blue and red curves are meridians with azimuthal coordinates $\phi_j = 2j\Gamma \mod 2\pi$ and $\beta_l = (2l+1)\Gamma \mod 2\pi$, respectively, with $\Gamma \equiv \frac{(2L+1)\pi}{2M}$ for $j = 0, 1, \ldots, M$ and $l = 0, 1, \ldots, M-1$. The brown and green curves are circles defined by constant polar angles ϵ_i and α_k, respectively, for $i = 1, 2, \ldots, N-1$ and $k = 0, 1, \ldots, N-1$. The points $\vec{a}_i^{(j)} = (\epsilon_i, \phi_j)$ are the intersection of the corresponding blue and brown curves. Similarly, the points $\vec{b}_k^{(l)} = (\alpha_k, \beta_l)$ are the intersection of the corresponding red and green curves. The points $\vec{a}_0$ and $\vec{a}_N$ correspond to the south and the north poles, respectively. The black curves represent arcs of great circles with the same angles, defined as $\theta_{N,M,L}$.

given by Theorem 2.1 and possibly to prove the WHCMH and the SHCMH consists in using techniques of geometric combinatorics for sets in $\mathbb{R}^n$ [97, 98].

Finally, we would like to stress that the key idea considered in this chapter is the investigation of Bell inequalities defined by continuous parameters. Some interesting recent results have been obtained with this approach [72]. This work can be extended to multipartite scenarios and to systems of higher dimension. These ideas can also be explored in terms of nonlocal games with continuous inputs [95].

Chapter 3

Bound on the Success Probability of Port-Based Teleportation from No-Cloning and No-Signalling

3.1 Introduction

It is interesting to investigate the limitations and possibilities on quantum information processing tasks that can be derived directly from no-signalling and other fundamental principles of quantum theory. There are important results that have been obtained with this approach. The maximum fidelity achieved by quantum cloning machines can be deduced from the no-signalling principle [37]. The security of quantum key distribution can be guaranteed as long as the no-signalling principle is satisfied [27]. The information causality principle [71] implies the Cirel'son bound for the CHSH inequality. The maximum guessing probability in quantum state discrimination can be derived from the no-signalling principle [73].

In this chapter, we present a proof, published by us in [99], of an upper bound on the success probability of a class of teleportation protocols, denoted as port-based teleportation. The proof is based on the no-cloning theorem and the no-signalling principle.

3.1.1 Port-Based Teleportation

Quantum teleportation is a fundamental protocol of quantum information theory in which an unknown quantum state $|\psi\rangle$ is destroyed at its original location by Alice and reconstructed at another location by Bob. The original quantum teleportation protocol [13] works as follows: Alice and Bob must initially share a maximally entangled state, Alice applies a Bell measurement on her systems, she communicates her measurement outcome to Bob, who then applies a unitary correction operation according to Alice's message (see section 1.2.5.2).

In this chapter, we consider a different type of teleportation protocol, denoted as *port-based teleportation* (PBT). PBT was devised by Ishizaka and Hiroshima [100, 101] with the purpose of implementing a universal programmable quantum processor that succeeds with probability arbitrarily close to unity; this task can be achieved using standard teleportation too, but with a very small success probability for input states of big dimension [102].

We consider general PBT protocols, which allow Alice to teleport an unknown quantum state $|\psi\rangle$ to one of N ports at Bob's site. PBT requires that Alice and Bob share quantum entanglement and consists in the following steps. Alice applies a measurement with outcome $k \in \{0, 1, \ldots, N\}$; if $k = 0$, teleportation fails, otherwise $|\psi\rangle$ is teleported to the kth port. Alice communicates k to Bob, who then discards the states at ports with index distinct to k. No further correction operations are required; this is an advantage over standard teleportation that makes PBT useful in various quantum information tasks. In the probabilistic version of PBT, $|\psi\rangle$ is teleported perfectly but with a success probability $p < 1$; in the deterministic version, the outcome $k = 0$ never occurs but the fidelity of the teleported state is smaller than unity [100, 101].

Besides its use as a universal programmable quantum processor, PBT can be used to implement instantaneous nonlocal quantum computation (INLQC), reducing exponentially the amount of needed entanglement compared to schemes based on standard teleportation [85]. INLQC is the application of a nonlocal unitary operation U on a state $|\psi\rangle$ shared by two or more distant parties with a single round of classical communication (CC); see Figure 1.4 and the discussion in section 1.3.2.2. If two rounds of CC are allowed, U can be implemented trivially

as follows: Alice teleports her part of $|\psi\rangle$ to Bob, who then applies U to $|\psi\rangle$, now in his location, and then teleports Alice's part of the state back to her. However, it is not trivial to complete this task with only one round of CC. This task can be implemented for a general unitary U and a state of arbitrary dimension using a recursive scheme based on standard teleportation, which consumes an amount of entanglement growing double exponentially with the number of qubits n of the input state $|\psi\rangle$ [82,84]. However, a scheme based on PBT allows the implementation of INLQC with an amount of entanglement growing only exponentially with n [85].

INLQC has application to other distributed quantum tasks: it allows the implementation of instantaneous nonlocal measurements (INLM) and also breaks the security of position-based quantum cryptography (PBQC) and some quantum tagging schemes [86–92]. INLM is the measurement of a nonlocal observable in a distributed quantum state with a single round of CC [77–84]. Quantum tagging [86–89, 93] and PBQC [91, 92] are cryptographic tasks that rely on quantum information processing and relativistic constraints with the goals of verifying the location of an object and providing secure communication with a party at a given location, respectively.

3.2 The Bound

In the rest of this chapter, we derive an upper bound on the success probability p of probabilistic PBT of an n-qubits state as a function of n and the number of ports N:

$$p \leq \frac{N}{4^n + N - 1}. \tag{3.1}$$

The proof is based on a version of the no-cloning theorem, which we state and prove in section 3.4, and the no-signalling principle. Our bound agrees with the maximum success probability obtained in [101] for the particular case $n = 1$:

$$p_{\max} = \frac{N}{3 + N}. \tag{3.2}$$

Thus, we confirm the hypothesis presented in [101] that (3.2) can be derived from fundamental laws of physics. It is an interesting open problem to find a probabilistic PBT protocol for the case $n > 1$ and to see whether our bound is achievable.

Comparing (3.1) and (3.2), we see that $(p_{\max})^n$ can be bigger than the upper bound on p, which means that applying PBT individually to each qubit of the input state $|\psi\rangle$ can give a higher success probability than applying PBT globally to $|\psi\rangle$. However, we justify the restriction that $|\psi\rangle$ must be localized to a single port by noting that the advantage of PBT as described here, at least for implementing a universal programmable quantum processor and INLQC, is that, before receiving Alice's message, Bob can apply the desired quantum operation on the state at every port, after which, $|\psi\rangle$ is transformed as desired. Clearly, this advantage is lost if the qubits of $|\psi\rangle$ spread among different ports, as done, for example, in the protocols presented in [103].

3.3 Summary of the Proof

Before summarizing our proof of the bound (3.1), it is useful to give a general description of the PBT protocol (see Figure 3.1). For simplicity of the exposition we consider a pure input state $|\psi\rangle_a \in \mathcal{H}_a$. Due to the linearity of quantum theory, the protocol works for mixed states too. Alice and Bob share a fixed entangled state $|\xi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, which is independent of $|\psi\rangle$ because this is arbitrary and unknown. Bob has N ports $\{B_j\}_{j=1}^N$, hence $\mathcal{H}_B = \bigotimes_{j=1}^{N} \mathcal{H}_{B_j}$, where $\dim\mathcal{H}_{B_j} = \dim\mathcal{H}_a = 2^n \ \forall j \in \{1, \ldots, N\}$. The system A includes any ancilla held by Alice and so has an arbitrarily big dimension. However, in [100, 101], $\mathcal{H}_A = \bigotimes_{j=1}^{N} \mathcal{H}_{A_j}$ and $\dim\mathcal{H}_{A_j} = \dim\mathcal{H}_a \ \forall j \in \{1, \ldots, N\}$. We follow a notation in which subindex a is written in $|\psi\rangle_a$ only when we wish to emphasize that the system a is in the state $|\psi\rangle$, similarly for other states and systems. The initial global state is

$$|G\rangle_{aAB} = |\psi\rangle_a |\xi\rangle_{AB}. \tag{3.3}$$

Alice applies a generalized measurement, which in general can be decomposed into a unitary operation U acting jointly on a and A, followed by a projective measurement. Alice obtains the outcome $k \in \{1, \ldots, N\}$ with probability $q_k > 0$ and $k = 0$ with probability $1 - \sum_{k=1}^{N} q_k$. Notice that since we consider that A has arbitrary dimension, we can include any ancilla as part of A that purifies the output states after any outcome $k \in \{0, 1, \ldots, N\}$. If $k \neq 0$, the global state is transformed into

$$|G_k\rangle_{aAB} = |\psi\rangle_{B_k} |R_k\rangle_{aA\tilde{B}_k}, \tag{3.4}$$

where $\tilde{B}_k \equiv B_1 B_2 \cdots B_{k-1} B_{k+1} B_{k+2} \cdots B_N$, hence, the state $|\psi\rangle$ is teleported to the port B_k. However, if $k = 0$, PBT fails; in this case we denote the final state as

$$|G_0\rangle_{aAB} = |F^{(\psi)}\rangle_{aAB}. \tag{3.5}$$

The total success probability is

$$p \equiv \sum_{j=1}^{N} q_j. \tag{3.6}$$

Now we are able to summarize the proof. First, in section 3.4, we present a version of the no-cloning theorem that allows us to show that the probabilities q_k and the states $|R_k\rangle$ cannot depend on $|\psi\rangle$, while the state $|F^{(\psi)}\rangle$ must do, as the notation suggests. Second, in section 3.5, we use the no-signalling principle to show that the state η_j of port B_j before implementing PBT must be of the form

$$\eta_j = q_j |\psi\rangle\langle\psi| + \sum_{\substack{i=1 \\ i \neq j}}^{N} q_i \gamma_{j,i} + (1 - p)\omega_j^{(\psi)}, \tag{3.7}$$

where $\gamma_{j,i}$ and $\omega_j^{(\psi)}$ are the states to which B_j transforms into after the outcomes $k = i \notin \{0, j\}$ and $k = 0$ are obtained, respectively. Since η_j, $\gamma_{j,i}$ and $\omega_j^{(\psi)}$ are reduced states of $|\xi\rangle$, $|R_i\rangle$ and $|F^{(\psi)}\rangle$, respectively, η_j and $\gamma_{j,i}$ do not depend on $|\psi\rangle$, while $\omega_j^{(\psi)}$ does. Third, we use the independence of these states from $|\psi\rangle$ and Equation (3.7) to show that if there exists a protocol that achieves success probability q_j for some states η_j and $\gamma_{j,i}$ then there exists a protocol that achieves

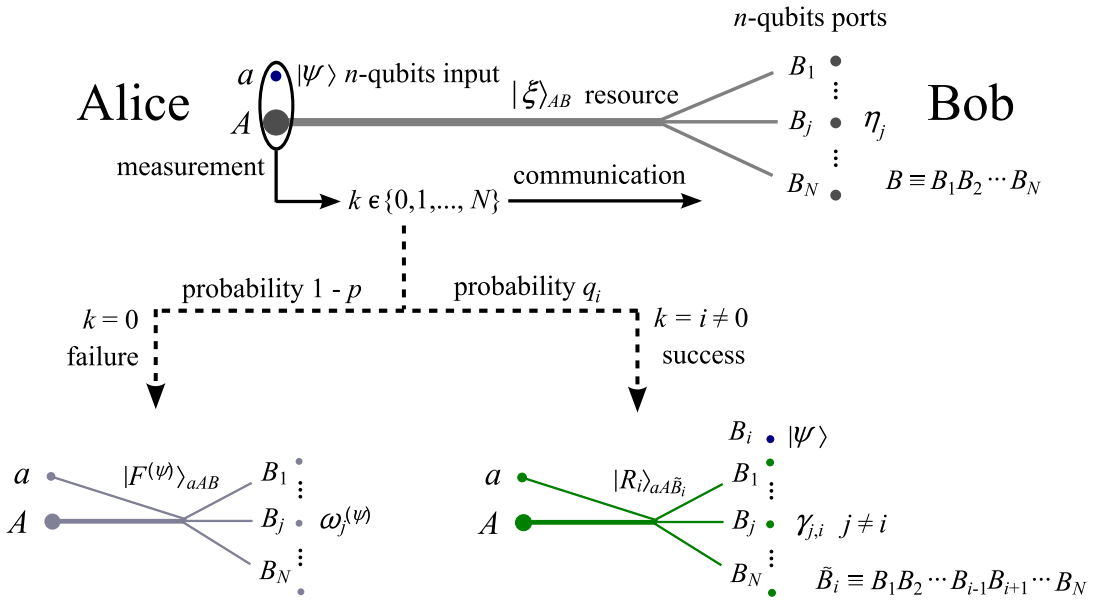


Figure 3.1: Probabilistic port-based teleportation. Alice teleports an unknown $n-$qubits state $|\psi\rangle$ to one of N ports at Bob's site. Alice applies a measurement and sends Bob the outcome k. The outcome $k = 0$, indicating failure, is obtained with a nonzero probability. If $k \neq 0$, Bob only needs to select the kth port in order to obtain the state perfectly. Alice's and Bob's resource is an arbitrary entangled state $|\xi\rangle_{AB}$. Bob's system B consists of N ports, which are $n-$qubits systems in states η_j, for $j = 0, 1, \ldots, N-1$. The global system aAB transforms into the state $|F^{(\psi)}\rangle_{aAB}$ if $k = 0$, or into the states $|\psi\rangle_{B_i}|R_i\rangle_{aA\tilde{B}_i}$ if $k = i \neq 0$. The states of the port B_j after an outcome $k = 0$ and $k = i \notin \{0, j\}$ are obtained are denoted as $\omega_j^{(\psi)}$ and $\gamma_{j,i}$, respectively. The states $|F^{(\psi)}\rangle$ and $\omega_j^{(\psi)}$ depend on $|\psi\rangle$, while the states $|R_i\rangle$ and $\gamma_{j,i}$ do not.

the same success probability and satisfies

$$\eta_j = \gamma_{j,i} = \frac{I}{2^n}. \tag{3.8}$$

Fourth, in section 3.6, we assume (3.8) and present a protocol in which Alice tries to send Bob a random message of $2n$ bits. This protocol combines the superdense coding protocol [12] and a modified PBT protocol in which Alice holds every port except for B_j, which is held by Bob, but does not allow communication. We show that this protocol succeeds with probability

$$p'_j = q_j + \frac{1}{4^n}(p - q_j) + (1 - p)r_j, \tag{3.9}$$

for some probability r_j. Since there is not communication in such a protocol, the no-signalling principle implies that Bob cannot obtain any information about Alice's message. This means that Bob can only obtain the correct message with the probability of making a random guess: $p'_j = \frac{1}{4^n}$.[1] Thus, we have

$$q_j + \frac{1}{4^n}(p - q_j) + (1 - p)r_j = \frac{1}{4^n}. \tag{3.10}$$

Summing over $j \in \{1, 2, \ldots, N\}$ and using (3.6), we obtain that

$$p = f_{n,N}(R),$$

where $R \equiv \sum_{j=1}^{N} r_j$ and

$$f_{n,N}(R) \equiv \left(1 + \frac{4^n - 1}{N - 4^n R}\right)^{-1}.$$

It is straightforward to obtain that the condition $0 \leq p \leq 1$ is satisfied only if $R \leq \frac{N}{4^n}$. Since the function $f_{n,N}(R)$ decreases monotonically with R in the range $\left[0, \frac{N}{4^n}\right]$, we have that $f_{n,N}(R) \leq f_{n,N}(0) = \frac{N}{N+4^n-1}$. Thus, we obtain the bound (3.1):

$$p \leq \frac{N}{4^n + N - 1}.$$

[1] This is shown in Equation (1.63) in section 1.3.2.

3.4 A More General No-Cloning Theorem

The following theorem is in the spirit of the no-cloning theorem [8, 9], in a probabilistic [33] and a stronger [10, 11] version, and tells us that it is impossible to extract any information from a single copy of an unknown quantum state without modifying it.

Theorem 3.1. *Consider a physical operation O that consists in a unitary operation U acting on a single copy of an unknown pure quantum state $|\psi\rangle_a \in \mathcal{H}_a$ and a fixed initial state $|\xi\rangle_b \in \mathcal{H}_b$ of an auxiliary system b of arbitrarily big dimension, followed by a projective measurement on b (or a subsystem of b). Let O induce a transformation T_k:*

$$|\psi\rangle_a|\xi\rangle_b \longrightarrow |\psi\rangle_a|R_k^{(\psi)}\rangle_b,$$

with probability $q_k^{(\psi)} > 0$, for $k \in \{1, 2, \ldots, N\}$, and a transformation T_0:

$$|\psi\rangle_a|\xi\rangle_b \longrightarrow |F^{(\psi)}\rangle_{ab},$$

with probability $1-\sum_{k=1}^{N} q_k^{(\psi)}$, for all $|\psi\rangle_a \in \mathcal{H}_a$, in which the index $j \in \{0, 1, \ldots, N\}$ of the induced transformation T_j is known after O is completed. The physical operation O is possible only if

$$q_k^{(\psi)} = q_k^{(\phi)} \equiv q_k, \qquad |R_k^{(\psi)}\rangle_b = |R_k^{(\phi)}\rangle_b \equiv |R_k\rangle_b,$$

for all $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$ and $k \in \{1, 2, \ldots, N\}$. Additionally, if $\sum_{k=1}^{N} q_k < 1$, the operation O must satisfy

$$\langle F^{(\phi)}|F^{(\psi)}\rangle = \langle\phi|\psi\rangle,$$

for all $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$.

Proof. By definition, the physical operation O corresponds to a unitary operation U acting on the input system ab, followed by a projective measurement on b (or a subsystem of b). In principle, more than one measurement outcome could correspond to a particular induced transformation. But, given that the output states are pure, only one outcome must be associated to a particular transformation. Consider for example that two or more outcomes induced T_0. In that case, the

output system ab of the transformation T_0 would be in a mixed state. In order to exclude this possibility, the projective measurement must correspond exactly to $N+1$ outcomes. Let I_a and I_b be the identity acting on $\mathcal{H}_a$ and $\mathcal{H}_b$, respectively, and Π_b^j be the projector acting on $\mathcal{H}_b$ that induces the transformation T_j, for $j = 0, 1, \ldots, N$. We have that $\sum_{j=0}^{N} \Pi_b^j = I_b$, and that

$$(I_a \otimes \Pi_b^0) U |\psi\rangle_a |\xi\rangle_b = \sqrt{1 - p^{(\psi)}} |F^{(\psi)}\rangle_{ab}, \tag{3.11}$$

$$(I_a \otimes \Pi_b^k) U |\psi\rangle_a |\xi\rangle_b = \sqrt{q_k^{(\psi)}} |\psi\rangle_a |R_k^{(\psi)}\rangle_b, \tag{3.12}$$

with $q_k^{(\psi)} > 0$ and $p^{(\psi)} \equiv \sum_{k=1}^{N} q_k^{(\psi)}$, for all $|\psi\rangle_a \in \mathcal{H}_a$ and $k \in \{1, 2, \ldots, N\}$. The unitary operation U is such that

$$U|\psi\rangle_a |\xi\rangle_b = \sqrt{1 - p^{(\psi)}} |F^{(\psi)}\rangle_{ab} + \sum_{k=1}^{N} \sqrt{q_k^{(\psi)}} |\psi\rangle_a |R_k^{(\psi)}\rangle_b, \tag{3.13}$$

for all $|\psi\rangle_a \in \mathcal{H}_a$. Notice that Equations (3.11) – (3.13) apply to the general case in which the projective measurement is implemented on any subsystem of b. The only requirement for b is that its dimension is not smaller than $N + 1$. This can always be satisfied because b has an arbitrarily big dimension, by definition.

Consider any pair of states $|\phi\rangle_a, |\psi\rangle_a \in \mathcal{H}_a$. There exists a state $|\tau\rangle_a \in \mathcal{H}_a$ such that $\langle\psi|\tau\rangle = 0$, for which we have

$$|\phi\rangle_a = e^{i\omega}\big(\sqrt{Q}|\psi\rangle_a + \sqrt{1-Q}|\tau\rangle_a\big), \tag{3.14}$$

for some $\omega \in \mathbb{R}$ and $0 \leq Q \leq 1$. It follows that

$$\begin{aligned} U|\phi\rangle_a |\xi\rangle_b &= U\Big[e^{i\omega}\big(\sqrt{Q}|\psi\rangle_a + \sqrt{1-Q}|\tau\rangle_a\big)\Big]|\xi\rangle_b \\ &= e^{i\omega}\sqrt{Q}U|\psi\rangle_a|\xi\rangle_b + e^{i\omega}\sqrt{1-Q}U|\tau\rangle_a|\xi\rangle_b, \\ &= e^{i\omega}\sqrt{Q}\Bigg(\sqrt{1-p^{(\psi)}}|F^{(\psi)}\rangle_{ab} + \sum_{k=1}^{N}\sqrt{q_k^{(\psi)}}|\psi\rangle_a|R_k^{(\psi)}\rangle_b\Bigg) \\ &\quad + e^{i\omega}\sqrt{1-Q}\Bigg(\sqrt{1-p^{(\tau)}}|F^{(\tau)}\rangle_{ab} + \sum_{k=1}^{N}\sqrt{q_k^{(\tau)}}|\tau\rangle_a|R_k^{(\tau)}\rangle_b\Bigg), \end{aligned} \tag{3.15}$$

where in the first line we used (3.14), in the second line we used the linearity of unitary evolution, and in the third line we used (3.13). On the other hand, we have

$$\begin{aligned} U|\phi\rangle_a|\xi\rangle_b &= \sqrt{1-p^{(\phi)}}|F^{(\phi)}\rangle_{ab} + \sum_{k=1}^{N}\sqrt{q_k^{(\phi)}}|\phi\rangle_a|R_k^{(\phi)}\rangle_b \\ &= \sqrt{1-p^{(\phi)}}|F^{(\phi)}\rangle_{ab} + \sum_{k=1}^{N}\sqrt{q_k^{(\phi)}}\Big[e^{i\omega}\big(\sqrt{Q}|\psi\rangle_a + \sqrt{1-Q}|\tau\rangle_a\big)\Big]|R_k^{(\phi)}\rangle_b, \end{aligned} \tag{3.16}$$

where in the first line we used (3.13) and in the second line we used (3.14).

Consider the following properties, which are shown at the end of this proof,

$$\begin{aligned} {}_b\langle R_k^{(\phi)}|R_{k'}^{(\psi)}\rangle_b &= 0, \text{ for } k,k' \in \{1,2,\ldots,N\} \text{ with } k \neq k', \quad (3.17) \\ {}_{ab}\langle F^{(\phi)}|\big(|\psi\rangle_a|R_k^{(\psi)}\rangle_b\big) &= 0, \text{ if } p^{(\phi)} < 1, \text{ for } k \in \{1,2,\ldots,N\}, \quad (3.18) \end{aligned}$$

for all $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$. Taking the inner product ${}_a\langle\psi|\,{}_b\langle R_k^{(\psi)}|U|\phi\rangle_a|\xi\rangle_b$ in (3.15) and (3.16), and using (3.17) and (3.18), together with the condition $\langle\psi|\tau\rangle = 0$, we have that satisfaction of both expressions (3.15) and (3.16) requires

$$\sqrt{Qq_k^{(\psi)}} = \sqrt{Qq_k^{(\phi)}}\langle R_k^{(\psi)}|R_k^{(\phi)}\rangle. \tag{3.19}$$

Thus, if $\langle\phi|\psi\rangle \neq 0$, which from (3.14) means that $Q > 0$, it follows that

$$q_k^{(\psi)} = q_k^{(\phi)}\big|\langle R_k^{(\psi)}|R_k^{(\phi)}\rangle\big|^2. \tag{3.20}$$

Since this is valid for any pair of states $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$ such that $\langle\phi|\psi\rangle \neq 0$, a similar expression is obtained by interchanging the roles of $|\psi\rangle$ and $|\phi\rangle$ in (3.20), which is

$$q_k^{(\phi)} = q_k^{(\psi)}\big|\langle R_k^{(\psi)}|R_k^{(\phi)}\rangle\big|^2. \tag{3.21}$$

From (3.19) – (3.21), it follows that

$$q_k^{(\psi)} = q_k^{(\phi)}, \quad |R_k^{(\psi)}\rangle_b = |R_k^{(\phi)}\rangle_b, \tag{3.22}$$

for all $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$ satisfying $\langle\phi|\psi\rangle \neq 0$ and all $k \in \{1, 2, \ldots, N\}$. Since the input state $|\psi\rangle_a$ is arbitrary and unknown, this property also applies for $|\psi\rangle_a, |\phi\rangle_a$ with $\langle\phi|\psi\rangle = 0$. To see this consider arbitrary states $|\psi\rangle_a, |\phi\rangle_a, |\phi'\rangle_a \in \mathcal{H}_a$ such that $\langle\phi'|\psi\rangle = 0$, $\langle\phi|\psi\rangle \neq 0$ and $\langle\phi|\phi'\rangle \neq 0$. Applying (3.22) to the three different pairs of states from the set $\{|\psi\rangle_a, |\phi\rangle_a, |\phi'\rangle_a\}$ we obtain that (3.22) holds for all $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$ and all $k \in \{1, 2, \ldots, N\}$, as claimed.

Consider the case $p^{(\psi)} < 1$, which from (3.22) implies that $p^{(\phi)} = p^{(\psi)} < 1$. Taking the inner product of $U|\psi\rangle_a|\xi\rangle_b$ and $U|\phi\rangle_a|\xi\rangle_b$, applying (3.13), and using (3.17), (3.18) and (3.22), we obtain

$$\langle F^{(\phi)}|F^{(\psi)}\rangle = \langle\phi|\psi\rangle, \tag{3.23}$$

for all $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$, as claimed.

Now we show (3.17). Let $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$ and $k, k' \in \{1, 2, \ldots, N\}$, with $k \neq k'$. Let V_a be the unitary operation acting on $\mathcal{H}_a$ that satisfies $|\phi\rangle_a = V_a|\psi\rangle_a$. From (3.12), we have

$$\begin{aligned}
\sqrt{q_k^{(\phi)} q_{k'}^{(\psi)}}\langle R_k^{(\phi)}|R_{k'}^{(\psi)}\rangle &= \sqrt{q_k^{(\phi)} q_{k'}^{(\psi)}}\,{}_a\langle\phi|\,{}_b\langle R_k^{(\phi)}|\big(|\phi\rangle_a|R_{k'}^{(\psi)}\rangle_b\big) \\
&= \sqrt{q_k^{(\phi)} q_{k'}^{(\psi)}}\,{}_a\langle\phi|\,{}_b\langle R_k^{(\phi)}|(V_a \otimes I_b)|\psi\rangle_a|R_{k'}^{(\psi)}\rangle_b \\
&= {}_a\langle\phi|\,{}_b\langle\xi|U^\dagger(I_a \otimes \Pi_b^k)(V_a \otimes I_b)(I_a \otimes \Pi_b^{k'})U|\psi\rangle_a|\xi\rangle_b \\
&= {}_a\langle\phi|\,{}_b\langle\xi|U^\dagger(V_a \otimes \Pi_b^k\Pi_b^{k'})U|\psi\rangle_a|\xi\rangle_b \\
&= 0,
\end{aligned} \tag{3.24}$$

where in the last line we used that $\Pi_b^k\Pi_b^{k'} = 0$ because $\{\Pi_b^j\}_{j=0}^N$ are projectors and $k \neq k'$. Equation (3.17) follows because $q_k^{(\phi)} > 0$ and $q_{k'}^{(\psi)} > 0$.

Finally, we show (3.18). Let $|\psi\rangle_a, |\phi\rangle_a \in \mathcal{H}_a$ and $k \in \{1, 2, \ldots, N\}$, with $p^{(\phi)} < 1$. From (3.11) and (3.12), we have

$$\begin{aligned}
\sqrt{\big(1 - p^{(\phi)}\big)q_k^{(\psi)}}\,{}_{ab}\langle F^{(\phi)}|\big(|\psi\rangle_a|R_k^{(\psi)}\rangle_b\big) &= {}_a\langle\phi|\,{}_b\langle\xi|U^\dagger(I_a \otimes \Pi_b^0)(I_a \otimes \Pi_b^k)U|\psi\rangle_a|\xi\rangle_b \\
&= {}_a\langle\phi|\,{}_b\langle\xi|U^\dagger(I_a \otimes \Pi_b^0\Pi_b^k)U|\psi\rangle_a|\xi\rangle_b \\
&= 0,
\end{aligned} \tag{3.25}$$

where we used that $\Pi_b^0 \Pi_b^k = 0$ because $\{\Pi_b^j\}_{j=0}^N$ are projectors and $k > 0$. Equation (3.18) follows because $p^{(\phi)} < 1$ and $q_k^{(\psi)} > 0$, which completes the proof. □

Notice that a general quantum operation acting on a single copy of an unknown pure quantum state $|\psi\rangle_a \in \mathcal{H}_a$ and an ancilla b in some fixed state, in which the output state includes $|\psi\rangle_a$ with some nonzero probability, can be obtained from the class of operations O considered in Theorem 3.1. This is because a general quantum operation can be implemented by including an ancilla c of sufficiently big dimension, applying a unitary operation followed by a projective measurement, and then discarding the ancilla. Since b can have an arbitrarily big dimension, the ancilla c can be included in b. Thus, after discarding c, by tracing out over its Hilbert space, a general quantum operation satisfying the properties mentioned above can be obtained from O. Also notice that the fact that the system b is not transformed into general mixed states, but into pure states, does not restrict the type of physical operations O. This follows because, given that the system b has arbitrary dimension, any system that purifies the output states can be included as part of b.

The no-cloning theorem [8,9] is easily obtained from Theorem 3.1. For convenience, we can set $N = 1$. We see that the state $|R_1\rangle$ cannot contain any copies of the input state $|\psi\rangle$ because $|R_1\rangle$ cannot have any relation to $|\psi\rangle$ at all. Thus, the probabilistic version of the no-cloning theorem is obtained. The deterministic version follows if we set $q_1 = 1$.

Theorem 3.1 implies the following lemma.

Lemma 3.1. *In a PBT protocol, as described by (3.3) – (3.5), for every input state $|\psi\rangle_a$ the following is true. The probability q_k of successful teleportation to port B_k and the residual state $|R_k\rangle_{aA\tilde{B}_k}$ when $|\psi\rangle$ is teleported to port B_k do not depend on $|\psi\rangle$. However, the global state $|F^{(\psi)}\rangle_{aAB}$ obtained after a failed PBT protocol depends on $|\psi\rangle$.*

Proof. We can identify the physical operation O in Theorem 3.1 with the PBT protocol described by (3.3) – (3.5) followed by a swap operation of systems a and B_k when outcome $k \neq 0$ is obtained. Therefore, according to Theorem 3.1, the probability q_k and the state $|R_k\rangle$ in (3.4) do not depend on $|\psi\rangle$, while the state $|F^{(\psi)}\rangle$ in (3.5) does. This is done precisely in the following way.

Let U_{aA} be the unitary operation and $\{P^j_{aA}\}_{j=0}^N$ be the projectors acting on the joint system aA corresponding to the PBT protocol given by (3.3) – (3.5). Let I_B be the identity acting on $\mathcal{H}_B$. We have that

$$(P^0_{aA} \otimes I_B)U_{aA}|\psi\rangle_a|\xi\rangle_{AB} = \sqrt{1-p^{(\psi)}}|F^{(\psi)}\rangle_{aAB}, \tag{3.26}$$

$$(P^k_{aA} \otimes I_B)U_{aA}|\psi\rangle_a|\xi\rangle_{AB} = \sqrt{q^{(\psi)}_k}|\psi\rangle_{B_k}|R^{(\psi)}_k\rangle_{aA\tilde{B}_k}, \tag{3.27}$$

for $k \in \{1, 2, \ldots, N\}$, where $p^{(\psi)} \equiv \sum_{k=1}^N q^{(\psi)}_k$. We introduce a system a' with $\dim\mathcal{H}_{a'} = \dim\mathcal{H}_a$ in a fixed pure state $|\chi\rangle_{a'}$. We identify the physical operation O in Theorem 3.1 with the PBT protocol given by (3.3) – (3.5) as follows. We define $b \equiv a'AB$, $|\xi'\rangle_b \equiv |\chi\rangle_{a'}|\xi\rangle_{AB}$ and

$$U' \equiv \left(P^0_{a'A} \otimes I_{aB} + \sum_{k=1}^N P^k_{a'A} \otimes S_{a,B_k}\right)U_{a'A}S_{a,a'}, \tag{3.28}$$

where $S_{c,d}$ is a unitary operation that swaps the states of systems c and d. Notice that we have primed the states and the unitary corresponding to the operation O in order to avoid confusion with the states and unitary of the PBT protocol, which remain unprimed. We also define the projectors acting on $\mathcal{H}_b$ corresponding to O by $\Pi^j_b \equiv P^j_{a'A} \otimes I_B$, for $j = 0, 1, \ldots, N$. Using the definitions for $|\xi'\rangle_b$ and $\{\Pi^j_b\}_{j=0}^N$, and using the expressions (3.26) – (3.28), it is straightforward to obtain that

$$(I_a \otimes \Pi^0_b)U'|\psi\rangle_a|\xi'\rangle_b = \sqrt{1-p^{(\psi)}}|\chi\rangle_a|F^{(\psi)}\rangle_b, \tag{3.29}$$

$$(I_a \otimes \Pi^k_b)U'|\psi\rangle_a|\xi'\rangle_b = \sqrt{q^{(\psi)}_k}|\psi\rangle_a|\chi\rangle_{B_k}|R^{(\psi)}_k\rangle_{a'A\tilde{B}_k}, \tag{3.30}$$

for $k = 1, 2, \ldots, N$. By identifying the output states of the physical operation O with $|F'^{(\psi)}\rangle_{ab} \equiv |\chi\rangle_a|F^{(\psi)}\rangle_b$ and $|R'^{(\psi)}_k\rangle_b \equiv |\chi\rangle_{B_k}|R^{(\psi)}_k\rangle_{a'A\tilde{B}_k}$, it follows from Theorem 3.1 that the success probabilities $q^{(\psi)}_k$ and the residual states $|R^{(\psi)}_k\rangle$ of the PBT protocol cannot depend on the input state $|\psi\rangle$. Additionally, it follows that the failure states in the PBT protocol satisfy $\langle F^{(\phi)}|F^{(\psi)}\rangle = \langle\phi|\psi\rangle$ for all $|\phi\rangle, |\psi\rangle \in \mathcal{H}_a$, and thus depend on the input state. □

The fact that the states $|R_k\rangle_{aA\tilde{B}_k}$ do not depend on $|\psi\rangle$, together with the fact that Alice knows the resource state $|\xi\rangle_{AB}$, her unitary operation U, her projective

measurement and its result k, implies that Alice knows the states $|R_k\rangle_{aA\tilde{B}_k}$. This is useful in section 3.6.

3.5 Conditions on the Port States

In this section, we deduce the form of the states in the port-based teleportation protocol. In particular, we prove (3.7) and (3.8).

We consider the state η_j of the port B_j held by Bob before the PBT protocol begins. From (3.3), we have that

$$\begin{aligned} \eta_j \quad &\equiv \mathrm{Tr}_{aA\tilde{B}_j} \left(|G\rangle\langle G|\right)_{aAB} \\ &= \mathrm{Tr}_{A\tilde{B}_j} \left(|\xi\rangle\langle\xi|\right)_{AB} . \end{aligned} \tag{3.31}$$

The no-signalling principle implies that from Bob's point of view, his state does not change with Alice's local operations if she does not send him any information. However, from Alice's point of view, after she applies her operations, Bob's state changes according to her measurement result k.

1) With probability $q_j, k = j$ and η_j changes to $|\psi\rangle\langle\psi|$, as can be seen from (3.4):

$$\mathrm{Tr}_{aA\tilde{B}_j} \left(|G_j\rangle\langle G_j|\right)_{aAB} = \left(|\psi\rangle\langle\psi|\right)_{B_j} .$$

2) With probability q_i, $k = i \notin \{0, j\}$ and η_j changes to some state that we denote as $\gamma_{j,i}$. From (3.4), we have that

$$\begin{aligned} \gamma_{j,i} \quad &\equiv \mathrm{Tr}_{aA\tilde{B}_j} \left(|G_i\rangle\langle G_i|\right)_{aAB} \\ &= \mathrm{Tr}_{aA\tilde{B}_{j,i}} \left(|R_i\rangle\langle R_i|\right)_{aA\tilde{B}_i} , \end{aligned} \tag{3.32}$$

where $\tilde{B}_{j,i} \equiv B_1 \cdots B_{j-1} B_{j+1} \cdots B_{i-1} B_{i+1} \cdots B_N$. In this case, $|\psi\rangle$ is successfully teleported to port $B_i \neq B_j$.

3) With probability $1 - p, k = 0$ and η_j changes to some state that we call $\omega_j^{(\psi)}$. From (3.5), we have that

$$\begin{aligned} \omega_j^{(\psi)} \quad &\equiv \mathrm{Tr}_{aA\tilde{B}_j} \left(|G_0\rangle\langle G_0|\right)_{aAB} \\ &= \mathrm{Tr}_{aA\tilde{B}_j} \left(|F^{(\psi)}\rangle\langle F^{(\psi)}|\right)_{aAB} . \end{aligned} \tag{3.33}$$

This is the failure result, hence $\omega_j^{(\psi)} \neq |\psi\rangle\langle\psi|$ in general.

Since the resource state $|\xi\rangle$ is fixed for any input state $|\psi\rangle$, we see from (3.31) that η_j does not depend on $|\psi\rangle$. Equations (3.32), (3.33) and Lemma 3.1 imply that q_j and $\gamma_{j,i}$ do not depend on $|\psi\rangle$, while $\omega_j^{(\psi)}$ does.

Due to the no-signalling principle, Bob cannot learn Alice's outcome before he receives any information from her. Therefore, from Bob's point of view, before receiving any information from Alice, his state is

$$\eta_j = q_j|\psi\rangle\langle\psi| + \sum_{\substack{i=1 \\ i\neq j}}^{N} q_i\gamma_{j,i} + (1-p)\omega_j^{(\psi)},$$

which is Equation (3.7).

Now we show that if there exists a protocol that achieves success probability q_j for some states η_j and $\gamma_{j,i}$ then there exists a protocol with corresponding states $\eta'_j, \gamma'_{j,i}$ and $\omega_j'^{(\psi)}$ that achieves the same success probability and satisfies $\eta'_j = \gamma'_{j,i} = \frac{I}{2^n}$, that is, Equation (3.8). The claimed protocol, which for convenience we call *primed*, is the following.

We define the set of unitary operations $\{V_l\}_{l=1}^{4^n} \equiv \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}^{\otimes n}$, where σ_0 is the identity acting on $\mathbb{C}^2$ and $\{\sigma_i\}_{i=1}^3$ are the Pauli matrices. Below, we use the identity

$$\frac{I}{2^n} \equiv \frac{1}{4^n}\sum_{l=1}^{4^n} V_l\rho V_l^\dagger, \tag{3.34}$$

which is satisfied for any quantum state ρ of dimension 2^n, and which follows from the identity (1.12) for a qubit state. Consider an ancilla a' with Hilbert space $\mathcal{H}_{a'}$ of dimension 4^n at Alice's site, which in general can be included as part of the system A, but which for clarity of the presentation is distinguished as a different system. Let $\{|\mu_l\rangle\}_{l=1}^{4^n}$ be an orthonormal basis of $\mathcal{H}_{a'}$. The ancilla a' is prepared in the state $|\phi\rangle \equiv \frac{1}{2^n}\sum_{l=1}^{4^n}|\mu_l\rangle$. Conditioned on a' being in the state $|\mu_l\rangle$, the following operations are performed. Before implementing PBT, Bob's system B_j is prepared in the state $V_l\eta_j V_l^\dagger$. Then, if Alice applies the PBT protocol described by (3.3) – (3.5), which satisfies (3.7), on her system aA then with probability q_j the state of the system B_j transforms into $V_l|\psi\rangle$ and with probability q_i transforms into $V_l\gamma_{j,i}V_l^\dagger$, where $i \notin \{j, 0\}$; this is clear from (3.7) and follows from the fact

that the operations on B_j commute with those on aA (no-signalling) and from the linearity of quantum theory (see details in Appendix C). Thus, consider that before doing this, Alice applies $V_l^\dagger$ on her input state $|\psi\rangle_a$. In this case, the state $|\psi\rangle$ is teleported without error. Since the states of the system B_j before implementing PBT and after an outcome $k = i \notin \{j, 0\}$ is obtained do not depend on the teleported state, these states remain the same. Hence, in the primed PBT protocol, we obtain that, after discarding the ancilla a', by taking the partial trace over $\mathcal{H}_{a'}$, the initial state of the system B_j is $\eta'_j = \frac{1}{4^n}\sum_{l=1}^{4^n} V_l \eta_j V_l^\dagger$ and its final state after an outcome $k = i \notin \{j, 0\}$ is obtained is $\gamma'_{j,i} = \frac{1}{4^n}\sum_{l=1}^{4^n} V_l \gamma_{j,i} V_l^\dagger$, both of which equal $\frac{I}{2^n}$, as follows from the identity (3.34). Therefore, we see from (3.7) that this protocol satisfies

$$\frac{I}{2^n} = q_j|\psi\rangle\langle\psi| + \sum_{\substack{i=1 \\ i\neq j}}^{N} q_i \frac{I}{2^n} + (1-p)\omega_j'^{(\psi)}, \tag{3.35}$$

where

$$\omega_j'^{(\psi)} \equiv \frac{1}{4^n}\sum_{l=1}^{4^n} V_l \omega_j^{(\psi_l)} V_l^\dagger, \tag{3.36}$$

and ψ_l refers to dependence on the state $V_l^\dagger|\psi\rangle$.

We have shown that the previous PBT protocol succeeds with probability q_j and satisfies (3.8). Thus, we assume (3.8) in the following section. Without loss of generality, we consider that the system a' is included in A, hence, we do not need to mention it again.

3.6 Implications from Superdense Coding

Now we present a protocol in which Alice tries to send Bob a random message of $2n$ bits that succeeds with the probability p'_j given by Equation (3.9). Note that, so far, we have considered the input system a to be in a pure state. However, the previous arguments work if a is in a mixed state too. Thus, consider that a is in a bipartite maximally entangled state $|\phi\rangle_{ab}$ with system b, held by Bob, and that Alice and Bob perform superdense coding [12] using this state. Alice wants to communicate Bob a $2n$-bits random message $x \in \{1, 2, \ldots, 4^n\}$. Alice

applies a local unitary operation U_x on a, after which, the system ab transforms into the state $U_x \otimes I|\phi\rangle_{ab}$. For clarity of the presentation, let us consider that $|\psi\rangle_{ab} = U_x \otimes I|\phi\rangle_{ab}$. The set of unitary operations $\{U_y\}_{y=1}^{4^n}$ is such that it generates an orthonormal basis, $\mathcal{B} = \{U_y \otimes I|\phi\rangle\}_{y=1}^{4^n}$. Instead of sending the system a directly to Bob, Alice teleports its state to the system B_j, at Bob's location, using the modified PBT protocol described below in which no communication is allowed (see Figure 3.2). Bob completes the superdense coding protocol by measuring the system $B_j b$ in the basis $\mathcal{B}$. Let y be Bob's measurement outcome. Bob obtains Alice's message correctly, that is $y = x$, if his outcome corresponds to the state $|\psi\rangle$.

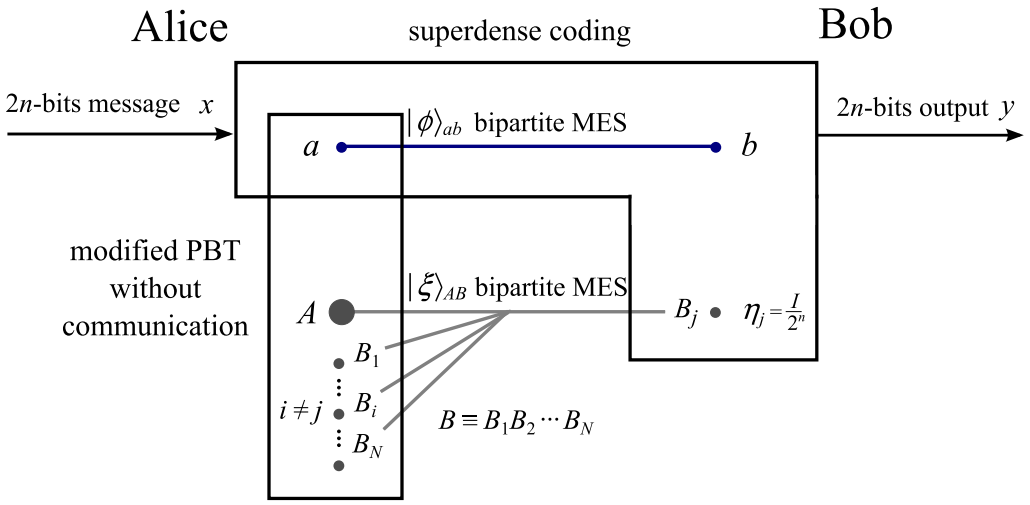


Figure 3.2: A superdense coding protocol without communication. Alice is given a random message x of $2n$ bits that she encodes in the $n-$qubits system a by performing the unitary operation of the superdense coding protocol. Alice's system a is in a bipartite maximally entangled state (MES) $|\phi\rangle_{ab}$ with Bob's system b. Then, Alice teleports the state of system a to Bob's port B_j, using a modified port-based teleportation protocol in which there is no communication. In this modified PBT protocol, Bob has the system $B_j b$ and Alice has the system $aA\tilde{B}_j$, where $\tilde{B}_j = B_1 B_2 \cdots B_{j-1} B_{j+1} B_{j+2} \cdots B_N$. Similar to the original PBT protocol, the resource state is $|\xi\rangle_{AB}$. The state of port B_j is completely mixed, which means that B_j is in a bipartite MES with Alice's system. Finally, Bob applies the projective measurement of the superdense coding protocol on his system bB_j. Bob's $2n-$bits measurement outcome y is his guess for Alice's input message x.

Bob has the system $B_j b$ and Alice has the system $aA\tilde{B}_j$. Similar to the original PBT protocol, the initial global state is given by $|\psi\rangle_{ab}|\xi\rangle_{AB}$, and Alice applies the same local operations on the systems a and A, only. Therefore, if Alice's measurement result is $k \neq 0$, the final state is $|\psi\rangle_{B_k b}|R_k\rangle_{aA\tilde{B}_k}$ and the residual state $|R_k\rangle_{aA\tilde{B}_k}$ is known by her. However, *Alice is not allowed to communicate with Bob*. From (3.8), we assume that Bob's system B_j is initially in the completely mixed state, meaning that it is maximally entangled with its purifying system, at Alice's site. Consider the possible situations according to Alice's outcome k.

1) Alice obtains $k = j$, so the system $B_j b$ is transformed into the state $|\psi\rangle_{B_j b}$; this occurs with probability q_j. Bob measures the system $B_j b$ in the basis $\mathcal{B}$ and obtains Alice's message correctly.

2) Alice obtains $k = i \notin \{0, j\}$. Thus, the state of the system a is teleported to the system B_i, at Alice's site. This occurs with probability q_i. We denote the composite system $aA\tilde{B}_{j,i}$ as $A_{j,i}$. Alice has the systems $A_{j,i}$ and B_i, while Bob has the system $B_j b$. The global system is in the state $|\psi\rangle_{B_i b}|R_i\rangle_{A_{j,i}B_j}$. Equation (3.8) tells us that the system B_j is completely mixed, meaning that it is maximally entangled with its purifying system $A_{j,i}$. It follows that

$$|R_i\rangle_{A_{j,i}B_j} = \frac{1}{\sqrt{2^n}} \sum_{l=1}^{2^n} |l_i\rangle_{A_{j,i}} |l_i\rangle_{B_j},$$

where $\{|l_i\rangle\}_{l=1}^{2^n}$ is the Schmidt basis of the state $|R_i\rangle_{A_{j,i}B_j}$. As mentioned in section 3.4, Alice knows the obtained state $|R_i\rangle_{A_{j,i}B_j}$, which means that she knows its Schmidt basis. Therefore, Alice can apply the local operations of the standard teleportation protocol [13] on the systems B_i and $A_{j,i}$ in order to teleport the state of the system B_i to the system B_j. Then, Bob completes the superdense coding protocol by measuring his system $B_j b$ in the basis $\mathcal{B}$. Since communication is not allowed, the no-signalling principle implies that Bob obtains Alice's message correctly with probability $\frac{1}{4^n}$. Thus, if $k \notin \{0, j\}$, the success probability is

$$\frac{1}{4^n} \sum_{\substack{i=1 \\ i \neq j}}^{N} q_i = \frac{1}{4^n}(p - q_j).$$

3) Alice obtains $k = 0$, hence the protocol fails; this occurs with probability $1-p$. In this case, we should allow for the possibility that the final state of the system $B_j b$ has nonzero overlap with the input state $|\psi\rangle$. Hence, after measuring in the basis $\mathcal{B}$, the system $B_j b$ transforms into the state $|\psi\rangle_{B_j b}$ with some probability r_j. Thus, if $k = 0$, Bob obtains Alice's message with probability r_j.

It follows that the total success probability p'_j of the previous protocol is given by (3.9):

$$p'_j = q_j + \frac{1}{4^n}(p - q_j) + (1 - p)r_j.$$

Thus, Equation (3.10) and our main result Equation (3.1), follow.

3.7 Discussion

Port-based teleportation (PBT) was introduced by Ishizaka and Hiroshima in [100, 101]. The case $n = 1$ in which a single qubit state is input to port-based teleportation was discussed in [101]. By direct optimization, the maximum success probability $p_{\max}$ in the probabilistic version and the maximum average fidelity $f_{\max}$ in the deterministic version were obtained: $p_{\max} = \frac{N}{N+3}$ (Equation (3.2)) and $f_{\max} = \frac{2}{3} + \frac{1}{3}\cos\frac{2\pi}{N+2}$. Given the simplicity of these expressions, it was hypothesized that they can be derived from fundamental laws of physics. In this chapter, we have confirmed such a hypothesis for the probabilistic version of PBT.

We have shown an upper bound on the success probability p of probabilistic PBT of an unknown n-qubits state as a function of n and the number of ports N, Equation (3.1). This bound implies a lower bound on the number of ports that are needed to achieve a given success probability p:

$$N \geq \frac{4^n - 1}{p^{-1} - 1}. \tag{3.37}$$

Our proof of (3.1) is based on the no-signalling principle and a version of the no-cloning theorem, Theorem 3.1, which we have presented and proven in section 3.4. Our bound on p agrees with the maximum success probability for the case $n = 1$, Equation (3.2). A probabilistic PBT protocol for the case $n > 1$ has not been developed explicitly; it would be interesting to know whether our

bound can be achieved in this case too. It would also be interesting to investigate whether our techniques are useful to show an upper bound on the maximum average fidelity achieved in the deterministic version of PBT.

An interesting question is, how much entanglement do Alice and Bob need to share to perform PBT with a given success probability p in the probabilistic version, or a given fidelity f in the deterministic version? An explicit deterministic PBT protocol for a general $n-$qubits state was given by Ishizaka and Hiroshima [100]. The resource state $|\xi\rangle_{AB}$ of this protocol was not optimized to achieve the maximum average fidelity. It consists of Nn singlets, each port consisting of n qubits in singlet states. The optimal PBT protocol was given only for the case $n = 1$ [101], where it was shown that the resource state $|\xi\rangle_{AB}$ optimizing this protocol is not a maximally entangled state.

As mentioned in section 3.1, an important application of PBT is that it allows the implementation of instantaneous nonlocal quantum computation (INLQC) with an amount of entanglement that is only exponential in the number of qubits n of the input state [85], compared to the double exponential amount of schemes based on standard teleportation [82, 84]. An INLQC consists in the application of a nonlocal unitary operation on a state $|\psi\rangle$ distributed among distant parties, with a single round of communication by the parties. INLQC has application to position-based quantum cryptography (PBQC) [91, 92] and some quantum tagging schemes [86–90] because it allows an eavesdropper to break their security, as described below.

In PBQC [91], a set of M distant parties called *verifiers* initially share a quantum state $|\psi\rangle_{v_1 v_2 \cdots v_M}$. The verifiers collaborate with the goal of authenticating that communication is performed with another party, the *prover*, who is at a particular position P in space. The verifiers send their respective systems v_j to the prover. The prover computes a nonlocal unitary U on the received systems and then sends the transformed systems back to the verifiers. The communication between the verifiers and the prover is performed at the speed of light. The verifiers should share the state $U|\psi\rangle$ at the end of this protocol. Each verifier requires that he receives his system back from the prover in the time that light takes to travel from his location to P and back to his location. The verifiers collaborate to verify that they share the state $U|\psi\rangle$ and that the communication

times are as expected.

A set of M collaborating eavesdroppers can break the security of PBQC in the following way [91]. Each eavesdropper is located between P and a verifier. The eavesdroppers intersect the systems v_j and then collaborate to implement an INLQC, after which they share the state $U|\psi\rangle$. Then the eavesdroppers send the corresponding systems back to the verifiers. If necessary, they wait some time before sending the systems so that the verifiers receive them at the correct times. Since the INLQC takes only a single round of communication among the eavesdroppers, the verifiers receive the systems at the right times and they share the correct state $U|\psi\rangle$. However, the prover does not communicate with the verifiers at all. Thus, this scheme breaks the security of PBQC.

We consider it useful to describe explicitly how an INLQC is implemented using port-based teleportation [85]. Alice and Bob share a quantum state $|\psi\rangle_{a_1 b}$ on which they want to implement an arbitrary nonlocal unitary operation U. Alice has the system a_1 of n_1 qubits and Bob has the system b of n_2 qubits, with $n = n_1 + n_2$. We notice that in general, a bipartite INLQC on a state $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ requires that the dimension of $\mathcal{H}_1 \otimes \mathcal{H}_2$ is $d \geq 4$, that is, the Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ correspond to at least one qubit each. Alice and Bob also share singlet states and the PBT resource state $|\xi\rangle_{AB}$, with $B = B_1 B_2 \cdots B_N$ denoting the N ports of n qubits each at Bob's site.

First, Bob applies Bell measurements on his system b and his part of n_2 singlets shared with Alice and obtains the outcome $\vec{x} = (x_1, x_2, \ldots, x_{n_2})$, with $x_j \in \{0,1\}^2$. He does not communicate his outcome to Alice. Thus, his state is teleported to a system a_2 at Alice's location, up to some Pauli errors $\sigma_{\vec{x}} = \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_{n_2}}$.

Second, Alice applies the measurement of PBT on his sytem aA and obtains the outcome k, where a denotes the $n-$qubits joint system $a_1 a_2$. If $k = i \neq 0$, the port B_i is transformed into the state $\sigma_{\vec{x}}|\psi\rangle$. Notice that, before receiving Alice's message, Bob does not know whether PBT has been successful and if so to which port the state has been teleported.

Third, Bob applies the string of Pauli operations $\sigma_{\vec{x}}$ followed by the $n-$qubits unitary operation U on each of his N ports. If Alice's measurement outcome is $k = i \neq 0$, the final state of port B_i is $U|\psi\rangle$.

Finally, Bob applies the standard teleportation protocol [13] to the corresponding n_1-qubits system for each of his N ports, which includes communication of his outcomes to Alice. Alice communicates her outcome k to Bob. Thus, if $k = i \neq 0$, Bob selects the port B_i and the state $U|\psi\rangle$ is shared by Alice and Bob, as desired. Notice that the communication from Alice to Bob and from Bob to Alice is made at the same time and thus this protocol requires a single round of communication, which, by definition, is a requirement for INLQC.

We hope the reader finds the previous discussion useful in clarifying what we see as the key benefit of PBT, that the only operation that Bob needs to apply in order to obtain the teleported state is to select a single of a set of N ports, whose identity is indicated by Alice in a single message. This important advantage of PBT requires a considerably big number of ports, as given by (3.37), in order to teleport an $n-$qubits state with a success probability p, in the probabilistic version, as follows from the bound (3.1) proven in this chapter. This follows from the no-signalling principle and the no-cloning theorem, as we have shown.

Chapter 4

Quantum Information Causality

4.1 Introduction

Quantum physics satisfies the no-signalling principle. The no-signalling principle states that a party, Alice, cannot communicate any information to a distant party, Bob, if she does not send him any physical systems, independently of any physical resources that they share [69], as we discussed in section 1.3.2. It implies that Bob must necessarily receive a physical system from Alice, or possibly from another party sharing correlations with her, in order to obtain information about data at Alice's location. Thus, an interesting question to ask is, *how much information can a transmitted physical system fundamentally communicate?*

Different scenarios for answering the previous question can be considered according to the properties of the transmitted system, the type of communicated information, the way in which information is quantified, the number of involved parties, the resources allowed among the parties, etc. The Holevo theorem states an upper bound on the amount of classical information that a transmitted quantum system can communicate, if shared quantum entanglement is not used by the communicating parties [7]. The principle of information causality can be stated in the context of hypothetical probabilistic theories more general than quantum mechanics. It states an upper bound on the amount of information that a transmitted classical system can communicate as a function of its dimension, independently of any non-signalling physical resources allowed by the considered theory

that the communicating parties previously shared [71]. In the case of quantum theory, to which we restrict in this thesis, unless otherwise stated, information causality applies to the scenario in which the communicating parties share arbitrary quantum resources. In this chapter, the principle of quantum information causality, published by us in [104], is presented. Quantum information causality is the quantum version of information causality. It states an upper bound on the amount of quantum information that a transmitted quantum system can communicate as a function of its dimension, independently of any quantum physical resources previously shared by the communicating parties.

4.1.1 The Holevo Bound

The Holevo theorem considers the following scenario involving two parties, Alice and Bob. Alice has a classical random variable X that takes the value $x \in \{0, 1, \ldots, d-1\}$ with probability P_x. Alice encodes X in a quantum system T as follows: if $X = x$, Alice prepares T in the quantum state ρ_x. Then, Alice sends Bob the system T. Bob applies a positive operator valued measure on T and obtains the outcome y, whose probability distribution defines the random variable Y. Bob tries to guess Alice's value x from his outcome y. A good measure of how much information Bob has obtained about X from his measurement is given by the classical mutual information between X and Y, $H(X:Y) \equiv H(X) + H(Y) - H(XY)$, where $H(X) \equiv -\sum_{x=0}^{d-1} P_x \log_2 P_x$ is the classical entropy of X, etc. The *Holevo bound* is the following:

$$H(X:Y) \leq S(\rho) - \sum_{x=0}^{d-1} P_x S(\rho_x), \tag{4.1}$$

where $\rho = \sum_{x=0}^{d-1} P_x \rho_x$. In this scenario, Alice and Bob do not use shared quantum entanglement. In particular, the transmitted system T is not entangled with Bob's system [5, 7].

The Holevo bound implies that Bob cannot obtain more than m bits of information about Alice's data, if Alice sends Bob a quantum system of m qubits.

More precisely, if the transmitted system T is an m-qubits system then

$$H(X:Y) \leq m. \tag{4.2}$$

The proof is as follows. From (4.1), we have that, in general, $H(X:Y) \leq S(\rho)$. Since the dimension of T is 2^m, the quantum entropy of any state of T cannot be bigger than m. Thus, $S(\rho) \leq m$ and Equation (4.2) follows. It is required that T is not entangled with Bob's system for this result to hold. If T were allowed to be entangled with Bob's system, by performing the superdense coding protocol, Bob could learn $2m$ of Alice's bits perfectly, in which case a value of $H(X:Y) = 2m$ could be achieved.

4.1.2 Information Causality

Information causality was introduced in the context of the following information task [71], which for convenience is denoted here as the *information causality* (*IC*) *game* (see Figure 4.1).

The IC game. Consider two parties at different locations, Alice and Bob. Alice is given a string of n random bits $\vec{x} \equiv (x_0, x_1, \ldots, x_{n-1})$ in a physical system A. Bob is given a random number $k \in \{0, 1, \ldots, n-1\}$. After Alice and Bob play the game, Bob outputs a bit y_k. If $y_k = x_k$, Alice and Bob win the game. Alice and Bob may play any strategy allowed by the theory, as long as their communication is limited to a single message $\vec{r}$, encoded in a system T of m bits, that Alice sends Bob, with $m < n$. In particular, Alice and Bob may use arbitrary non-signalling physical resources allowed by the theory, which they share in the bipartite system $A'B$, where A' is held by Alice and B is held by Bob. The probability to win the IC game is:

$$P_{\text{IC}} \equiv \frac{1}{n} \sum_{k=0}^{n-1} P(y_k = x_k). \tag{4.3}$$

We can consider the more general situation in which Alice's inputs are dits, which are variables of $d > 2$ possible values, instead of bits. In this case Alice's message is an m-dits number, with $m < n$, and Bob's output is a dit. For convenience, we only discuss the bit case, unless otherwise stated.

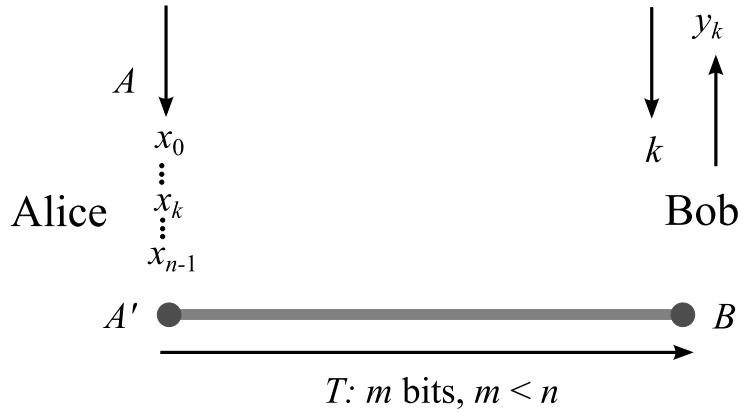


Figure 4.1: The information causality game. Alice and Bob share an arbitrary non-signalling resource in the physical systems A' and B. Alice is given a system A containing a string of n random bits, $x_0, x_1, \ldots, x_{n-1}$. Bob is given a random number $k \in \{0, 1, \ldots, n-1\}$. After Alice and Bob play the game, Bob outputs a bit y_k. Alice and Bob win the game if $y_k = x_k$. They may play any strategy allowed by the theory, as long as their communication is limited to a single message from Alice to Bob only encoded in a system T of m bits, with $m < n$.

The IC game is an extension of quantum random access coding. The idea of quantum random access coding was first considered by Wiesner with the name of conjugate coding [6]. Formally introduced in [105], an (n, m, p) quantum random access code (QRAC) is a map, applied by Alice, that encodes n bits into a quantum state of m qubits that Alice sends Bob, with $m < n$, and a set of n possible measurements that Bob applies on the received state. If Bob applies the kth measurement, he decodes Alice's kth bit with a probability not smaller than p. It is a requirement that $p > \frac{1}{2}$, because $p = \frac{1}{2}$ can be achieved by a random guess. In a (classical) random access code (RAC), Alice sends Bob m bits instead of m qubits, Bob applies an operation that depends on the message received from Alice and on the bit that he wants to learn from Alice's inputs. In general, QRACs achieve higher success probabilities than RACs. RACs and QRACs do not use entanglement shared by Alice and Bob; the use of shared randomness is discussed in [106]. RACs in which Alice and Bob use shared entanglement are denoted as entanglement-assisted random access codes (EARACs) [107]. Generally, EARACs achieve higher success probabilities than QRACs. A general strategy

to play the IC game is an EARAC.

Some interesting questions that can be asked regarding the information causality game are, how much information can Bob obtain about $\vec{x}$ from the message $\vec{\tau}$ and his local resources in the system B? Is there any strategy that allows Alice and Bob to achieve $P_{\text{IC}} = 1$, given that $m < n$? What is the maximum value of P_{IC} that can be achieved?

The no-signalling principle provides simple answers to the previous questions in the case $m = 0$, in which Alice does not send Bob any bits. It says that, in this case, Bob cannot learn anything about Alice's bit-string $\vec{x}$. Thus, for any strategy with $m = 0$, Bob outputs the correct number with the probability of making a random guess: $P_{\text{IC}} = \frac{1}{2}$.[1] Therefore, $P_{\text{IC}} = \frac{1}{2}$, if $m = 0$.

The principle of *information causality* states an upper bound on the amount of information that a message of m bits can communicate:

$$I(A : TB) \leq m, \tag{4.4}$$

where $I(A : TB)$ is the mutual information between the system A containing Alice's data $\vec{x}$ and the joint system TB at Bob's location, which includes the received system T encoding the m-bits message $\vec{\tau}$ and Bob's local resources B [71].

Information causality holds in more general probabilistic theories in which the definition of mutual information $I(X : Y)$ between two systems X and Y satisfies a few properties. In the paper that introduced information causality [71], it was shown that together with symmetry and non-negativity, sufficient conditions on the mutual information for satisfaction of information causality are:

Consistency If both systems X and Y are classical, $I(X : Y)$ reduces to the classical mutual information.

Data-processing inequality Acting locally on one of the systems cannot increase the mutual information (see Equation (1.30) for the quantum case). That is, if a physical transformation allowed by the theory acts on the system Y only, transforming it to Y', then $I(X : Y') \leq I(X : Y)$.

[1] This is shown in Equation (1.63) in section 1.3.2.

Chain rule There exists a conditional mutual information $I(X:Y|Z)$ that satisfies the following: $I(X:YZ) \equiv I(X:Z) + I(X:Y|Z)$. This condition, together with the symmetry property of the mutual information, implies the identity $I(X:YZ) - I(X:Z) = I(X:Y|Z) = I(Y:XZ) - I(Y:Z)$.

It can also be shown that information causality follows from a few physical conditions on the measure of entropy H [108]:

Consistency If X is a classical system then $H(X)$ is the classical entropy.

Evolution with an ancilla Consider a system composed of two subsystems X and Y. If a transformation is performed only on a single subsystem, $Y \to Y'$, then the increase of entropy of the composite system, $\Delta H(XY) \equiv H(XY') - H(XY)$, cannot be smaller than the increase of entropy of the transformed subsystem, $\Delta H(Y) \equiv H(Y') - H(Y)$. That is, $\Delta H(XY) \geq \Delta H(Y)$.

The previous sets of conditions are satisfied by quantum theory if the mutual information and the entropy are defined as the quantum mutual information and the quantum entropy, respectively. Therefore, information causality is satisfied by quantum theory. Similarly, information causality is satisfied by classical probabilistic theory. This follows straightforwardly from the fact that the quantum entropy of a classical system reduces to the classical entropy, which is the consistency condition.

Although originally defined in [71] as satisfaction of (4.4), information causality is usually stated as satisfaction of the following bound:

$$\sum_{k=0}^{n-1} H(x_k : y_k) \leq m, \tag{4.5}$$

where $H(x_k : y_k)$ is the classical mutual information between Bob's output y_k and Alice's bit x_k, when Bob receives the number k [109]. An advantage of (4.5) over (4.4) is that the quantity $\sum_{k=0}^{n-1} H(x_k : y_k)$ is completely defined in classical terms, while the quantity $I(A:TB)$ requires a definition for the mutual information in the particular theory that is being considered. On the other hand, if the theory is

restricted to be quantum, we consider the bound (4.4) to be more advantageous than the bound (4.5), because the former applies to a more general scenario than the information causality game. Moreover, (4.4) implies (4.5), because it was shown in [71] that

$$\sum_{k=0}^{n-1} H(x_k : y_k) \leq I(A : TB), \tag{4.6}$$

while the inverse does not necessarily hold. We consider more convenient to define information causality as satisfaction of the bound (4.4), hence, we adopt such a convention here. In fact, we present a more general bound in section 4.2.2, from which (4.4) is obtained.

The bound (4.5) is saturated by the following strategy in the IC game, which here is denoted as *naive*. As previously agreed by Alice and Bob, Alice sends Bob the message $\vec{\tau} = (x_0, x_1, \ldots, x_{m-1})$. Bob receives the number k. If $k < m$, Bob outputs the correct bit $y_k = x_k$, otherwise he outputs a random bit. It is straightforward to obtain that this strategy succeeds with a probability $P_{\text{IC}} = \frac{1}{2}(1 + \frac{m}{n})$.

The naive strategy does not achieve the maximum success probability, because a different strategy achieves a higher success probability $P_{\text{IC}} = \frac{1}{2}(1 + \frac{1}{\sqrt{n}})$ in the case $m = 1$ [108]. Therefore, the quantity $\sum_{k=0}^{n-1} H(x_k : y_k)$ does not necessarily quantify how well Alice and Bob have played the IC game. But, it has the advantage of having a simple and achievable upper bound that applies in the general case $m < n$. On the other hand, the maximum value of P_{IC} is only known if $m = 1$ [107, 108]. However, an upper bound on P_{IC} that applies in the general case $m < n$ can be derived from information causality.

It is shown in [71] that satisfaction of (4.5) implies

$$\sum_{k=0}^{n-1} h(P_k) \geq n - m, \tag{4.7}$$

where $P_k \equiv P(y_k = x_k)$ and $h(x) \equiv -x \log_2 x - (1 - x) \log_2(1 - x)$ is the binary entropy. The concavity property of the classical entropy implies that $h(P_{\text{IC}}) \geq$

$\frac{1}{n}\sum_{k=0}^{n-1} h(P_k)$, which from (4.7) implies the bound:

$$P_{\mathrm{IC}} \leq P'_{\mathrm{IC}}, \tag{4.8}$$

where P'_{IC} is defined as the maximum solution of the equation $h(P'_{\mathrm{IC}}) = 1 - \frac{m}{n}$. The lower bound $1-P'_{\mathrm{IC}} \leq P_{\mathrm{IC}}$ follows from the bound (4.8): if a strategy achieved a success probability $P_{\mathrm{IC}} = p$ such that $p < 1 - P'_{\mathrm{IC}}$ then a strategy that flips the outcomes would achieve a success probability $1 - p$ that violates the inequality (4.8).

Information causality has important implications for the set of quantum correlations [71,110–113]. It implies [71] the Cirel'son bound, while the no-signalling principle does not [70]. The Cirel'son bound [44] states the maximum violation of the CHSH inequality [42] that can be achieved by quantum theory. It can be equivalently stated as the maximum success probability achieved by quantum theory in the CHSH game. The CHSH game involves two parties at different locations, Alice and Bob. Alice has a physical system A on which she applies one of two measurements, chosen randomly and labelled by $a \in \{0, 1\}$. Similarly, Bob has a physical system B on which he applies a random measurement $b \in \{0, 1\}$. Alice and Bob obtain the outcomes r and s, respectively, where $r, s \in \{0, 1\}$. The game's goal is that Alice and Bob output numbers r and s that satisfy $r \oplus s = ab$, where $\oplus$ denotes sum modulo 2. The success probability is defined as $P_{\mathrm{CHSH}} \equiv P(r \oplus s = ab)$. The Cirel'son bound is:

$$P_{\mathrm{CHSH}} \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right). \tag{4.9}$$

The no-signalling principle does not imply satisfaction of Cirel'son's bound, because there exist theoretical correlation boxes, the PR boxes, for which $P_{\mathrm{CHSH}} = 1$, that still satisfy the no-signalling principle [70] (see section 1.3.2.1 for details). However, information causality does imply Cirel'son's bound. The proof considers a particular protocol to play the IC game in the case $m = 1$ that uses hypothetical non-signalling correlation boxes, not restricted to be described by quantum theory. If boxes violating (4.9) were available in the protocol then the bound (4.5) would be violated for a sufficiently big value of n, which would imply

violation of information causality, Equation (4.4) [71].

It was hypothesized that the complete set of correlations allowed by quantum theory could be derived from information causality [71]. However, it was shown that information causality, being a bipartite information principle, could not imply the complete set of quantum correlations for an arbitrary number of parties [112, 113].

4.2 Quantum Information Causality

The principle of *quantum information causality* states that the maximum amount of quantum information that a quantum system can communicate is limited by its dimension, independently of any quantum physical resources previously shared by the communicating parties. It considers the following scenario, which is illustrated in Figure 4.2. Alice, Bob and Charlie have quantum systems A, B and C, respectively, of any dimension. The total system ABC is in an arbitrary quantum state. Alice applies local operations on her system in order to obtain a quantum system T of m qubits that she sends Bob. Apart from its dimension, there are no other constraints on the transmitted system. In particular, the transmitted system can be entangled in any way with Alice's, Bob's and Charlie's systems. Bob receives T and applies local operations on the system BT, which is denoted as B' after Bob's operations.

The principle of *quantum information causality* states an upper bound on the amount of quantum information that m qubits can communicate:

$$\Delta I(C : B) \leq 2m, \tag{4.10}$$

where $\Delta I(C : B) \equiv I(C : B') - I(C : B)$ is Bob's gain of quantum information about C, $I(C : B) \equiv S(C) + S(B) - S(CB)$ is the quantum mutual information between C and B, $S(C)$ is the quantum entropy [4, 5] of C, etc. Since the quantum mutual information quantifies the total correlations between two quantum systems [30–32], we consider $\Delta I(C : B)$ to be a good measure for the communicated quantum information.[1]

[1]Note that there are measures [30–32] for the purely classical and purely quantum parts

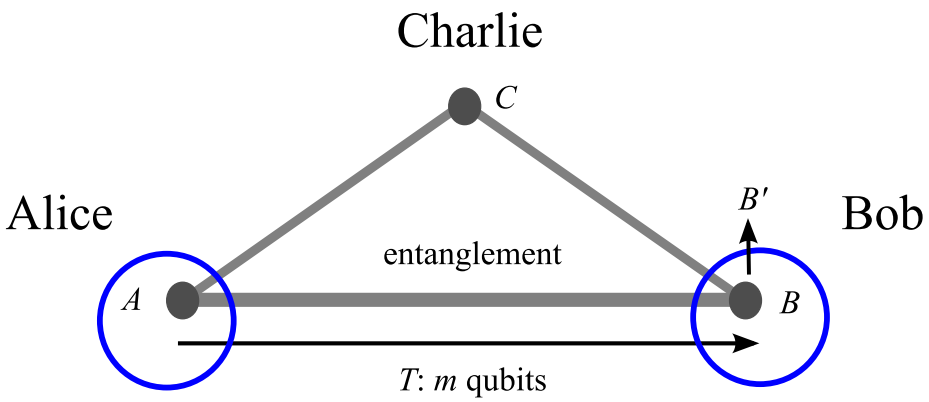


Figure 4.2: Setting for quantum information causality. Alice, Bob and Charlie have respective quantum systems A, B and C in an arbitrary quantum state, which can be entangled in any possible way. After applying local operations on her system, Alice obtains a quantum system T of m qubits that she sends Bob. Bob receives T and applies local operations on the system BT, which is denoted as B' after Bob's operations.

The proof of quantum information causality is very simple. It follows from three properties of the quantum entropy: subadditivity [28], the triangle inequality (also called the Araki-Lieb inequality) [29] and the data-processing inequality [5]. By definition of the quantum mutual information,

$$I(C : BT) = S(C) + S(BT) - S(CBT). \tag{4.11}$$

From the subadditivity property, we have that

$$S(BT) \leq S(B) + S(T). \tag{4.12}$$

The triangle inequality, $|S(CB) - S(T)| \leq S(CBT)$, implies that

$$-S(CBT) \leq S(T) - S(CB). \tag{4.13}$$

of the correlations between two quantum systems, whose sum is equal to the quantum mutual information (see [114] for a review). We do not consider such a classification in our discussion.

Equations (4.11) – (4.13) imply

$$I(C : BT) \leq 2S(T) + I(C : B). \tag{4.14}$$

The data-processing inequality states that local operations cannot increase the quantum mutual information [5]. Thus, $I(C : B') \leq I(C : BT)$, which from (4.14) implies that $I(C : B') \leq 2S(T) + I(C : B)$. It follows that

$$\Delta I(C : B) \leq 2S(T). \tag{4.15}$$

Finally, since $S(T) \leq \log_2 (\dim T)$, the quantum information that T can communicate is limited by its dimension. Therefore, if T is a system of m qubits, Equation (4.10) follows from Equation (4.15), because $S(T) \leq m$ in this case.

The previous proof does not require to mention Alice's system. This means that Equation (4.10) is valid independently of how much quantum entanglement Alice and Bob share. This also means that Equation (4.10) is valid too if we consider that Alice and Charlie are actually the same party. Thus, quantum information causality shows: *the maximum possible increase of the quantum mutual information between Charlie's and Bob's systems is only a function of the dimension of the system T received by Bob, independently of whether it is Alice or Charlie who sends Bob the system T and of how much quantum entanglement Bob shares with them.*

4.2.1 Achievability of the Bound

Achievability of equality in (4.10) requires that the transmitted system T is maximally entangled with Charlie's system C, as shown below.

Following the proof of the bound (4.10), we note that equality requires the following conditions to be satisfied. First, the transmitted system T has to be in a product state with Bob's system B in order to satisfy $S(BT) = S(B) + S(T)$. Second, the system T can only be entangled with the joint system CB, so that we have $-S(CBT) = S(T) - S(CB)$, as shown below. Third, the state of the system T has to be completely mixed so that its entropy is maximum: $S(T) = m$; this means that T has to be maximally entangled with its purifying system. Together,

the previous conditions imply that T has to be maximally entangled with C. It is also required that the quantum mutual information between BT and C does not decrease by Bob's operations, that is, $I(C : B') = I(C : BT)$.

Now we show the second condition: satisfaction of $-S(CBT) = S(T) - S(CB)$ is achieved if and only if T is entangled only with the joint system CB [5]. Recall that the original system at Alice's site is denoted as A, from which Alice obtains the transmitted system T after performing local operations. It is convenient to consider that Alice initially has both systems A and T and then applies some local operation on the joint system AT. The systems A, B and C are arbitrarily big. Thus, without loss of generality, we can consider that the global system $ACBT$ is in a pure state. Alice's quantum operation on the system AT can in general be represented by a unitary operation followed by a projective measurement. Thus, after Alice's operation, the global system $ACBT$ remains in a pure state. Due to the Schmidt decomposition of a bipartite pure state, it follows that

$$\begin{aligned} S(CB) &= S(AT), \\ S(A) &= S(CBT). \end{aligned} \tag{4.16}$$

From subadditivity, it is obtained that

$$S(AT) \leq S(A) + S(T), \tag{4.17}$$

which from (4.16) implies that

$$S(CB) \leq S(CBT) + S(T). \tag{4.18}$$

Equality in (4.18) is achieved if and only if equality in (4.17) is satisfied, which occurs if and only if T is in a product state with A. Therefore, the relation $-S(CBT) = S(T) - S(CB)$ is satisfied if and only if T is entangled only with the system CB, as claimed.

4.2.2 The Case of Information Causality

If the transmitted system T is classical, equality in (4.10) cannot be achieved. In this case, the following bound is satisfied:

$$\Delta I(C:B) \leq m, \tag{4.19}$$

where C and B are quantum systems and $I(C:B)$ denotes their quantum mutual information. From now on, this bound is denoted as *information causality*. It considers a situation more general than the information causality principle originally introduced in [71], Equation (4.4). It reduces to Equation (4.4) if the following conditions are satisfied. First, Charlie and Bob do not share correlations initially, hence, $I(C:B) = 0$. Second, Charlie and Alice are actually the same party, who are identified as Alice. Third, Alice's systems are re-labelled as follows: $A \to A'$ and $C \to A$. Fourth, the (re-labelled) system A is restricted to be classical and correspond to a string $\vec{x}$ of n bits. Finally, the system B' denotes the system BT before Bob applies any operations.

The proof of the information causality bound, Equation (4.19), is similar to the proof of the quantum information causality bound, Equation (4.10). The only difference is that if T is classical then the bound $-S(CBT) \leq S(T) - S(CB)$ cannot be achieved. In fact, in this case the smaller upper bound $-S(CBT) \leq -S(CB)$ is satisfied. A way to see this is that, if T is a classical variable, the state of the joint system CBT is a distribution over all possible values $\vec{\tau}$ of T and states of CB for each $\vec{\tau}$. Therefore, there exists a transformation $\vec{\tau} \to (CB)_{\vec{\tau}}$. Thus, the data-processing inequality implies that $I(CB:T) \leq I(T:T)$. Hence, since $I(CB:T) = S(CB) + S(T) - S(CBT)$ and $I(T:T) = S(T)$, it follows that $-S(CBT) \leq -S(CB)$ [71, 108].

4.3 The Quantum Information Causality Game

Quantum information causality implies an upper bound on the success probability of a new quantum information task, the *quantum information causality* (*QIC*) *game*. We present two version of this game.

The QIC game (version I). This task is illustrated in Figure 4.3. Initially, Alice and Bob may share an arbitrary entangled state. However, they do not share any correlations with Charlie. Let A' and B denote the quantum systems at Alice's and Bob's locations, respectively. Charlie prepares the qubits A_j and C_j in the singlet state $|\Psi^-\rangle$, for $j = 0, 1, \ldots, n-1$. Charlie keeps the system $C \equiv C_0 C_1 \cdots C_{n-1}$ and sends Alice the system $A \equiv A_0 A_1 \cdots A_{n-1}$. Charlie generates a random integer $k \in \{0, 1, \ldots, n-1\}$ and gives it to Bob. Bob gives Charlie a qubit B_k, whose joint state with the qubit C_k, denoted as ω_k, must be as close as possible to the singlet. Alice and Bob may play any strategy allowed by quantum physics as long as the following constraint is satisfied: their communication is limited to a single message from Alice to Bob only, encoded in a quantum system T of m qubits, with $m < n$. Extra classical communication is not allowed. Let B' denote the joint system BT after Bob's quantum operations. In general, the qubit B_k is obtained by Bob from B'. Charlie applies a Bell measurement on the joint system $C_k B_k$. Alice and Bob win the game if Charlie obtains the outcome corresponding to the singlet. The success probability is

$$P \equiv \frac{1}{n} \sum_{k=0}^{n-1} \langle \Psi^- | \omega_k | \Psi^- \rangle. \tag{4.20}$$

The QIC game (version II). This version is similar to version I, with the following differences. Charlie does not prepare singlet states. Instead, Charlie prepares n qubits in the pure states $\{|\psi_j\rangle\}_{j=0}^{n-1}$, completely randomly. Charlie sends Alice the qubit A_j in the quantum state $|\psi_j\rangle$, for $j = 0, 1, \ldots, n-1$, and keeps a classical record of the states. We denote the global system that Alice receives from Charlie as $A \equiv A_0 A_1 \cdots A_{n-1}$. Bob gives Charlie a qubit B_k in the state ρ_k, which must be as close as possible to $|\psi_k\rangle$. Charlie measures the received state ρ_k in the orthonormal basis $\{|\psi_k\rangle, |\psi_k^\perp\rangle\}$, where $|\psi_k^\perp\rangle$ is the qubit state with Bloch vector antiparallel to that one of $|\psi_k\rangle$. Alice and Bob win the game if Charlie's measurement outcome corresponds to the state $|\psi_k\rangle$. The

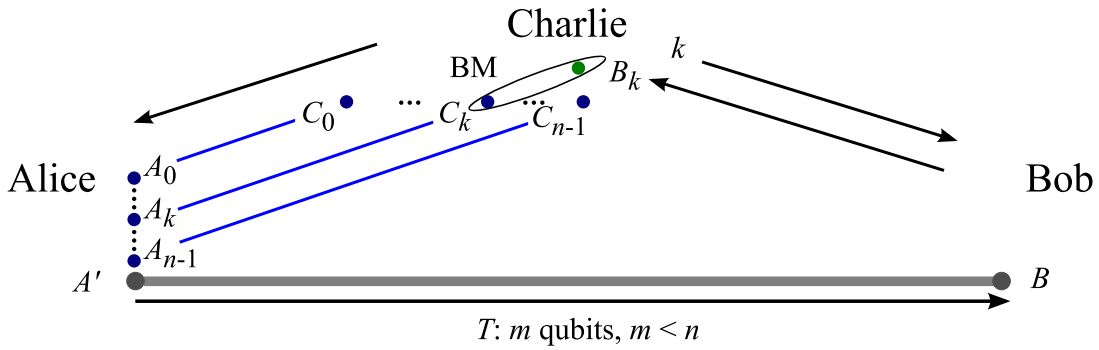


Figure 4.3: The QIC game (version I). Alice and Bob share an arbitrary entangled state in the quantum systems A' and B. Alice is given n qubits, $A_0, A_1, \ldots, A_{n-1}$, which are in singlet states with Charlie's respective qubits, $C_0, C_1, \ldots, C_{n-1}$. Bob is given a random integer $k \in \{0, 1, \ldots, n-1\}$ by Charlie. Bob gives Charlie a qubit B_k, whose joint state with the qubit C_k must be as close as possible to the singlet. Alice and Bob may play any quantum strategy as long as their communication is limited to a single message from Alice to Bob only, encoded in a quantum system T of m qubits, with $m < n$. Charlie applies a Bell measurement (BM) on the joint system $C_k B_k$. Alice and Bob win the game if Charlie obtains the outcome corresponding to the singlet.

success probability is

$$p \equiv \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \left(\frac{1}{n} \sum_{k=0}^{n-1} \langle \psi_k | \rho_k | \psi_k \rangle \right), \tag{4.21}$$

where $\int d\mu_j$ is the normalized integral over the Bloch sphere corresponding to the state $|\psi_j\rangle$.

We show in section 4.4.1 that the two version of the QIC game are equivalent and that their success probabilities satisfy the relation

$$p = \frac{1}{3}(1 + 2P). \tag{4.22}$$

For convenience, we only refer to version I from now on, unless otherwise stated.

Consider the following *naive* strategy to play the QIC game. Alice simply sends Bob m of the n qubits received from Charlie without applying any operations on these. Alice and Bob previously agree on which qubits Alice would send Bob, for example, those with index $0 \leq j < m$. If Bob receives from Charlie a number $k < m$, he outputs the correct state; in this case, $\langle \Psi^- | \omega_k | \Psi^- \rangle = 1$. However, if $k \geq m$, Bob does not have the correct state, hence, he can only give Charlie a fixed state, say $|0\rangle$; in this case, $\langle \Psi^- | \omega_k | \Psi^- \rangle = \frac{1}{4}$. Thus, this strategy succeeds with probability

$$P_{\mathrm{N}} = \frac{1}{4}\left(1 + 3\frac{m}{n}\right), \tag{4.23}$$

where the label N stands for *naive*. This strategy saturates the quantum information causality bound, as can be easily seen to achieve $\Delta I(C : B) = 2m$. But, it does not achieve the maximum success probability, because there are other strategies that achieve success probabilities higher than P_{N} (see section 4.5).

There is not an obvious relation between the quantum information causality bound and the maximum success probability in the QIC game. However, quantum information causality implies an upper bound on P. In particular, $P < 1$, if $m < n$.

4.4 Upper Bound on the Success Probability in the QIC Game

Quantum information causality implies an upper bound on the success probability in the QIC game:

$$P \leq P', \tag{4.24}$$

where P' is defined as the maximum solution of the equation

$$h(P') + (1 - P') \log_2 3 = 2\Big(1 - \frac{m}{n}\Big), \tag{4.25}$$

and $h(x) \equiv -x \log_2 x - (1-x) \log_2 (1-x)$ denotes the binary entropy. The value of P' is a strictly increasing function of the ratio $\frac{m}{n}$. It achieves $P' = \frac{1}{4}$, if $m = 0$ and $P' = 1$, if $m = n$. It follows that $P < 1$, if $m < n$. Some values of P' are plotted in Figure 4.6. The proof of the bound (4.24) requires several steps.

First, we show in section 4.4.1 that versions I and II of the QIC game are equivalent and that their success probabilities satisfy the relation (4.22).

Second, using version II of the QIC game, we show in section 4.4.2 that for any strategy that Alice and Bob may play that achieves success probability p, there exists a covariant strategy achieving the same value of p that Alice and Bob can perform. By covariance, we mean the following: if, when Alice's input qubit A_k is in the state $|\psi_k\rangle$, Bob's output qubit state is ρ_k, then, when A_k is in the state $U|\psi_k\rangle$, Bob's output state is $U\rho_k U^\dagger$, for any qubit state $|\psi_k\rangle \in \mathbb{C}^2$ and unitary operation $U \in \mathrm{SU}(2)$. Recall that k is the number that Charlie gives Bob. Therefore, without loss of generality, we consider that a covariant strategy is implemented. This means that the Bloch sphere of the qubit A_k is contracted uniformly and output in the qubit B_k. This implies that, in version II of the QIC game, the joint system $C_k B_k$ is transformed into the state

$$\omega_k = \lambda_k \Psi^- + \frac{1 - \lambda_k}{3}\big(\Psi^+ + \Phi^+ + \Phi^-\big), \tag{4.26}$$

where $\frac{1}{4} \leq \lambda_k \leq 1$ and Ψ^- denotes $|\Psi^-\rangle\langle\Psi^-|$, etc. That is, the depolarizing map [5] is applied to the qubit A_k and output by Bob in the qubit B_k.

Third, the data-processing inequality and the fact that the qubits C_j and $C_{j'}$

are in a product state for every $j \neq j'$ are used in section 4.4.3 to show that

$$\sum_{k=0}^{n-1} I(C_k : B_k) \leq I(C : B'). \tag{4.27}$$

In the QIC game, Charlie's and Bob's systems are initially uncorrelated. Thus, quantum information causality, Equation (4.10), reduces to $I(C : B') \leq 2m$ in this case. From this bound and (4.27), we obtain that

$$\sum_{k=0}^{n-1} I(C_k : B_k) \leq 2m. \tag{4.28}$$

Finally, below we use (4.26) and (4.28) to obtain an upper bound on $\frac{1}{n}\sum_{k=0}^{n-1}\lambda_k$, which equals P, as easily seen from (4.20) and (4.26).

We obtain from (4.26) that $I(C_k : B_k) = 2 - S(\omega_k)$. Thus, from (4.28), we have that

$$\frac{1}{n}\sum_{k=0}^{n-1} S(\omega_k) \geq 2\left(1 - \frac{m}{n}\right). \tag{4.29}$$

Consider the state $\omega \equiv \frac{1}{n}\sum_{k=0}^{n-1}\omega_k$. From the concavity property of the quantum entropy [5], we obtain that $S(\omega) \geq \frac{1}{n}\sum_{k=0}^{n-1} S(\omega_k)$, which together with Equation (4.29) implies

$$S(\omega) \geq 2\left(1 - \frac{m}{n}\right). \tag{4.30}$$

From the definition of P, Equation (4.20), and the form of the states ω_k, Equation (4.26), we obtain that

$$P = \frac{1}{n}\sum_{k=0}^{n-1}\lambda_k. \tag{4.31}$$

From the definition of the state ω and Equations (4.26) and (4.31), we have that

$$\omega = P\Psi^- + \frac{1-P}{3}\big(\Psi^+ + \Phi^+ + \Phi^-\big). \tag{4.32}$$

The quantum entropy of this state is $S(\omega) = h(P) + (1-P)\log_2 3$, where $h(x) \equiv$

$-x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy. Thus, from (4.30), we obtain

$$h(P)+(1-P)\log_2 3 \geq 2\left(1-\frac{m}{n}\right). \tag{4.33}$$

Satisfaction of (4.33) implies satisfaction of (4.24). This can be seen as follows. The function $h(P)+(1-P)\log_2 3$ corresponds to the classical entropy of a random variable taking four values, one with probability P and the others with probability $\frac{1}{3}(1-P)$ [5]. It is a strictly increasing function of P in the range $\left[0,\frac{1}{4}\right]$ and a strictly decreasing function in the range $\left[\frac{1}{4},1\right]$. It takes the values $\log_2 3$ at $P=0$ and $P=0.609$, 2 at $P=\frac{1}{4}$, and 0 at $P=1$. If $2\left(1-\frac{m}{n}\right)\geq\log_2 3$, Equation (4.25) has two solutions, one in the range $\left[0,\frac{1}{4}\right]$ and the other one in the range $\left[\frac{1}{4},0.609\right]$. Otherwise, Equation (4.25) has a single solution in the range $(0.609,1]$. Therefore, the maximum solution of Equation (4.25) is in the range $\left[\frac{1}{4},1\right]$. Since in this range the function $h(P)+(1-P)\log_2 3$ is strictly decreasing, Equation (4.33) implies Equation (4.24). In particular, it is easy to see from (4.30) that if $m<n$ then $S(\omega)>0$. Thus, in this case, ω cannot be a perfect singlet, which from (4.32) implies that $P<1$.

4.4.1 Equivalence of the Two Versions of the Game

Versions I and II of the QIC game are equivalent. This means that, if Alice and Bob play a strategy in version I of the QIC game that achieves a success probability P, the same strategy applied to version II achieves a success probability p that satisfies

$$p=\frac{1}{3}(1+2P), \tag{4.34}$$

for any strategy that they may play, and vice versa. We present the proof below.

For convenience, we use the notation $|\uparrow_{\vec{r}_k}\rangle\equiv|\psi_k\rangle$, $|\downarrow_{\vec{r}_k}\rangle\equiv|\psi_k^\perp\rangle$, in order to make clear that $|\uparrow_{\vec{r}_k}\rangle$ and $|\downarrow_{\vec{r}_k}\rangle$ correspond to pure qubit states with Bloch vectors $\vec{r}_k$ and $-\vec{r}_k$, respectively.

Version II of the QIC game is equivalent to the following. For every $j\in\{0,1,\ldots,n-1\}$, Charlie prepares the pair of qubits A_j and C_j in the singlet state $|\Psi^-\rangle$, he chooses a vector $\vec{r}_j$ completely randomly from the Bloch sphere, and he measures the qubit C_j in the orthonormal basis $\{|\uparrow_{\vec{r}_j}\rangle,|\downarrow_{\vec{r}_j}\rangle\}$. Due to the

properties of the singlet, if C_j projects into the state with Bloch vector $\pm\vec{r}_j$ then A_j projects into the state with Bloch vector $\mp\vec{r}_j$. Charlie sends Alice the system $A \equiv A_0 A_1 \cdots A_{n-1}$ and keeps the system $C \equiv C_0 C_1 \cdots C_{n-1}$. Charlie generates a random integer $k \in \{0, 1, \ldots, n-1\}$ that he gives Bob. Alice and Bob play the QIC game. Bob outputs a qubit B_k that he gives Charlie. Charlie measures B_k in the basis $\{|\uparrow_{\vec{r}_k}\rangle, |\downarrow_{\vec{r}_k}\rangle\}$. Alice and Bob win the game if B_k projects into the state with Bloch vector antiparallel to that one of the state of C_k. Since Charlie's initial measurements on his system C commute with Alice's and Bob's operations, it is equivalent to consider that Charlie does not apply any measurements on C before sending A to Alice, that he waits until receiving the qubit B_k to measure the joint system $C_k B_k$ in the basis $\mathcal{B}_{\vec{r}_k} \equiv \{|\uparrow_{\vec{r}_k}\rangle|\uparrow_{\vec{r}_k}\rangle, |\downarrow_{\vec{r}_k}\rangle|\downarrow_{\vec{r}_k}\rangle, |\uparrow_{\vec{r}_k}\rangle|\downarrow_{\vec{r}_k}\rangle, |\downarrow_{\vec{r}_k}\rangle|\uparrow_{\vec{r}_k}\rangle\}$. Opposite outcomes correspond to success. Therefore, the success probability p that Alice and Bob achieve in version II of the QIC game, defined by (4.21), equals the following:

$$p = \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \left[\frac{1}{n} \sum_{k=0}^{n-1} \left(\langle\uparrow_{\vec{r}_k}|\langle\downarrow_{\vec{r}_k}|\omega_k|\uparrow_{\vec{r}_k}\rangle|\downarrow_{\vec{r}_k}\rangle + \langle\downarrow_{\vec{r}_k}|\langle\uparrow_{\vec{r}_k}|\omega_k|\downarrow_{\vec{r}_k}\rangle|\uparrow_{\vec{r}_k}\rangle \right) \right], \tag{4.35}$$

where $\int d\mu_j$ is the normalized integral over the Bloch sphere corresponding to the Bloch vector $\vec{r}_j$ and we denote ω_k to the state of the joint system $C_k B_k$.

The Bell states defined in the basis $\mathcal{B}_{\vec{r}_k}$ are

$$\begin{aligned} |\Phi^{\pm}_{\vec{r}_k}\rangle &\equiv \frac{1}{\sqrt{2}}\left(|\uparrow_{\vec{r}_k}\rangle|\uparrow_{\vec{r}_k}\rangle \pm |\downarrow_{\vec{r}_k}\rangle|\downarrow_{\vec{r}_k}\rangle\right), \\ |\Psi^{\pm}_{\vec{r}_k}\rangle &\equiv \frac{1}{\sqrt{2}}\left(|\uparrow_{\vec{r}_k}\rangle|\downarrow_{\vec{r}_k}\rangle \pm |\downarrow_{\vec{r}_k}\rangle|\uparrow_{\vec{r}_k}\rangle\right). \end{aligned} \tag{4.36}$$

Consider that instead of measuring the state ω_k in the basis $\mathcal{B}_{\vec{r}_k}$, Charlie measures it in this Bell basis. Since the singlet state is the same in any basis, this corresponds to version I of the QIC game. Therefore, versions I and II of the QIC game are equivalent. We show below that their success probabilities satisfy the claimed relation.

Using the previous Bell basis, we obtain from (4.35) that

$$p = \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \left[\frac{1}{n} \sum_{k=0}^{n-1} \left(\langle \Psi^-_{\vec{r}_k} | \omega_k | \Psi^-_{\vec{r}_k} \rangle + \langle \Psi^+_{\vec{r}_k} | \omega_k | \Psi^+_{\vec{r}_k} \rangle \right) \right]. \tag{4.37}$$

Since the singlet state $|\Psi^-_{\vec{r}_k}\rangle$ is the same in any basis, from the definition of P, Equation (4.20), we have that

$$\int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \frac{1}{n} \sum_{k=0}^{n-1} \langle \Psi^-_{\vec{r}_k} | \omega_k | \Psi^-_{\vec{r}_k} \rangle = P. \tag{4.38}$$

On the other hand, we obtain that

$$\begin{aligned} \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \langle \Psi^+_{\vec{r}_k} | \omega_k | \Psi^+_{\vec{r}_k} \rangle &= \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \mathrm{Tr}\left(\omega_k | \Psi^+_{\vec{r}_k} \rangle \langle \Psi^+_{\vec{r}_k} | \right) \\ &= \mathrm{Tr}\left(\int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \omega_k | \Psi^+_{\vec{r}_k} \rangle \langle \Psi^+_{\vec{r}_k} | \right) \\ &= \mathrm{Tr}\left(\omega_k \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} | \Psi^+_{\vec{r}_k} \rangle \langle \Psi^+_{\vec{r}_k} | \right) \\ &= \mathrm{Tr}\left(\omega_k \int d\mu_k | \Psi^+_{\vec{r}_k} \rangle \langle \Psi^+_{\vec{r}_k} | \right), \end{aligned} \tag{4.39}$$

where in the second line we used the linearity of the trace; in the third line we used the fact that ω_k does not depend on the Bloch vector $\vec{r}_k$ because Charlie chooses it completely randomly to define the measurement basis $\mathcal{B}_{\vec{r}_k}$, and can do so after Bob gives him the qubit B_k, and naturally does not depend on the Bloch vectors $\vec{r}_j$ with $j \neq k$ for the same reason; and in the last line we used that the state $|\Psi^+_{\vec{r}_k}\rangle$ is defined in terms of the Bloch vector $\vec{r}_k$, which is parameterized by μ_k, and so is independent of the parameters μ_j with $j \neq k$.

Using the expressions

$$\begin{aligned} |\uparrow_{\vec{r}}\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right)|1\rangle, \\ |\downarrow_{\vec{r}}\rangle &= \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{i\phi} \cos\left(\frac{\theta}{2}\right)|1\rangle, \end{aligned} \tag{4.40}$$

for $\vec{r} \equiv (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, and computing the integral over the Bloch

sphere, $\int d\mu = \frac{1}{4\pi}\int_0^\pi d\theta \sin\theta \int_0^{2\pi} d\phi$, it is straightforward to obtain that

$$\int d\mu_k |\Psi^+_{\vec{r}_k}\rangle\langle\Psi^+_{\vec{r}_k}| = \frac{1}{3}\left(I - |\Psi^-\rangle\langle\Psi^-|\right), \tag{4.41}$$

where $|\Psi^-\rangle \equiv \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big)$ is the singlet state in the computational basis and I is the identity operator acting on $\mathbb{C}^4$. From (4.39), (4.41) and the definition of P, given by (4.20), we have that

$$\frac{1}{n}\sum_{k=0}^{n-1}\int d\mu_0 \int d\mu_1 \cdots \int d\mu_{n-1} \langle\Psi^+_{\vec{r}_k}|\omega_k|\Psi^+_{\vec{r}_k}\rangle = \frac{1}{3} - \frac{1}{3}P. \tag{4.42}$$

Finally, we substitute (4.38) and (4.42) into (4.37) to obtain the claimed relation, Equation (4.34).

4.4.2 Reduction to a Covariant Strategy

We show that for any strategy to play the QIC game there exists a covariant strategy that achieves the same success probability. For convenience, we consider version II of the QIC game.

Recall version II of the QIC game. Charlie gives Alice n qubits in the state $\vec{\psi} \equiv \otimes_{j=0}^{n-1}\big(|\psi_j\rangle\langle\psi_j|\big)_{A_j} \in \mathcal{D}\Big(\big(\mathbb{C}^2\big)^{\otimes n}\Big)$, where we define $\mathcal{D}(\mathcal{H})$ to be the set of density operators acting on the Hilbert space $\mathcal{H}$. Charlie gives Bob the number k. Let $\Gamma_k : \mathcal{D}\Big(\big(\mathbb{C}^2\big)^{\otimes n}\Big) \to \mathcal{D}\big(\mathbb{C}^2\big)$ be the map that Alice and Bob apply to the state $\vec{\psi}$. Bob outputs the state $\rho_k \equiv \Gamma_k\big(\vec{\psi}\big)$ and gives it to Charlie. Taking the average over all possible input pure product states of qubits with index $j \neq k$, Bob's output only depends on the state $\psi_k \equiv |\psi_k\rangle\langle\psi_k|$, as follows:

$$\bar{\Gamma}_k(\psi_k) \equiv \int d\mu_0 \int d\mu_1 \cdots \int d\mu_{k-1} \int d\mu_{k+1} \int d\mu_{k+2} \cdots \int d\mu_{n-1} \Gamma_k\big(\vec{\psi}\big), \tag{4.43}$$

where $\int d\mu_j$ is the normalized integral over the Bloch sphere corresponding to the state $|\psi_j\rangle$. From the definitions (4.21) and (4.43), we see that the success probability is

$$p = \frac{1}{n}\sum_{k=0}^{n-1}\int d\mu_k \langle\psi_k|\bar{\Gamma}_k(\psi_k)|\psi_k\rangle. \tag{4.44}$$

We notice that the success probability only depends on the averaged output $\bar{\Gamma}_k(\psi_k)$. Thus, the same success probability is achieved if we consider that Bob's output state is $\bar{\Gamma}_k(\psi_k)$. We show below that for any map $\Gamma_k\big(\vec{\psi}\,\big)$ that achieves success probability p, there exits a covariant averaged map $\bar{\Gamma}_k^{\text{cov}}(\psi_k)$ that Alice and Bob can implement achieving the same success probability p.

Consider the following map:

$$\bar{\Gamma}_k^{\text{cov}}(\phi) \equiv \int d\nu U_\nu^\dagger \bar{\Gamma}_k\big(U_\nu \phi U_\nu^\dagger\big) U_\nu, \tag{4.45}$$

where $\phi \in \mathcal{D}\big(\mathbb{C}^2\big)$, $U_\nu \in \text{SU}(2)$ and $d\nu$ is the Haar measure on SU(2). It is easy to see that this map is covariant, that is, $\bar{\Gamma}_k^{\text{cov}}\big(U\phi U^\dagger\big) = U\bar{\Gamma}_k^{\text{cov}}(\phi)U^\dagger$, for all $\phi \in \mathcal{D}\big(\mathbb{C}^2\big)$ and $U \in \text{SU}(2)$. In principle, for any map Γ_k that Alice and Bob perform, they can implement the covariant map $\bar{\Gamma}_k^{\text{cov}}$ as follows. Alice and Bob initially share randomness. With uniform probability, they obtain the random number ν in the range $d\nu$ that corresponds to an, ideally, infinitesimal region of the Haar measure on SU(2). This can be done, for example, if Alice and Bob share a maximally entangled state of arbitrarily big dimension and they both apply a local projective measurement in the Schmidt basis on their part of the state, with their measurement outcome indicating the number ν. Alice applies the unitary operation U_ν parameterized by the obtained number ν on each of her input qubit states $|\psi_j\rangle$. Then, Alice and Bob apply the map Γ_k to the input state $\otimes_{j=0}^{n-1}\big(U_\nu|\psi_j\rangle\langle\psi_j|U_\nu^\dagger\big)_{A_j}$. Finally, Bob applies the unitary $U_\nu^\dagger$ to his output qubit. From the definitions (4.43) and (4.45), we see that, taking the average over all shared random numbers ν and over all possible input pure qubit states with index distinct to k, Bob's output is $\bar{\Gamma}_k^{\text{cov}}(\psi_k)$.

It is straightforward to see that the map $\bar{\Gamma}_k^{\text{cov}}$ satisfies

$$\int d\mu_k \langle\psi_k|\bar{\Gamma}_k^{\text{cov}}(\psi_k)|\psi_k\rangle = \int d\mu_k \langle\psi_k|\bar{\Gamma}_k(\psi_k)|\psi_k\rangle. \tag{4.46}$$

From (4.44) and (4.46), we see that the map $\bar{\Gamma}_k^{\text{cov}}(\psi_k)$ achieves the same success probability as $\bar{\Gamma}_k(\psi_k)$. Thus, for convenience, we consider that Alice and Bob

implement the covariant map $\bar{\Gamma}_k^{\text{cov}}(\psi_k)$. In general, this is the depolarizing map [5]:

$$\bar{\Gamma}_k^{\text{cov}}(\phi) = \sum_{i=0}^{3} E_i \phi E_i^\dagger,$$

where $\phi \in \mathcal{D}\big(\mathbb{C}^2\big)$, $E_0 = \sqrt{\lambda_k} I$, $E_i = \sqrt{\frac{1}{3}(1-\lambda_k)}\sigma_i$, $\frac{1}{4} \leq \lambda_k \leq 1$ and σ_i are the Pauli matrices, for $i = 1, 2, 3$. Application of the depolarizing map to a qubit that is in the singlet state with another qubit, as in version I of the QIC game, gives the output state

$$\omega_k = \lambda_k \Psi^- + \frac{1-\lambda_k}{3}\big(\Psi^+ + \Phi^+ + \Phi^-\big), \tag{4.47}$$

where $\frac{1}{4} \leq \lambda_k \leq 1$ and Ψ^- denotes $|\Psi^-\rangle\langle\Psi^-|$, etc., as in (4.26).

4.4.3 A Useful Bound

We show the following bound:

$$\sum_{k=0}^{n-1} I\left(C_k : B_k\right) \leq I\left(C : B'\right). \tag{4.48}$$

The proof is equivalent to the one for classical bits [71].

From the definition of the quantum mutual information, we obtain

$$\begin{aligned} I\left(C : B'\right) &\equiv I\left(C_0 C_1 \cdots C_{n-1} : B'\right) \\ &= I\left(C_0 : B'\right) + I\left(C_1 C_2 \cdots C_{n-1} : B' C_0\right) - I\left(C_1 C_2 \cdots C_{n-1} : C_0\right). \end{aligned} \tag{4.49}$$

Since Charlie's qubits are in a product state with each other, we have that

$$I\left(C_1 C_2 \cdots C_{n-1} : C_0\right) = 0. \tag{4.50}$$

The data-processing inequality implies that discarding a quantum system cannot

increase the quantum mutual information. Thus, it follows that

$$I\left(C_1C_2\cdots C_{n-1}:B'C_0\right)\geq I\left(C_1C_2\cdots C_{n-1}:B'\right). \tag{4.51}$$

From (4.49) – (4.51), we obtain that

$$I\left(C_0C_1\cdots C_{n-1}:B'\right)\geq I\left(C_0:B'\right)+I\left(C_1C_2\cdots C_{n-1}:B'\right).$$

After iterating these steps $n-1$ times, we have

$$I\left(C:B'\right)\geq\sum_{k=0}^{n-1}I\left(C_k:B'\right). \tag{4.52}$$

Since the system B_k is output by Bob after local operations on his system B', applying the data-processing inequality, we obtain $I(C_k:B')\geq I(C_k:B_k)$, which from (4.52) implies the bound (4.48).

4.5 Strategies in the QIC Game

As mentioned in section 4.3, a simple strategy in the QIC game is the naive strategy. For completeness of this section, we present it again.

The naive strategy in the QIC game. Alice sends Bob m of the n qubits received from Charlie without applying any operations on these. Alice and Bob previously agree on which qubits Alice would send Bob, for example, those with index $0\leq j<m$. If Bob receives from Charlie a number $k<m$, he outputs the correct state; in this case, $\langle\Psi^-|\omega_k|\Psi^-\rangle=1$. However, if $k\geq m$, Bob does not have the correct state, hence, he can only give Charlie a fixed state, say $|0\rangle$; in this case, $\langle\Psi^-|\omega_k|\Psi^-\rangle=\frac{1}{4}$. Thus, this strategy succeeds with probability

$$P_{\mathrm{N}}=\frac{1}{4}\Big(1+3\frac{m}{n}\Big), \tag{4.53}$$

where the label N stands for *naive*.

The naive strategy saturates the quantum information causality bound, Equation (4.10), because it achieves $I(C:B)=2m$. Bob obtains complete quantum

information about m of the n qubit states prepared by Charlie, but he does not know anything about the other ones. This strategy is extremely simple. It does not require that Alice and Bob share any entanglement. There exists a more powerful class of strategies, which requires entanglement and uses the protocol of quantum teleportation.

4.5.1 Teleportation Strategies

The *teleportation strategies* aim to teleport the n input qubit states from Alice's to Bob's location. This cannot be done perfectly due to the restricted amount of communication. The quantum states of the n input qubits are immediately accessible to Bob after Alice has applied the corresponding Bell measurements, but with some teleportation errors. Alice and Bob perform a protocol, which involves the transmission of m qubits from Alice to Bob, so that, with high probability, Bob can correct the teleportation error of the qubit state asked by Charlie. The correction stage involves a task of classical inputs and outputs, the IC-2 game.

The IC-2 game is similar to the IC game, described in section 4.1.2, with the difference that the inputs and outputs are two bit numbers (see Figure 4.4).

The IC-2 game. Alice is given a random string of n two bit numbers, $\vec{x} \equiv (x_0, x_1, \ldots, x_{n-1})$, where $x_j \equiv (x_j^0, x_j^1)$ and $x_j^0, x_j^1 \in \{0,1\}$, for $j = 0, 1, \ldots, n-1$. Bob is given a random value of $k = 0, 1, \ldots, n-1$. The game's goal is that Bob outputs x_k. Alice and Bob can perform any strategy allowed by quantum physics with the only condition that communication is limited to a single message of $2m$ bits from Alice to Bob, with $m < n$. In particular, Alice and Bob may use an arbitrary entangled state. Let $y_k \equiv (y_k^0, y_k^1)$ be Bob's output, where $y_k^0, y_k^1 \in \{0,1\}$.

The success probability in the IC-2 game is defined as

$$Q \equiv \frac{1}{n} \sum_{k=0}^{n-1} P\left(y_k = x_k\right). \tag{4.54}$$

The teleportation strategies combine the protocols of quantum teleportation [13], superdense coding [12] and the IC-2 game (see Figure 4.5).

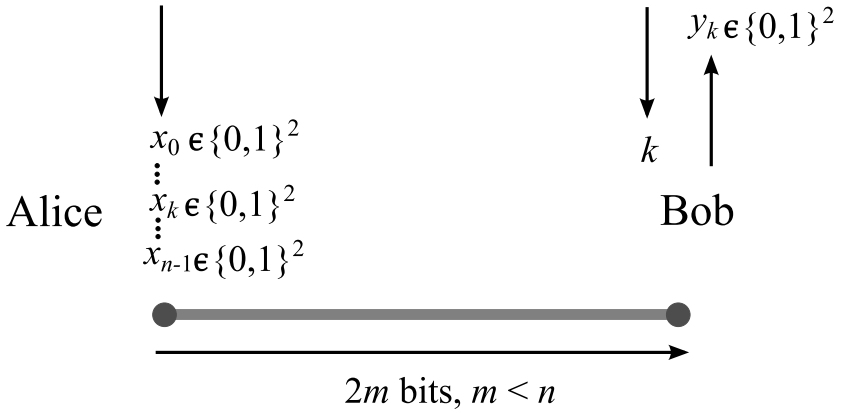


Figure 4.4: The IC-2 game. Alice is given a random string of n two bit numbers, $x_0, x_1, \ldots, x_{n-1}$. Bob is given a random number $k = 0, 1, \ldots, n-1$. Bob outputs a two bit number y_k. Alice and Bob win the game if $y_k = x_k$. Alice and Bob can play any strategy allowed by quantum physics with the only condition that communication is limited to a single message of $2m$ bits from Alice to Bob, with $m < n$. In particular, Alice and Bob may use an arbitrary entangled state.

Teleportation strategies in the QIC game. Alice and Bob share a singlet state in the qubits A'_j, at Alice's site, and B_j, at Bob's site, for $j = 0, 1, \ldots, n-1$. Alice applies a Bell measurement on her qubits $A_j A'_j$ and obtains the two bit outcome $x_j \equiv (x_j^0, x_j^1)$. Thus, the state of the qubit A_j is teleported to Bob's qubit B_j, up to the Pauli error σ_{x_j}. This means that the joint state of the system $C_j B_j$ transforms into one of the four Bell states, according to the value of x_j. Alice and Bob play the IC-2 game, with Alice's and Bob's inputs being $\vec{x} = (x_0, x_1, \ldots, x_{n-1})$ and k, respectively. However, instead of sending Bob the $2m-$bits message directly, Alice encodes it in m qubits via superdense coding. Bob receives the m qubits and decodes the correct $2m$-bits message, which he inputs to his part of the IC-2 game. Bob outputs the two bit number $y_k \equiv (y_k^0, y_k^1)$ and applies the Pauli correction operation σ_{y_k} on the qubit B_k, which then he outputs and gives to Charlie. If $y_k = x_k$, the output state ω_k of the system $C_k B_k$ is the singlet; otherwise, we have that $\langle \Psi^- | \omega_k | \Psi^- \rangle = 0$. Thus, from the definition of P, Equation (4.20), we see that $P = Q$, where Q is defined by (4.54).

The best strategy that we have found to play the QIC game in the case $m = 1$ is a teleportation strategy in which the IC-2 game is played with two

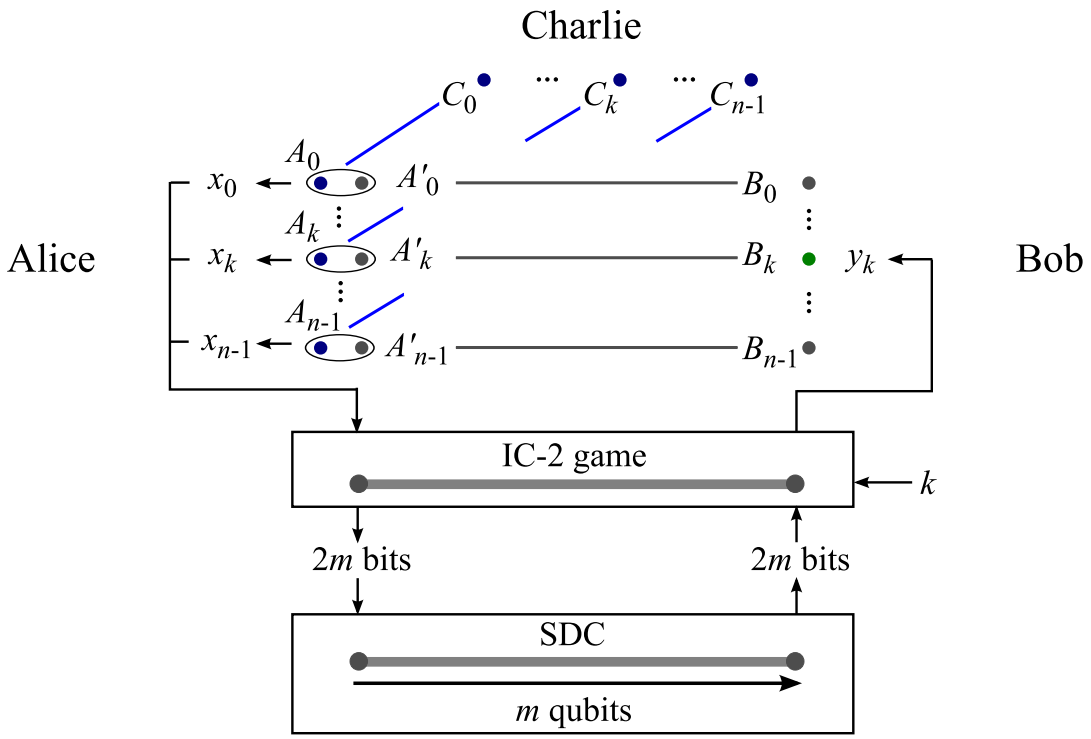


Figure 4.5: Teleportation strategies in the QIC game. Alice and Bob share singlets in their respective qubits $A'_0, A'_1, \ldots, A'_{n-1}$ and $B_0, B_1, \ldots, B_{n-1}$. Alice applies a Bell measurement on her qubits $A_j A'_j$ and obtains the two bit outcome x_j, for $j = 0, 1, \ldots, n-1$. Alice and Bob play the IC-2 game, with Alice's and Bob's inputs being $x_0, x_1, \ldots, x_{n-1}$ and k, respectively. Alice encodes her $2m-$bits message in m qubits via superdense coding (SDC). Bob outputs the two bit number y_k and applies the encoded Pauli correction operation σ_{y_k} on the qubit B_k, which then he outputs and gives to Charlie. If $y_k = x_k$, the state of the qubit A_k is teleported to the qubit B_k without error, which means that the system $C_k B_k$ is transformed into the singlet, and hence that Alice and Bob win the QIC game.

equivalent and independent protocols in the IC-1 game.[1] In both protocols Bob inputs the number k, while Alice inputs the bits $\{x_j^0\}_{j=0}^{n-1}$ in the first protocol and the bits $\{x_j^1\}_{j=0}^{n-1}$ in the second one. If Bob outputs the correct value of x_k^0 with probability q in the first protocol, and similarly, he outputs the correct value of x_k^1 with probability q in the second protocol, for any k, then the success probability in the IC-2 game is $Q = q^2$. The maximum value of q that has been shown [107, 108] is $q = \frac{1}{2}\left(1 + \frac{1}{\sqrt{n}}\right)$. With this value of Q, Alice and Bob achieve a success probability in the QIC game of

$$P_{\mathrm{T}} = \frac{1}{4}\left(1 + \frac{1}{\sqrt{n}}\right)^2, \tag{4.55}$$

where the label T stands for *teleportation*. Some values of P_{T}, P_{N} and P', in the case $m = 1$, are plotted in Figure 4.6.

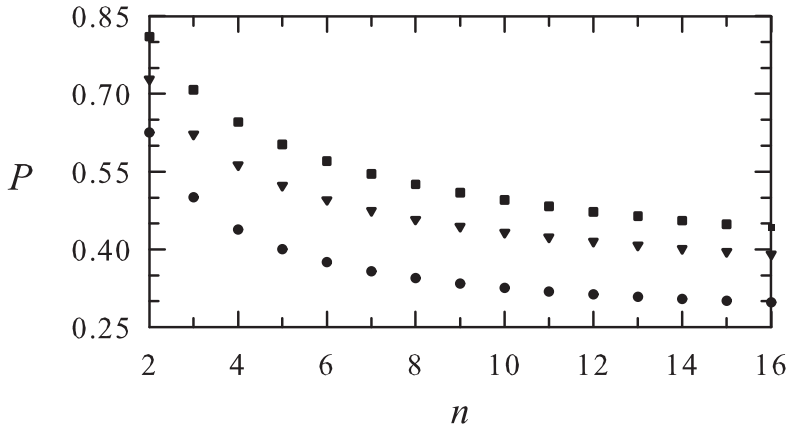


Figure 4.6: Success probability (P) in the QIC game for $m = 1$ achieved with the naive strategy, P_{N} (circles), and with the best teleportation strategy that we have found, P_{T} (triangles). The upper bound on P obtained from quantum information causality, P' (squares), is plotted too.

[1] We denote the IC game described in section 4.1.2 as the IC-1 game in order to make clear that the inputs and outputs are one bit numbers.

An explicit strategy to achieve the success probability $q = \frac{1}{2}\big(1 + \frac{1}{\sqrt{n}}\big)$ in the IC-1 game for $m = 1$ is given by an EARAC in the case $n = 2^h 3^l$ with h, l nonnegative integers [107]. This protocol consists in a concatenation of two primitive EARACs, $\Big(2, 1, \frac{1}{2}\big(1 + \frac{1}{\sqrt{2}}\big)\Big)$ and $\Big(3, 1, \frac{1}{2}\big(1 + \frac{1}{\sqrt{3}}\big)\Big)$. Recall from section 4.1.2 that in an (n, m, p) EARAC, Alice has n input bits, she sends Bob m bits, Bob outputs any, but only one, of Alice's bits with probability at least p and shared entanglement is used.

We review the $\Big(2, 1, \frac{1}{2}\big(1 + \frac{1}{\sqrt{2}}\big)\Big)$ EARAC presented in [107]. Alice and Bob share a singlet state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big)$. Let Alice's input bits be x_0 and x_1. Alice and Bob measure their qubits in the orthonormal bases $\{|e_r^x\rangle\}_{r=0}^1$ and $\{|f_s^k\rangle\}_{s=0}^1$, respectively. Alice measures in the basis with label $x = x_0 \oplus x_1 \in \{0, 1\}$, where $\oplus$ denotes sum modulo 2. Bob measures in the basis with label $k \in \{0, 1\}$ in order to learn the bit x_k. Alice and Bob obtain the bit outcomes r and s, respectively. Alice sends Bob the one bit message $\tau = x_0 \oplus r$. Bob outputs the bit $y_k = \tau \oplus s$. It is easy to see that $y_k = x_k$ with probability $P(r \oplus s = xk)$. Recall from section 4.1.2 that $P(r \oplus s = xk)$ is the probability to win the CHSH game, which satisfies Cirel'son's bound, Equation (4.9). Thus, its maximum value is $P(r \oplus s = xk) = \frac{1}{2}\big(1 + \frac{1}{\sqrt{2}}\big)$. It is achieved with the following basis states:

$$\begin{aligned} |e_r^x\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\gamma_r^x \pi}|1\rangle\big), \\ |f_s^k\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\delta_s^k \pi}|1\rangle\big), \end{aligned}$$

where $\gamma_0^0 = \frac{1}{4}$, $\gamma_1^0 = -\frac{3}{4}$, $\gamma_0^1 = -\frac{1}{4}$, $\gamma_1^1 = \frac{3}{4}$, $\delta_0^0 = 1$, $\delta_1^0 = 0$, $\delta_0^1 = -\frac{1}{2}$, $\delta_1^1 = \frac{1}{2}$.

4.5.2 An Optimal Strategy

An optimal strategy in the QIC game is a teleportation strategy in which the IC-2 game is played optimally. For a fixed value of m and n such that $m < n$, we define $Q_{\max}$ and $P_{\max}$ to be the maximum values of Q and P over all possible strategies to play the IC-2 game and the QIC game, respectively. We show that

$$P_{\max} = Q_{\max}. \tag{4.56}$$

It was shown above that a teleportation strategy achieves a success probability $P = Q$, where Q is the success probability in the IC-2 game played within the teleportation strategy. Thus, a teleportation strategy in which the IC-2 game is played optimally achieves a success probability $P = Q_{\max}$. Therefore, Equation (4.56) follows if

$$P \leq Q_{\max}, \tag{4.57}$$

for a general strategy in the QIC game. To show (4.57), we consider the following class of strategies to play the IC-2 game (see Figure 4.7).

Superdense coding strategies in the IC-2 game. Alice and Bob initially share a singlet state in the qubits A_j and C_j, for $j = 0, 1, \ldots, n-1$. Alice has the system $A \equiv A_0 A_1 \cdots A_{n-1}$. Bob has the system $C \equiv C_0 C_1 \cdots C_{n-1}$. Alice and Bob share an arbitrary entangled state in the system A', at Alice's location, and B at Bob's location. Alice applies the unitary operation σ_{x_j} on the qubit A_j, for $j = 0, 1, \ldots, n-1$, where $\sigma_{0,0} \equiv I$ is the identity operator acting on $\mathbb{C}^2$ and $\sigma_{0,1} \equiv \sigma_1$, $\sigma_{1,0} \equiv \sigma_2$, $\sigma_{1,1} \equiv \sigma_3$ are the Pauli matrices. Then, Alice and Bob play the QIC game. Alice applies operations on the input system A and her ancilla A', and obtains a system T of m qubits. But, instead of sending T directly to Bob, Alice teleports [13] its state, using more entanglement shared with Bob. Thus, communication consists of $2m$ bits only, as required by the IC-2 game. Bob applies operations on the teleported state and his system B to obtain the output qubit B_k. At this stage, for consistency with the QIC game, Bob does not apply any operations on the system C. As previously indicated, we can consider that in a general strategy in the QIC game, the depolarizing map is applied on the qubit A_k and output by Bob in the qubit B_k. Since this map commutes with the operation σ_{x_k} applied by Alice on A_k, Bob outputs B_k in the following joint state with the qubit C_k: $\Omega_k = (\sigma_{x_k} \otimes I)\omega_k(\sigma_{x_k} \otimes I)$. From the form of ω_k, Equation (4.47), we have that

$$\Omega_k = \sigma_{x_k} \otimes I \Big[\lambda_k \Psi^- + \frac{1-\lambda_k}{3} \big(\Psi^+ + \Phi^+ + \Phi^- \big) \Big] \sigma_{x_k} \otimes I. \tag{4.58}$$

Bob applies a Bell measurement on the state Ω_k. The outcome $y_k \in \{0,1\}^2$ indicates that Ω_k projects into the Bell state $\sigma_{y_k} \otimes I |\Psi^-\rangle_{B_k C_k}$. From (4.58), the

probability that y_k equals the value x_k encoded by Alice is $P(y_k = x_k) = \lambda_k$. Thus, from (4.54), we have that $Q = \frac{1}{n}\sum_{k=0}^{n-1}\lambda_k$. It follows from (4.31) that $Q = P$. That is, the success probability Q achieved by this class of strategies in the IC-2 game equals the success probability P in the QIC game played within. Since the QIC game is played arbitrarily and $Q \leq Q_{\max}$, we obtain (4.57).

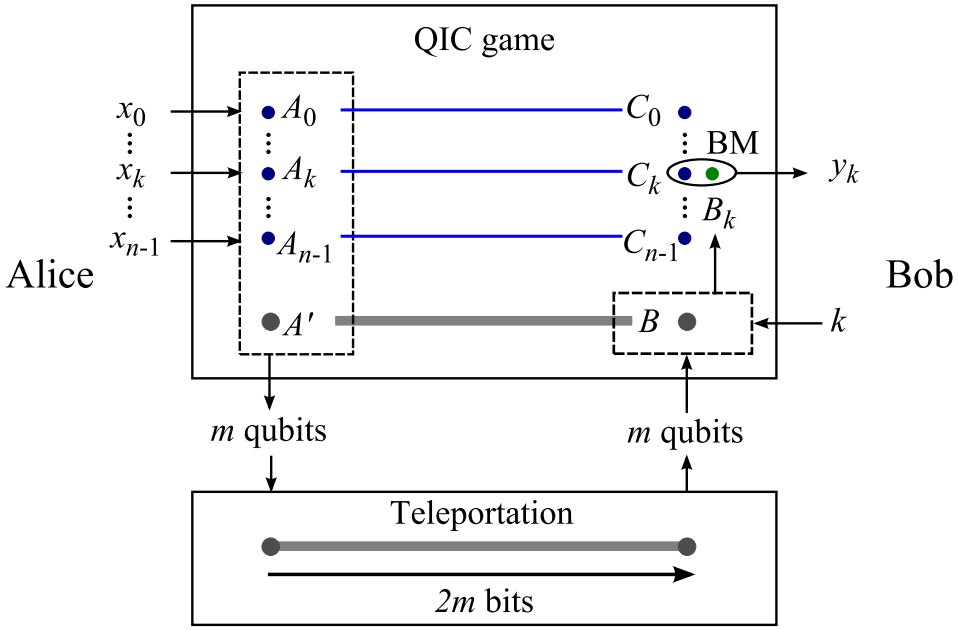


Figure 4.7: Superdense coding strategies in the IC-2 game. Alice and Bob share singlets in the qubits $A_0, A_1, \ldots, A_{n-1}$ and $C_0, C_1, \ldots, C_{n-1}$. Alice encodes her two bit inputs x_k by applying the Pauli operations σ_{x_k} on her qubits A_k. Then, Alice and Bob play the QIC game using their ancillary system $A'B$. Alice's $m-$qubits message is sent to Bob via quantum teleportation. Bob outputs a qubit B_k in the QIC game. Then, Bob applies a Bell measurement (BM) on C_kB_k, and obtains the two bit outcome y_k. The probability to win the IC-2 game equals the probability to win the QIC game played within.

The value of $Q_{\max}$ and a strategy that achieves it remain as open problems. We have obtained an upper bound on Q for a particular class of strategies, *nonlocal strategies*, in the case $m = 1$.

4.5.3 Nonlocal Strategies

We consider teleportation strategies in the case $m = 1$ for which the IC-2 game is played as follows.

Nonlocal strategies in the IC-2 game. Alice and Bob share an entangled state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Alice has the system A and Bob has the system B. Alice and Bob measure their systems in the orthonormal bases $\{|\nu^{\vec{x}}_{r,s}\rangle\}^1_{r,s=0}$ and $\{|w^k_{t,u}\rangle\}^1_{t,u=0}$, respectively. They choose their measurements according to the value of $\vec{x} = (x_0, x_1, \ldots, x_{n-1})$ and k. Recall that $x_j \equiv (x^0_j, x^1_j)$ is a two bit number, for $j = 0, 1, \ldots, n-1$. Alice's and Bob's measurement outcomes are the two bit numbers (a^0_k, a^1_k) and (b^0_k, b^1_k), respectively. That is, after the measurement is completed, $|\psi\rangle$ projects into the state $|\nu^{\vec{x}}_{a^0_k,a^1_k}\rangle|w^k_{b^0_k,b^1_k}\rangle$. Alice sends Bob her outcome. Bob outputs the two bit value $y_k \equiv (y^0_k, y^1_k)$, where $y^j_k = a^j_k \oplus b^j_k$, for $j = 0, 1$, and $\oplus$ denotes sum modulo 2. The success probability is

$$Q = \frac{1}{n}\sum_{k=0}^{n-1} P\left(y^0_k = x^0_k, y^1_k = x^1_k\right). \tag{4.59}$$

There is an upper bound on Q for this class of strategies:

$$Q \leq Q', \tag{4.60}$$

where $Q' \equiv \frac{1}{4}\left(1 + \frac{3}{\sqrt{n}}\right)$. This bound does not imply that $Q_{\max} \leq Q'$, because there can be strategies more general than the nonlocal strategies, for example, those in which Bob uses Alice's message in order to choose his measurement. Moreover, quantum information causality implies that the previous bound cannot be achieved for $n \geq 50$. It can easily be computed that if $m = 1$ and $n \geq 50$, $P' < Q'$, where P' is defined by (4.25). Therefore, if the bound (4.60) were saturated, a teleportation strategy achieving $P = Q'$ would satisfy $P' < P$, violating the inequality (4.24), and hence quantum information causality.

The proof of (4.60) is presented in Appendix D. It is an extension of the one given in [108] for the IC-1 game.

4.6 Discussion

In this chapter, we have introduced the principle of quantum information causality. Quantum information causality, Equation (4.10), states the maximum amount of quantum information that a transmitted quantum system can communicate as a function of its dimension, independently of any quantum physical resources previously shared by the communicating parties. Its proof follows from three properties of the quantum entropy: subadditivity, the data-processing inequality and the triangle inequality. The triangle inequality provides the main difference compared to the proof of information causality. Information causality, Equation (4.19), considers the particular case in which the transmitted system is classical. If the transmitted system is classical, the triangle inequality, Equation (4.13), in the proof of quantum information causality cannot be saturated.

The concept of entropy in mathematical frameworks for general probabilistic theories [33, 115, 116] and its implication for information causality have been recently investigated [108, 117–119]. Particularly, it has been shown that a physical condition on the measure of entropy implies subadditivity and the data-processing inequality, and hence that information causality follows from this condition [108]. It would be interesting to investigate whether physically-sensible definitions of entropy for more general probabilistic theories satisfy subadditivity, the data-processing and the triangle inequalities, and hence a generalized version of quantum information causality. A different version of information causality in more general probabilistic theories has been considered in [120].

We have presented a new quantum information task, the QIC game. We have shown an upper bound, Equation (4.24), on the success probability P in the QIC game from quantum information causality. The bound implies, in particular, that $P < 1$, if $m < n$. This means that Bob is unable to perfectly reproduce the kth state from a set of n unknown qubit states at Alice's location, if Alice does not know the number k and Bob only receives a message of less than n qubits from Alice, independently of any quantum physical resources previously shared by them. We have presented two versions of the QIC game, which we have shown are equivalent and whose success probabilities satisfy an equality relation, Equation (4.34). In version I, Charlie prepares singlets; in version II, he prepares

pure qubit states, totally randomly. It would be interesting to investigate more general versions of the game, for example, versions in which the input states have higher dimension or in which they are not generated completely randomly. It would also be interesting to investigate possible extensions to multipartite scenarios.

We have presented a class of strategies in the QIC game, teleportation strategies, that combine the protocols of quantum teleportation, superdense coding and a task with classical inputs and outputs, the IC-2 game. The IC-2 game is intimately related to the QIC game, as suggested by (4.56). Moreover, as easily seen from Figures 4.5 and 4.7, the teleportation strategies in the QIC game and the superdense coding strategies in the IC-2 game are related in a way that resembles the relation between the quantum teleportation and superdense coding protocols. We have shown that an optimal strategy in the QIC game is a teleportation strategy in which the IC-2 game is played optimally. An optimal strategy in the IC-2 game remains as an interesting open problem.

Chapter 5

Conclusions

Quantum theory predicts the existence of correlations that violate the Bell inequalities, and hence that cannot be described by local hidden variable theories (LHVT) [2]. However, these nonlocal quantum correlations cannot be used for instantaneous communication because of the no-signalling principle [69]. The no-signalling principle states that two distant parties cannot communicate any information without the transmission of any physical systems, despite any quantum physical resources shared by them. This is a fundamental physical principle that allows quantum theory to be consistent with relativistic causality. The no-signalling principle imposes important constraints on quantum information tasks. Our PhD research focused on the investigation of Bell inequalities from a new perspective [94], the implications of the no-signalling principle for quantum information tasks [99], and extensions of the no-signalling principle [104].

The problems that we have discussed along this thesis can be presented in a unifying scenario. Consider a general information task performed by two distant parties, Alice and Bob. This task can be extended to include multiple parties, but we restrict here to consider the bipartite case. The information properties of different physical theories, quantum or non-quantum, can be investigated in this scenario. The goal of the considered task is that Bob outputs some specific information originally at Alice's location. Alice and Bob can perform any strategy allowed by the theory that is being analyzed, for which they can use physical resources of certain type, and are required to satisfy specific constraints. The information task is defined by the type of information originally at Alice's

location, the type of information that Bob has to output, the physical resources that Alice and Bob have access to, the constraints that they need to satisfy, and the physical theory ruling the task.

Physical theories satisfying the principle of local causality are investigated by tasks in which Alice and Bob cannot transmit any physical systems to each other, the resources they have access to are described by LHVT, and the task goal is that, after they input respective random numbers $A \in \mathcal{A}$ and $B \in \mathcal{B}$ to their resources, Alice and Bob output numbers a and b that are correlated in a specific way defined by the task. Bounds on the probability to succeed in these tasks define Bell inequalities, which characterize the information limitations of LHVT.

Bell inequalities in which $\mathcal{A}$ and $\mathcal{B}$ are finite sets have been investigated in great detail. Important Bell inequalities are the CHSH [42] and the Braunstein-Caves [45] inequalities, which consider the cases $|\mathcal{A}| = |\mathcal{B}| = 2$ and $|\mathcal{A}| = |\mathcal{B}| = N$, respectively, for which a and b take one of two possible values. Our contribution in chapter 2 has been to introduce a setting in which $\mathcal{A}$ and $\mathcal{B}$ are chosen from a continuous set, thus generalizing the settings considered by the CHSH and the Braunstein-Caves inequalities. We have considered the particular case in which this set is a pair of unit spheres, which follows from the constraint studied by us in which a and b can have only two possible values. In the case we have considered, A and B are chosen randomly, but are fixed to satisfy a given separation angle θ in the spheres. We obtained Bell inequalities for all values of $\theta \in [0, \frac{\pi}{2}]$, given by Theorem 2.1. These inequalities distinguish all LHV correlations from the singlet state quantum correlations for $\theta \in \left(0, \frac{\pi}{3}\right)$, as stated by Lemma 2.4. We have motivated and explored, numerically and analytically, hypotheses implying that our obtained Bell inequalities are not optimal for all range of θ. The strong hemispherical colouring maximality hypothesis (SHCMH) states that an LHVT in which the possible outcomes a correspond to a sphere with opposite hemispheres coloured oppositely and the possible outcomes b correspond to a sphere with the reverse colouring, in which different colours determine different measurement outcomes, maximizes the LHV anticorrelations for a continuous range of $\theta > 0$. The weak hemispherical colouring maximality hypothesis (WHCMH) states that such a colouring maximizes the LHV anticorrelations for a continuous range of $\theta > 0$ among restricted colourings in which the pair of spheres are coloured

oppositely. The investigation of different geometries for continuous sets $\mathcal{A}$ and $\mathcal{B}$, corresponding to bigger numbers of possible values that a and b can take, will lead to Bell inequalities generalizing the ones we have investigated.

Different quantum information tasks can be investigated in the general setting introduced above. An important class of quantum tasks corresponds to quantum teleportation protocols [13]. In quantum teleportation, Bob needs to output an unknown quantum state originally at Alice's location, Alice and Bob have access to an arbitrary quantum state that they share, and they can perform arbitrary communication, as long as this is classical.

Port-based teleportation (PBT) protocols [100, 101] were considered in chapter 3. These protocols have the particular characteristic that, in order to obtain the teleported state, the only operation that Bob needs to perform after receiving Alice's message consists in selecting the particular port informed by Alice. We analyzed PBT protocols in a general setting in which the teleported state is an unknown $n-$qubits state, the resources used by Alice and Bob consist of an arbitrary quantum state $|\xi\rangle_{AB}$, and Alice's operations correspond to a general quantum measurement. In the PBT protocols we considered, the state is teleported perfectly, which requires the protocol to fail with some finite probability. Our contribution is a proof of the upper bound (3.1) on the success probability of PBT from the no-signalling principle and a version of the no-cloning theorem, Theorem 3.1, introduced by us. It is an interesting open problem to find whether the obtained bound is achievable. It would also be interesting to investigate whether the no-signalling principle implies an upper bound on the average fidelity of deterministic PBT protocols, in which the protocol always succeeds but the state is teleported with a fidelity smaller than unity.

Physical theories restricted by the no-signalling principle are investigated by tasks in which Alice's and Bob's resources are constrained by this principle, Alice and Bob cannot transmit any physical systems to each other, and the task goal is that Bob outputs some specific information previously unknown to him that is at Alice's location. Theories satisfying particular extensions of the no-signalling principle can be investigated if Alice and Bob can transmit a finite amount of physical systems restricted to be of a given dimension. The information causality principle [71] considers the scenario in which the information originally at Alice's

location that Bob needs to output and the transmitted physical system are classical. The quantum information causality principle, introduced by us in chapter 4, considers the scenario in which the information at Alice's location that Bob needs to output and the transmitted system are quantum.

Quantum information causality states the maximum amount of quantum information that a transmitted quantum system can communicate as a function of its dimension, independently of any quantum physical resources previously shared by the communicating parties, Equation (4.10). We have found that an important application of quantum information causality is that it imposes an upper bound, Equation (4.24), on the success probability in the QIC game, a new quantum information task introduced in section 4.3. This bound implies, in particular, that Bob is unable to perfectly reproduce the kth state from a set of n unknown qubit states at Alice's location, if Alice does not know the number k and Bob only receives a message of less than n qubits from Alice, independently of any quantum physical resources previously shared by them. It was shown in section 4.5.2 that the maximum success probability in the QIC game is achieved by a strategy that combines quantum teleportation, superdense coding and the IC-2 game, a task with classical inputs, in which the IC-2 game is played optimally. An optimal strategy in the IC-2 game remains as an interesting open problem.

The principles of information causality and quantum information causality can be generalized even further by considering that the inputs by Alice, the outputs by Bob, and the transmitted systems are arbitrary information systems, described by more general probabilistic theories, that generalize the concept of a quantum state. An example of such a more general principle has been considered in [120].

Appendix A

Details of Numerical Work

In this appendix, we present some details of the numerical work corresponding to section 2.4. We present the expressions for the correlations $C_x(\theta)$ corresponding to the colourings $x = 2, 3, 4, 2_\Delta, 3_\delta$ shown in Figure 2.4 and defined in (2.17). We computed these correlations numerically using a computer program coded in Mathematica. This code is given and described in Appendix B. The results are plotted in Figures 2.5, 2.6 and 2.7. We also show Equation (2.18).

We use the azimuthal symmetry of the colourings $x = 2, 3, 4, 2_\Delta, 3_\delta$ defined in (2.17), the antipodal property (2.7) and the constraint (2.14) to reduce the correlation given by (2.8) to:

$$C_x(\theta) = -\frac{1}{\pi}\int_0^{\frac{\pi}{2}} d\epsilon \sin\epsilon a_x(\epsilon) \int_0^{\pi} d\omega a_x[\alpha(\theta,\epsilon,\omega)], \tag{A.1}$$

where $\alpha(\theta,\epsilon,\omega)$ is given by (2.10). The integrals with respect to ω are computed analytically in the previous expression. We define the function

$$\chi(\theta,a,b,\alpha) \equiv \frac{2}{\pi}\int_a^b d\epsilon \sin\epsilon \arccos\Big(\frac{\cos\theta\cos\epsilon - \cos\alpha}{\sin\theta\sin\epsilon}\Big), \tag{A.2}$$

where $a, b, \alpha \in [0,\pi]$ and $\theta \in \left[0, \frac{\pi}{2}\right]$. The obtained expressions for the correlations $C_x(\theta)$ include terms of the form (A.2). These expressions are:

$$
\begin{aligned}
C_2(\theta) \quad &= \begin{cases} h_2^1(\theta) & \text{if } \theta \in [0, \pi/4], \\ h_2^2(\theta) & \text{if } \theta \in (\pi/4, \pi/2], \end{cases} \\
C_3(\theta) \quad &= \begin{cases} h_3^1(\theta) & \text{if } \theta \in [0, \pi/6], \\ h_3^2(\theta) & \text{if } \theta \in (\pi/6, \pi/4], \\ h_3^3(\theta) & \text{if } \theta \in (\pi/4, \pi/3], \\ h_3^4(\theta) & \text{if } \theta \in (\pi/3, \pi/2], \end{cases} \\
C_4(\theta) \quad &= \begin{cases} h_4^1(\theta) & \text{if } \theta \in [0, \pi/8], \\ h_4^2(\theta) & \text{if } \theta \in (\pi/8, \pi/4], \\ h_4^3(\theta) & \text{if } \theta \in (\pi/4, 3\pi/8], \\ h_4^4(\theta) & \text{if } \theta \in (3\pi/8, \pi/2], \end{cases} \\
C_{2_\Delta}(\theta) \quad &= \begin{cases} R_\Delta^1(\theta) & \text{if } \theta \in \left[\frac{\pi}{4} + \Delta, \frac{\pi}{2} - 2\Delta\right], \\ R_\Delta^2(\theta) & \text{if } \theta \in \left[\frac{\pi}{2} - 2\Delta, \frac{\pi}{2}\right], \end{cases} \\
C_{3_\delta}(\theta) \quad &= \begin{cases} r_\delta^1(\theta) & \text{if } \delta \in \left[-\frac{\pi}{18}, 0\right] \text{ and } \theta \in \left[\frac{\pi}{3}, \frac{\pi}{3} - \delta\right], \\ r_\delta^2(\theta) & \text{if } \delta \in \left[-\frac{\pi}{18}, 0\right] \text{ and } \theta \in \left(\frac{\pi}{3} - \delta, \frac{\pi}{2} + \delta\right], \\ r_\delta^3(\theta) & \text{if } \delta \in \left[-\frac{\pi}{18}, 0\right] \text{ and } \theta \in \left(\frac{\pi}{2} + \delta, \frac{\pi}{2}\right], \\ r_\delta^4(\theta) & \text{if } \delta \in \left(0, \frac{\pi}{24}\right] \text{ and } \theta \in \left[\frac{\pi}{3}, \frac{\pi}{3} + 2\delta\right], \\ r_\delta^2(\theta) & \text{if } \delta \in \left(0, \frac{\pi}{24}\right] \text{ and } \theta \in \left(\frac{\pi}{3} + 2\delta, \frac{\pi}{2} - \delta\right], \\ r_\delta^5(\theta) & \text{if } \delta \in \left(0, \frac{\pi}{24}\right] \text{ and } \theta \in \left(\frac{\pi}{2} - \delta, \frac{\pi}{2}\right], \end{cases}
\end{aligned}
\tag{A.3}
$$

for $\Delta \in \left[0, \frac{\pi}{12}\right]$, and where

$$
\begin{aligned}
h_2^1(\theta) \equiv\ & -1 + 2\left[\cos\left(\frac{\pi}{4}\right) - \cos\left(\frac{\pi}{4} + \theta\right)\right] + \chi\left(\theta, \frac{\pi}{4} - \theta, \frac{\pi}{4}, \frac{\pi}{4}\right) - \chi\left(\theta, \frac{\pi}{4}, \frac{\pi}{4} + \theta, \frac{\pi}{4}\right) \\
& + \chi\left(\theta, \frac{\pi}{2} - \theta, \frac{\pi}{2}, \frac{\pi}{2}\right), \\
h_2^2(\theta) \equiv\ & 1 + 2\left[\cos\left(\frac{\pi}{4}\right) - \cos\left(\theta - \frac{\pi}{4}\right)\right] + \chi\left(\theta, \theta - \frac{\pi}{4}, \frac{\pi}{4}, \frac{\pi}{4}\right) - \chi\left(\theta, \frac{\pi}{2} - \theta, \frac{\pi}{4}, \frac{\pi}{2}\right) \\
& + \chi\left(\theta, \frac{\pi}{4}, \frac{\pi}{2}, \frac{\pi}{2}\right) - \chi\left(\theta, \frac{\pi}{4}, \frac{\pi}{2}, \frac{\pi}{4}\right) - \chi\left(\theta, \frac{3\pi}{4} - \theta, \frac{\pi}{2}, \frac{3\pi}{4}\right);
\end{aligned}
$$

$$
\begin{aligned}
h_3^1(\theta) \equiv\ & -1+2\Big[\cos\Big(\frac{\pi}{6}\Big)-\cos\Big(\frac{\pi}{6}+\theta\Big)+\cos\Big(\frac{\pi}{3}\Big)-\cos\Big(\frac{\pi}{3}+\theta\Big)\Big]+\chi\Big(\theta,\frac{\pi}{6}-\theta,\frac{\pi}{6},\frac{\pi}{6}\Big)\\
& -\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{6}+\theta,\frac{\pi}{6}\Big)+\chi\Big(\theta,\frac{\pi}{3}-\theta,\frac{\pi}{3},\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{3}+\theta,\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{2},\frac{\pi}{2}\Big),\\
h_3^2(\theta) \equiv\ & 1+2\Big[\cos\Big(\frac{\pi}{6}\Big)-\cos\Big(\theta-\frac{\pi}{6}\Big)+\cos\Big(\frac{\pi}{6}+\theta\Big)-\cos\Big(\frac{\pi}{3}\Big)\Big]+\chi\Big(\theta,\theta-\frac{\pi}{6},\frac{\pi}{6},\frac{\pi}{6}\Big)\\
& -\chi\Big(\theta,\frac{\pi}{3}-\theta,\frac{\pi}{6},\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{2}-\theta,\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{6}\Big)+\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{3},\frac{\pi}{3}\Big)\\
& -\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{3},\frac{\pi}{2}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{6}+\theta,\frac{\pi}{6}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)\\
& -\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{2},\frac{2\pi}{3}\Big),\\
h_3^3(\theta) \equiv\ & 1+2\Big[\cos\Big(\frac{\pi}{6}\Big)-\cos\Big(\theta-\frac{\pi}{6}\Big)+\cos\Big(\frac{\pi}{6}+\theta\Big)-\cos\Big(\frac{\pi}{3}\Big)\Big]-\chi\Big(\theta,\frac{\pi}{3}-\theta,\frac{\pi}{6},\frac{\pi}{3}\Big)\\
& +\chi\Big(\theta,\theta-\frac{\pi}{6},\frac{\pi}{6},\frac{\pi}{6}\Big)+\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{6}\Big)-\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{3},\frac{\pi}{2}\Big)\\
& +\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{6}+\theta,\frac{\pi}{6}\Big)-\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{2},\frac{2\pi}{3}\Big),\\
h_3^4(\theta) \equiv\ & -1+2\Big[\cos\Big(\theta-\frac{\pi}{3}\Big)-\cos\Big(\frac{\pi}{6}\Big)+\cos\Big(\theta-\frac{\pi}{6}\Big)-\cos\Big(\frac{\pi}{3}\Big)\Big]-\chi\Big(\theta,\theta-\frac{\pi}{3},\frac{\pi}{6},\frac{\pi}{3}\Big)\\
& +\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{6},\frac{\pi}{2}\Big)+\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{2}\Big)-\chi\Big(\theta,\theta-\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{6}\Big)\\
& +\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{3},\frac{2\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)\\
& +\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{6}\Big)+\chi\Big(\theta,\frac{5\pi}{6}-\theta,\frac{\pi}{2},\frac{5\pi}{6}\Big);
\end{aligned}
$$

$$
\begin{aligned}
h_4^1(\theta) \equiv & -1+2\left[\cos\left(\frac{\pi}{8}\right)-\cos\left(\frac{\pi}{8}+\theta\right)+\cos\left(\frac{\pi}{4}\right)-\cos\left(\frac{\pi}{4}+\theta\right)+\cos\left(\frac{3\pi}{8}\right)-\cos\left(\frac{3\pi}{8}+\theta\right)\right] \\
& +\chi\left(\theta,\frac{\pi}{8}-\theta,\frac{\pi}{8},\frac{\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{8}+\theta,\frac{\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{4}-\theta,\frac{\pi}{4},\frac{\pi}{4}\right)-\chi\left(\theta,\frac{\pi}{4},\frac{\pi}{4}+\theta,\frac{\pi}{4}\right) \\
& +\chi\left(\theta,\frac{3\pi}{8}-\theta,\frac{3\pi}{8},\frac{3\pi}{8}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{3\pi}{8}+\theta,\frac{3\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{2},\frac{\pi}{2}\right), \\
h_4^2(\theta) \equiv & \ 1+2\left[\cos\left(\frac{\pi}{8}\right)-\cos\left(\theta-\frac{\pi}{8}\right)+\cos\left(\theta+\frac{\pi}{8}\right)-\cos\left(\frac{\pi}{4}\right)+\cos\left(\theta+\frac{\pi}{4}\right)-\cos\left(\frac{3\pi}{8}\right)\right] \\
& +\chi\left(\theta,\theta-\frac{\pi}{8},\frac{\pi}{8},\frac{\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{4}-\theta,\frac{\pi}{8},\frac{\pi}{4}\right)+\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{4},\frac{\pi}{4}\right)-\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{4},\frac{\pi}{8}\right) \\
& -\chi\left(\theta,\frac{3\pi}{8}-\theta,\frac{\pi}{4},\frac{3\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{4},\frac{\pi}{8}+\theta,\frac{\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{3\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{\pi}{4}\right) \\
& -\chi\left(\theta,\frac{\pi}{2}-\theta,\frac{3\pi}{8},\frac{\pi}{2}\right)+\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{4}+\theta,\frac{\pi}{4}\right)+\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{\pi}{2}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{3\pi}{8}\right) \\
& -\chi\left(\theta,\frac{5\pi}{8}-\theta,\frac{\pi}{2},\frac{5\pi}{8}\right), \\
h_4^3(\theta) \equiv & -1+2\left[\cos\left(\theta-\frac{\pi}{4}\right)-\cos\left(\frac{\pi}{8}\right)+\cos\left(\theta-\frac{\pi}{8}\right)-\cos\left(\frac{\pi}{4}\right)+\cos\left(\frac{3\pi}{8}\right)-\cos\left(\theta+\frac{\pi}{8}\right)\right] \\
& -\chi\left(\theta,\theta-\frac{\pi}{4},\frac{\pi}{8},\frac{\pi}{4}\right)+\chi\left(\theta,\frac{3\pi}{8}-\theta,\frac{\pi}{8},\frac{3\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{4},\frac{3\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{4},\frac{\pi}{4}\right) \\
& -\chi\left(\theta,\theta-\frac{\pi}{8},\frac{\pi}{4},\frac{\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{4},\frac{\pi}{2}\right)-\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{\pi}{2}\right)+\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{3\pi}{8}\right) \\
& -\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{\pi}{4}\right)+\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{\pi}{8}\right)+\chi\left(\theta,\frac{5\pi}{8}-\theta,\frac{3\pi}{8},\frac{5\pi}{8}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{5\pi}{8}\right) \\
& +\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{\pi}{2}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{3\pi}{8}\right)+\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{\pi}{4}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{8}+\theta,\frac{\pi}{8}\right) \\
& +\chi\left(\theta,\frac{3\pi}{4}-\theta,\frac{\pi}{2},\frac{3\pi}{4}\right), \\
h_4^4(\theta) \equiv & \ 1+2\left[\cos\left(\frac{\pi}{8}\right)-\cos\left(\theta-\frac{3\pi}{8}\right)+\cos\left(\frac{\pi}{4}\right)-\cos\left(\theta-\frac{\pi}{4}\right)+\cos\left(\frac{3\pi}{8}\right)-\cos\left(\theta-\frac{\pi}{8}\right)\right] \\
& +\chi\left(\theta,\theta-\frac{3\pi}{8},\frac{\pi}{8},\frac{3\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{8},\frac{\pi}{2}\right)+\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{4},\frac{\pi}{2}\right)-\chi\left(\theta,\frac{\pi}{8},\frac{\pi}{4},\frac{3\pi}{8}\right) \\
& +\chi\left(\theta,\theta-\frac{\pi}{4},\frac{\pi}{4},\frac{\pi}{4}\right)-\chi\left(\theta,\frac{5\pi}{8}-\theta,\frac{\pi}{4},\frac{5\pi}{8}\right)+\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{5\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{\pi}{2}\right) \\
& +\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{3\pi}{8}\right)-\chi\left(\theta,\frac{\pi}{4},\frac{3\pi}{8},\frac{\pi}{4}\right)+\chi\left(\theta,\theta-\frac{\pi}{8},\frac{3\pi}{8},\frac{\pi}{8}\right)-\chi\left(\theta,\frac{3\pi}{4}-\theta,\frac{3\pi}{8},\frac{3\pi}{4}\right) \\
& +\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{3\pi}{4}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{5\pi}{8}\right)+\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{\pi}{2}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{3\pi}{8}\right) \\
& +\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{\pi}{4}\right)-\chi\left(\theta,\frac{3\pi}{8},\frac{\pi}{2},\frac{\pi}{8}\right)-\chi\left(\theta,\frac{7\pi}{8}-\theta,\frac{\pi}{2},\frac{7\pi}{8}\right);
\end{aligned}
$$

$$
\begin{aligned}
R^1_\Delta(\theta) \equiv 1 + 2\Big[&-\cos\Big(-\frac{\pi}{4}+\Delta+\theta\Big)+\cos\Big(\frac{\pi}{4}-\Delta\Big)\Big]+\chi\Big(\theta,-\frac{\pi}{4}+\Delta+\theta,\frac{\pi}{4}-\Delta,\frac{\pi}{4}-\Delta\Big)\\
&-\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{4}-\Delta,\frac{\pi}{2}\Big)+\chi\Big(\theta,\frac{\pi}{4}-\Delta,\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{4}-\Delta,\frac{\pi}{2},\frac{\pi}{4}-\Delta\Big)\\
&-\chi\Big(\theta,\frac{3\pi}{4}+\Delta-\theta,\frac{\pi}{2},\frac{3\pi}{4}+\Delta\Big),\\
R^2_\Delta(\theta) \equiv 1 + 2\Big[&-\cos\Big(\frac{\pi}{4}-\Delta\Big)+\cos\Big(\theta-\frac{\pi}{4}+\Delta\Big)\Big]-\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{4}-\Delta,\frac{\pi}{2}\Big)\\
&+\chi\Big(\theta,\frac{\pi}{4}-\Delta,\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\theta-\frac{\pi}{4}+\Delta,\frac{\pi}{2},\frac{\pi}{4}-\Delta\Big)-\chi\Big(\theta,\frac{3\pi}{4}+\Delta-\theta,\frac{\pi}{2},\frac{3\pi}{4}+\Delta\Big);
\end{aligned}
$$

$$
\begin{aligned}
r^1_\delta(\theta) \equiv -1 + 2\Big[&\cos\Big(\theta-\frac{\pi}{3}\Big)-\cos\Big(\frac{\pi}{6}+\delta\Big)+\cos\Big(\theta-\frac{\pi}{6}-\delta\Big)-\cos\Big(\frac{\pi}{3}\Big)+\cos\Big(\theta+\frac{\pi}{6}+\delta\Big)\Big]\\
&-\chi\Big(\theta,\theta-\frac{\pi}{3},\frac{\pi}{6}+\delta,\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{3},\frac{\pi}{2}\Big)\\
&-\chi\Big(\theta,\theta-\frac{\pi}{6}-\delta,\frac{\pi}{3},\frac{\pi}{6}+\delta\Big)+\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{3},\frac{2\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)\\
&+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\theta+\frac{\pi}{6}+\delta,\frac{\pi}{6}+\delta\Big),\\
r^2_\delta(\theta) \equiv -1 + 2\Big[&\cos\Big(\theta-\frac{\pi}{3}\Big)-\cos\Big(\frac{\pi}{6}+\delta\Big)+\cos\Big(\theta-\frac{\pi}{6}-\delta\Big)-\cos\Big(\frac{\pi}{3}\Big)\Big]\\
&-\chi\Big(\theta,\theta-\frac{\pi}{3},\frac{\pi}{6}+\delta,\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{6}+\delta,\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{2}\Big)\\
&+\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{3}\Big)-\chi\Big(\theta,\theta-\frac{\pi}{6}-\delta,\frac{\pi}{3},\frac{\pi}{6}+\delta\Big)+\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{3},\frac{2\pi}{3}\Big)\\
&-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{6}+\delta\Big)\\
&+\chi\Big(\theta,\frac{5\pi}{6}-\delta-\theta,\frac{\pi}{2},\frac{5\pi}{6}-\delta\Big),\\
r^3_\delta(\theta) \equiv -1 + 2\Big[&\cos\Big(\frac{\pi}{6}+\delta\Big)-\cos\Big(\theta-\frac{\pi}{3}\Big)+\cos\Big(\frac{\pi}{3}\Big)-\cos\Big(\theta-\frac{\pi}{6}-\delta\Big)\Big]\\
&+\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{6}+\delta,\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{2}\Big)+\chi\Big(\theta,\theta-\frac{\pi}{3},\frac{\pi}{3},\frac{\pi}{3}\Big)\\
&+\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{3},\frac{2\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)\\
&+\chi\Big(\theta,\theta-\frac{\pi}{6}-\delta,\frac{\pi}{2},\frac{\pi}{6}+\delta\Big)+\chi\Big(\theta,\frac{5\pi}{6}-\delta-\theta,\frac{\pi}{2},\frac{5\pi}{6}-\delta\Big),
\end{aligned}
$$

$$
\begin{aligned}
r_\delta^4(\theta) \equiv -1 + 2\Big[&\cos\Big(\theta-\frac{\pi}{3}\Big)-\cos\Big(\theta-\frac{\pi}{6}-\delta\Big)+\cos\Big(\frac{\pi}{6}+\delta\Big)-\cos\Big(\frac{\pi}{3}\Big)\Big]\\
&-\chi\Big(\theta,\theta-\frac{\pi}{3},\frac{\pi}{6}+\delta,\frac{\pi}{3}\Big)+\chi\Big(\theta,\theta-\frac{\pi}{6}-\delta,\frac{\pi}{6}+\delta,\frac{\pi}{6}+\delta\Big)+\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{6}+\delta,\frac{\pi}{2}\Big)\\
&-\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{2}\Big)+\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{6}+\delta\Big)\\
&+\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{3},\frac{2\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)\\
&+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{6}+\delta\Big)+\chi\Big(\theta,\frac{5\pi}{6}-\delta-\theta,\frac{\pi}{2},\frac{5\pi}{6}-\delta\Big),\\
r_\delta^5(\theta) \equiv -1 + 2\Big[&\cos\Big(\theta-\frac{\pi}{3}\Big)-\cos\Big(\frac{\pi}{6}+\delta\Big)+\cos\Big(\theta-\frac{\pi}{6}-\delta\Big)-\cos\Big(\frac{\pi}{3}\Big)\Big]\\
&+\chi\Big(\theta,\frac{\pi}{2}-\theta,\frac{\pi}{6}+\delta,\frac{\pi}{2}\Big)-\chi\Big(\theta,\theta-\frac{\pi}{3},\frac{\pi}{6}+\delta,\frac{\pi}{3}\Big)-\chi\Big(\theta,\frac{2\pi}{3}-\theta,\frac{\pi}{6}+\delta,\frac{2\pi}{3}\Big)\\
&+\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{2\pi}{3}\Big)-\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{2}\Big)+\chi\Big(\theta,\frac{\pi}{6}+\delta,\frac{\pi}{3},\frac{\pi}{3}\Big)\\
&-\chi\Big(\theta,\theta-\frac{\pi}{6}-\delta,\frac{\pi}{3},\frac{\pi}{6}+\delta\Big)-\chi\Big(\theta,\frac{5\pi}{6}-\delta-\theta,\frac{\pi}{3},\frac{5\pi}{6}-\delta\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{5\pi}{6}-\delta\Big)\\
&-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)-\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)+\chi\Big(\theta,\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{6}+\delta\Big).
\end{aligned}
$$

Now we show (2.18):

$$C_3\Big(\frac{\pi}{2}-\tau\Big) = -1.5\tau + \mathcal{O}(\tau^2). \tag{A.4}$$

Let $0 \le \tau \ll 1$. We expand $C_3\big(\frac{\pi}{2}-\tau\big)$ in its Taylor series to obtain

$$C_3\Big(\frac{\pi}{2}-\tau\Big) = C_3\Big(\frac{\pi}{2}\Big) + \tau\Big[\frac{d}{d\tau}C_3\Big(\frac{\pi}{2}-\tau\Big)\Big]_{\tau=0} + \mathcal{O}(\tau^2). \tag{A.5}$$

As shown in section 2.2, the correlation satisfies $C_x(\frac{\pi}{2}) = 0$ for every colouring $x \in \mathcal{X}$. Thus, we have that $C_3\big(\frac{\pi}{2}\big) = 0$. From (A.3), we have that $C_3\big(\frac{\pi}{2}-\tau\big) = h_3^4\big(\frac{\pi}{2}-\tau\big)$ for $0 \le \tau \ll 1$. Thus, we only need to show that

$$\Big[\frac{d}{d\theta}h_3^4(\theta)\Big]_{\theta=\pi/2} = 1.5. \tag{A.6}$$

The function $h_3^4(\theta)$ has terms of the form

$$\chi(\theta, a, b, \alpha) \equiv \int_a^b d\epsilon \xi(\theta, \epsilon, \alpha), \tag{A.7}$$

where

$$\xi(\theta, \epsilon, \alpha) \equiv \frac{2}{\pi} \sin\epsilon \arccos\Big(\frac{\cos\theta\cos\epsilon - \cos\alpha}{\sin\theta\sin\epsilon}\Big), \tag{A.8}$$

as defined by (A.2). Differentiating the function χ, we obtain

$$\frac{d}{d\theta}\chi(\theta, a, b, \alpha) = \xi(\theta, b, \alpha)\frac{db}{d\theta} - \xi(\theta, a, \alpha)\frac{da}{d\theta} + \int_a^b d\epsilon \frac{\partial}{\partial\theta}\xi(\theta, \epsilon, \alpha). \tag{A.9}$$

We have that

$$\Big[\frac{\partial}{\partial\theta}\xi(\theta, \epsilon, \alpha)\Big]_{\theta=\pi/2} = \frac{2\cos\epsilon}{\pi\sqrt{1 - \left(\frac{\cos\alpha}{\sin\epsilon}\right)^2}}. \tag{A.10}$$

We obtain that

$$\frac{2}{\pi}\int_a^b \frac{d\epsilon\cos\epsilon}{\sqrt{1 - \left(\frac{\cos\alpha}{\sin\epsilon}\right)^2}} = \mu(a, b, \alpha), \tag{A.11}$$

where

$$\mu(a, b, \alpha) \equiv \frac{2}{\pi}\Big(\sqrt{\sin^2 b - \cos^2\alpha} - \sqrt{\sin^2 a - \cos^2\alpha}\Big), \tag{A.12}$$

for $\cos^2\alpha \leq \sin^2 b$ and $\cos^2\alpha \leq \sin^2 a$. We define

$$\nu(\epsilon, \alpha) \equiv \xi\Big(\frac{\pi}{2}, \epsilon, \alpha\Big). \tag{A.13}$$

From the definition of $h_3^4(\theta)$, given by (A.3), and Equations (A.9) – (A.13), it is

straightforward to obtain that

$$\begin{aligned}\Big[\frac{d}{d\theta}h_3^4(\theta)\Big]_{\theta=\pi/2} \quad &= -2\Big[\sin\Big(\frac{\pi}{6}\Big)+\sin\Big(\frac{\pi}{3}\Big)\Big]+\nu\Big(0,\frac{\pi}{2}\Big)+\nu\Big(\frac{\pi}{6},\frac{\pi}{3}\Big)+\nu\Big(\frac{\pi}{6},\frac{2\pi}{3}\Big)\\ &\quad +\nu\Big(\frac{\pi}{3},\frac{\pi}{6}\Big)+\nu\Big(\frac{\pi}{3},\frac{5\pi}{6}\Big)+\mu\Big(0,\frac{\pi}{6},\frac{\pi}{2}\Big)-\mu\Big(\frac{\pi}{6},\frac{\pi}{6},\frac{\pi}{3}\Big)\\ &\quad +\mu\Big(\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{3}\Big)-\mu\Big(\frac{\pi}{6},\frac{\pi}{3},\frac{\pi}{2}\Big)+\mu\Big(\frac{\pi}{6},\frac{\pi}{3},\frac{2\pi}{3}\Big)\\ &\quad -\mu\Big(\frac{\pi}{3},\frac{\pi}{3},\frac{\pi}{6}\Big)+\mu\Big(\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{2}\Big)+\mu\Big(\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{6}\Big)\\ &\quad -\mu\Big(\frac{\pi}{3},\frac{\pi}{2},\frac{2\pi}{3}\Big)-\mu\Big(\frac{\pi}{3},\frac{\pi}{2},\frac{\pi}{3}\Big)+\mu\Big(\frac{\pi}{3},\frac{\pi}{2},\frac{5\pi}{6}\Big). \qquad \text{(A.14)}\end{aligned}$$

We use (A.8), (A.12) and (A.13), and notice that $\nu\big(0,\frac{\pi}{2}\big)=0$ in order to evaluate the previous expression. We obtain

$$\Big[\frac{d}{d\theta}h_3^4(\theta)\Big]_{\theta=\pi/2}=\frac{1}{\pi}\Big[6-4\big(\sqrt{3}-\sqrt{2}\big)\Big]=1.5, \qquad \text{(A.15)}$$

as claimed.

Appendix B

Code for the Computer Program

In this appendix, we present the code of our Mathematica program used to compute the correlations given by (A.3). The code is given in six parts. Each part is given in a figure of this appendix.

From Figure B.1, we see that the integrals are computed with a *precision* of 6 and an *accuracy* of 7. The code *precision* gives the effective number of digits of precision in the computed values, while the *accuracy* corresponds to the effective number of digits to the right of the decimal point in the computed values. Thus, considering the factor $\frac{2}{\pi}$ in (A.2) and the number of terms of the form (A.2) in the expressions for the correlations (A.3) being of the order of 10, we expect the obtained correlations to have a precision of the order of 10^{-5}, which is good enough for our claims in section 2.4. For example, it is easily observed from the plots in Figure 2.6 that $C_{3_{-0.038\pi}}(\theta) < C_1(\theta)$ for $\theta \in \left[0.386\pi, \frac{\pi}{2}\right)$[1] and that $C_1(\theta) - C_{3_{-0.038\pi}}(\theta)$ achieves values of the order of 10^{-2} in this range. This can also be seen from the numerical values output by the program.

The given code takes a computation time of a few seconds and outputs results with a precision of the order of 10^{-5}. One of the reasons for computing analyti-

[1]The value 0.386π for the upper bound $\theta^{\mathrm{w}}_{\mathrm{max}} \leq 0.386\pi$ was not obtained just from observation of the plots. It was obtained by computing the correlations $C_{3_{-0.038\pi}}(\theta)$ and $C_1(\theta)$ numerically at several values of θ to guarantee the given precision. Similarly, the bound $\theta^{\mathrm{s}}_{\mathrm{max}} \leq 0.345\pi$ was obtained by computing $C_{2_\Delta}(\theta)$ and $-C_1(\theta)$ for several values of θ and Δ to guarantee the given precision.

cally the integrals with respect to ω in (A.1) is that, by doing this, the numerical computations of our program take times of a few seconds, compared to times of hours if the integrals with respect to ω are computed numerically. Furthermore, by computing the integrals with respect to ω analytically, the achieved numerical precision is much higher. In fact, we decided to constrain our numerical computations to colourings with azimuthal symmetry in order to have a high control over the obtained precision. We expect that arbitrary colourings can be investigated numerically with adequate numerical techniques and computer programs.

```
χ[θ_, a_, b_, α_] :=
  (2 / Pi) NIntegrate[Sin[ε] ArcCos[((Cos[θ] Cos[ε]) - Cos[α]) / (Sin[θ] Sin[ε])],
    {ε, a, b}, PrecisionGoal → 6, AccuracyGoal → 7]


h21[θ_] := -1 + 2 (Cos[Pi / 4] - Cos[(Pi / 4) + θ]) + χ[θ, (Pi / 4) - θ, Pi / 4, Pi / 4] -
   χ[θ, Pi / 4, (Pi / 4) + θ, Pi / 4] + χ[θ, (Pi / 2) - θ, Pi / 2, Pi / 2]

h22[θ_] := 1 + 2 (Cos[Pi / 4] - Cos[θ - (Pi / 4)]) + χ[θ, θ - (Pi / 4), Pi / 4, Pi / 4] -
   χ[θ, (Pi / 2) - θ, Pi / 4, Pi / 2] + χ[θ, Pi / 4, Pi / 2, Pi / 2] -
   χ[θ, Pi / 4, Pi / 2, Pi / 4] - χ[θ, (3 Pi / 4) - θ, Pi / 2, 3 Pi / 4]

C2[θ_] := Which[0 ≤ θ ≤ π / 4, h21[θ], π / 4 < θ ≤ π / 2, h22[θ]]
```

Figure B.1: Program code I. This code defines the function given by (A.2) and the correlation function for colouring 2.

```
h31[θ_] := -1 + 2 (Cos[Pi / 6] - Cos[(Pi / 6) + θ] + Cos[Pi / 3] - Cos[(Pi / 3) + θ]) +
  χ[θ, (Pi / 6) - θ, Pi / 6, Pi / 6] - χ[θ, Pi / 6, (Pi / 6) + θ, Pi / 6] + χ[θ, (Pi / 3) - θ,
   Pi / 3, Pi / 3] - χ[θ, Pi / 3, (Pi / 3) + θ, Pi / 3] + χ[θ, (Pi / 2) - θ, Pi / 2, Pi / 2]

h32[θ_] := 1 + 2 (Cos[Pi / 6] - Cos[θ - (Pi / 6)] + Cos[(Pi / 6) + θ] - Cos[Pi / 3]) +
  χ[θ, θ - (Pi / 6), Pi / 6, Pi / 6] - χ[θ, (Pi / 3) - θ, Pi / 6, Pi / 3] +
  χ[θ, Pi / 6, (Pi / 2) - θ, Pi / 3] - χ[θ, Pi / 6, Pi / 3, Pi / 6] + χ[θ, (Pi / 2) - θ, Pi / 3, Pi / 3] -
  χ[θ, (Pi / 2) - θ, Pi / 3, Pi / 2] + χ[θ, Pi / 3, (Pi / 6) + θ, Pi / 6] +
  χ[θ, Pi / 3, Pi / 2, Pi / 2] - χ[θ, Pi / 3, Pi / 2, Pi / 3] - χ[θ, (2 Pi / 3) - θ, Pi / 2, 2 Pi / 3]

h33[θ_] := 1 + 2 (Cos[Pi / 6] - Cos[θ - (Pi / 6)] + Cos[(Pi / 6) + θ] - Cos[Pi / 3]) -
  χ[θ, (Pi / 3) - θ, Pi / 6, Pi / 3] + χ[θ, θ - (Pi / 6), Pi / 6, Pi / 6] +
  χ[θ, Pi / 6, Pi / 3, Pi / 3] - χ[θ, Pi / 6, Pi / 3, Pi / 6] -
  χ[θ, (Pi / 2) - θ, Pi / 3, Pi / 2] + χ[θ, Pi / 3, Pi / 2, Pi / 2] - χ[θ, Pi / 3, Pi / 2, Pi / 3] +
  χ[θ, Pi / 3, (Pi / 6) + θ, Pi / 6] - χ[θ, (2 Pi / 3) - θ, Pi / 2, 2 Pi / 3]

h34[θ_] := -1 + 2 (Cos[θ - (Pi / 3)] - Cos[Pi / 6] + Cos[θ - (Pi / 6)] - Cos[Pi / 3]) -
  χ[θ, θ - (Pi / 3), Pi / 6, Pi / 3] + χ[θ, (Pi / 2) - θ, Pi / 6, Pi / 2] +
  χ[θ, Pi / 6, Pi / 3, Pi / 3] - χ[θ, Pi / 6, Pi / 3, Pi / 2] - χ[θ, θ - (Pi / 6), Pi / 3, Pi / 6] +
  χ[θ, (2 Pi / 3) - θ, Pi / 3, 2 Pi / 3] - χ[θ, Pi / 3, Pi / 2, 2 Pi / 3] + χ[θ, Pi / 3, Pi / 2, Pi / 2] -
  χ[θ, Pi / 3, Pi / 2, Pi / 3] + χ[θ, Pi / 3, Pi / 2, Pi / 6] + χ[θ, (5 Pi / 6) - θ, Pi / 2, 5 Pi / 6]

C3[θ_] := Which[0 ≤ θ ≤ π / 6, h31[θ], π / 6 < θ ≤ π / 4,
  h32[θ], π / 4 < θ ≤ π / 3, h33[θ], π / 3 < θ ≤ π / 2, h34[θ]]
```

Figure B.2: Program code II. This code defines the correlation function for colouring 3.

```
h41[θ_] := -1 + 2 (Cos[Pi / 8] - Cos[(Pi / 8) + θ] + Cos[Pi / 4] - Cos[(Pi / 4) + θ] +
      Cos[3 Pi / 8] - Cos[(3 Pi / 8) + θ]) + χ[θ, (Pi / 8) - θ, Pi / 8, Pi / 8] -
  χ[θ, Pi / 8, (Pi / 8) + θ, Pi / 8] + χ[θ, (Pi / 4) - θ, Pi / 4, Pi / 4] -
  χ[θ, Pi / 4, (Pi / 4) + θ, Pi / 4] + χ[θ, (3 Pi / 8) - θ, 3 Pi / 8, 3 Pi / 8] -
  χ[θ, 3 Pi / 8, (3 Pi / 8) + θ, 3 Pi / 8] + χ[θ, (Pi / 2) - θ, Pi / 2, Pi / 2]

h42[θ_] := 1 + 2 (Cos[Pi / 8] - Cos[θ - (Pi / 8)] +
      Cos[θ + (Pi / 8)] - Cos[Pi / 4] + Cos[θ + (Pi / 4)] - Cos[3 Pi / 8]) +
  χ[θ, θ - (Pi / 8), Pi / 8, Pi / 8] - χ[θ, (Pi / 4) - θ, Pi / 8, Pi / 4] + χ[θ, Pi / 8, Pi / 4, Pi / 4] -
  χ[θ, Pi / 8, Pi / 4, Pi / 8] - χ[θ, (3 Pi / 8) - θ, Pi / 4, 3 Pi / 8] +
  χ[θ, Pi / 4, (Pi / 8) + θ, Pi / 8] + χ[θ, Pi / 4, 3 Pi / 8, 3 Pi / 8] -
  χ[θ, Pi / 4, 3 Pi / 8, Pi / 4] - χ[θ, (Pi / 2) - θ, 3 Pi / 8, Pi / 2] +
  χ[θ, 3 Pi / 8, (Pi / 4) + θ, Pi / 4] + χ[θ, 3 Pi / 8, Pi / 2, Pi / 2] -
  χ[θ, 3 Pi / 8, Pi / 2, 3 Pi / 8] - χ[θ, (5 Pi / 8) - θ, Pi / 2, 5 Pi / 8]

h43[θ_] := -1 + 2 (Cos[θ - (Pi / 4)] - Cos[Pi / 8] +
      Cos[θ - (Pi / 8)] - Cos[Pi / 4] + Cos[3 Pi / 8] - Cos[θ + (Pi / 8)]) -
  χ[θ, θ - (Pi / 4), Pi / 8, Pi / 4] + χ[θ, (3 Pi / 8) - θ, Pi / 8, 3 Pi / 8] -
  χ[θ, Pi / 8, Pi / 4, 3 Pi / 8] + χ[θ, Pi / 8, Pi / 4, Pi / 4] - χ[θ, θ - (Pi / 8), Pi / 4, Pi / 8] +
  χ[θ, (Pi / 2) - θ, Pi / 4, Pi / 2] - χ[θ, Pi / 4, 3 Pi / 8, Pi / 2] +
  χ[θ, Pi / 4, 3 Pi / 8, 3 Pi / 8] - χ[θ, Pi / 4, 3 Pi / 8, Pi / 4] + χ[θ, Pi / 4, 3 Pi / 8, Pi / 8] +
  χ[θ, (5 Pi / 8) - θ, 3 Pi / 8, 5 Pi / 8] - χ[θ, 3 Pi / 8, Pi / 2, 5 Pi / 8] +
  χ[θ, 3 Pi / 8, Pi / 2, Pi / 2] - χ[θ, 3 Pi / 8, Pi / 2, 3 Pi / 8] + χ[θ, 3 Pi / 8, Pi / 2, Pi / 4] -
  χ[θ, 3 Pi / 8, (Pi / 8) + θ, Pi / 8] + χ[θ, (3 Pi / 4) - θ, Pi / 2, 3 Pi / 4]

h44[θ_] := 1 + 2 (Cos[Pi / 8] - Cos[θ - (3 Pi / 8)] +
      Cos[Pi / 4] - Cos[θ - (Pi / 4)] + Cos[3 Pi / 8] - Cos[θ - (Pi / 8)]) +
  χ[θ, θ - (3 Pi / 8), Pi / 8, 3 Pi / 8] - χ[θ, (Pi / 2) - θ, Pi / 8, Pi / 2] +
  χ[θ, Pi / 8, Pi / 4, Pi / 2] - χ[θ, Pi / 8, Pi / 4, 3 Pi / 8] + χ[θ, θ - (Pi / 4), Pi / 4, Pi / 4] -
  χ[θ, (5 Pi / 8) - θ, Pi / 4, 5 Pi / 8] + χ[θ, Pi / 4, 3 Pi / 8, 5 Pi / 8] -
  χ[θ, Pi / 4, 3 Pi / 8, Pi / 2] + χ[θ, Pi / 4, 3 Pi / 8, 3 Pi / 8] - χ[θ, Pi / 4, 3 Pi / 8, Pi / 4] +
  χ[θ, θ - (Pi / 8), 3 Pi / 8, Pi / 8] - χ[θ, (3 Pi / 4) - θ, 3 Pi / 8, 3 Pi / 4] +
  χ[θ, 3 Pi / 8, Pi / 2, 3 Pi / 4] - χ[θ, 3 Pi / 8, Pi / 2, 5 Pi / 8] +
  χ[θ, 3 Pi / 8, Pi / 2, Pi / 2] - χ[θ, 3 Pi / 8, Pi / 2, 3 Pi / 8] + χ[θ, 3 Pi / 8, Pi / 2, Pi / 4] -
  χ[θ, 3 Pi / 8, Pi / 2, Pi / 8] - χ[θ, (7 Pi / 8) - θ, Pi / 2, 7 Pi / 8]

C4[θ_] := Which[0 ≤ θ ≤ π / 8, h41[θ], π / 8 < θ ≤ π / 4,
  h42[θ], π / 4 < θ ≤ 3 π / 8, h43[θ], 3 π / 8 < θ ≤ π / 2, h44[θ]]
```

Figure B.3: Program code III. This code defines the correlation function for colouring 4.

```
R1[θ_, Δ_] := 1 + 2 (-Cos[- (Pi / 4) + Δ + θ] + Cos[(Pi / 4) - Δ]) +
   χ[θ, - (Pi / 4) + Δ + θ, (Pi / 4) - Δ, (Pi / 4) - Δ] -
   χ[θ, (Pi / 2) - θ, (Pi / 4) - Δ, Pi / 2] + χ[θ, (Pi / 4) - Δ, Pi / 2, Pi / 2] -
   χ[θ, (Pi / 4) - Δ, Pi / 2, (Pi / 4) - Δ] - χ[θ, (3 Pi / 4) + Δ - θ, Pi / 2, (3 Pi / 4) + Δ]

R2[θ_, Δ_] := 1 + 2 (-Cos[(Pi / 4) - Δ] + Cos[θ - (Pi / 4) + Δ]) -
   χ[θ, (Pi / 2) - θ, (Pi / 4) - Δ, Pi / 2] + χ[θ, (Pi / 4) - Δ, Pi / 2, Pi / 2] -
   χ[θ, θ - (Pi / 4) + Δ, Pi / 2, (Pi / 4) - Δ] - χ[θ, (3 Pi / 4) + Δ - θ, Pi / 2, (3 Pi / 4) + Δ]

C2Δ[θ_, Δ_] :=
 Which[(π / 4) + Δ <= θ ≤ (π / 2) - (2 Δ), R1[θ, Δ], (π / 2) - (2 Δ) < θ ≤ π / 2, R2[θ, Δ]]
```

Figure B.4: Program code IV. This code defines the correlation function for colouring 2_Δ.

```
r1[θ_, δ_] := -1 + 2
    (Cos[θ - (Pi / 3)] - Cos[(Pi / 6) + δ] + Cos[θ - (Pi / 6) - δ] - Cos[Pi / 3] + Cos[θ + (Pi / 6) + δ]) -
  χ[θ, θ - (Pi / 3), (Pi / 6) + δ, Pi / 3] + χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 3] -
  χ[θ, (Pi / 2) - θ, Pi / 3, Pi / 2] - χ[θ, θ - (Pi / 6) - δ, Pi / 3, (Pi / 6) + δ] +
  χ[θ, (2 Pi / 3) - θ, Pi / 3, 2 Pi / 3] - χ[θ, Pi / 3, Pi / 2, 2 Pi / 3] + χ[θ, Pi / 3, Pi / 2, Pi / 2] -
  χ[θ, Pi / 3, Pi / 2, Pi / 3] + χ[θ, Pi / 3, θ + (Pi / 6) + δ, (Pi / 6) + δ]

r2[θ_, δ_] := -1 + 2 (Cos[θ - (Pi / 3)] - Cos[(Pi / 6) + δ] + Cos[θ - (Pi / 6) - δ] - Cos[Pi / 3]) -
  χ[θ, θ - (Pi / 3), (Pi / 6) + δ, Pi / 3] + χ[θ, (Pi / 2) - θ, (Pi / 6) + δ, Pi / 2] -
  χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 2] + χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 3] -
  χ[θ, θ - (Pi / 6) - δ, Pi / 3, (Pi / 6) + δ] + χ[θ, (2 Pi / 3) - θ, Pi / 3, 2 Pi / 3] -
  χ[θ, Pi / 3, Pi / 2, 2 Pi / 3] + χ[θ, Pi / 3, Pi / 2, Pi / 2] - χ[θ, Pi / 3, Pi / 2, Pi / 3] +
  χ[θ, Pi / 3, Pi / 2, (Pi / 6) + δ] + χ[θ, (5 Pi / 6) - δ - θ, Pi / 2, (5 Pi / 6) - δ]

r3[θ_, δ_] := -1 + 2 (Cos[(Pi / 6) + δ] - Cos[θ - (Pi / 3)] + Cos[Pi / 3] - Cos[θ - (Pi / 6) - δ]) +
  χ[θ, (Pi / 2) - θ, (Pi / 6) + δ, Pi / 2] - χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 2] +
  χ[θ, θ - (Pi / 3), Pi / 3, Pi / 3] + χ[θ, (2 Pi / 3) - θ, Pi / 3, 2 Pi / 3] -
  χ[θ, Pi / 3, Pi / 2, 2 Pi / 3] + χ[θ, Pi / 3, Pi / 2, Pi / 2] - χ[θ, Pi / 3, Pi / 2, Pi / 3] +
  χ[θ, θ - (Pi / 6) - δ, Pi / 2, (Pi / 6) + δ] + χ[θ, (5 Pi / 6) - δ - θ, Pi / 2, (5 Pi / 6) - δ]

r4[θ_, δ_] := -1 + 2 (Cos[θ - (Pi / 3)] - Cos[θ - (Pi / 6) - δ] + Cos[(Pi / 6) + δ] - Cos[Pi / 3]) -
  χ[θ, θ - (Pi / 3), (Pi / 6) + δ, Pi / 3] + χ[θ, θ - (Pi / 6) - δ, (Pi / 6) + δ, (Pi / 6) + δ] +
  χ[θ, (Pi / 2) - θ, (Pi / 6) + δ, Pi / 2] - χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 2] +
  χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 3] - χ[θ, (Pi / 6) + δ, Pi / 3, (Pi / 6) + δ] +
  χ[θ, (2 Pi / 3) - θ, Pi / 3, 2 Pi / 3] - χ[θ, Pi / 3, Pi / 2, 2 Pi / 3] +
  χ[θ, Pi / 3, Pi / 2, Pi / 2] - χ[θ, Pi / 3, Pi / 2, Pi / 3] +
  χ[θ, Pi / 3, Pi / 2, (Pi / 6) + δ] + χ[θ, (5 Pi / 6) - δ - θ, Pi / 2, (5 Pi / 6) - δ]

r5[θ_, δ_] := -1 + 2 (Cos[θ - (Pi / 3)] - Cos[(Pi / 6) + δ] + Cos[θ - (Pi / 6) - δ] - Cos[Pi / 3]) +
  χ[θ, (Pi / 2) - θ, (Pi / 6) + δ, Pi / 2] - χ[θ, θ - (Pi / 3), (Pi / 6) + δ, Pi / 3] -
  χ[θ, (2 Pi / 3) - θ, (Pi / 6) + δ, 2 Pi / 3] + χ[θ, (Pi / 6) + δ, Pi / 3, 2 Pi / 3] -
  χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 2] + χ[θ, (Pi / 6) + δ, Pi / 3, Pi / 3] -
  χ[θ, θ - (Pi / 6) - δ, Pi / 3, (Pi / 6) + δ] - χ[θ, (5 Pi / 6) - δ - θ, Pi / 3, (5 Pi / 6) - δ] +
  χ[θ, Pi / 3, Pi / 2, (5 Pi / 6) - δ] - χ[θ, Pi / 3, Pi / 2, 2 Pi / 3] +
  χ[θ, Pi / 3, Pi / 2, Pi / 2] - χ[θ, Pi / 3, Pi / 2, Pi / 3] + χ[θ, Pi / 3, Pi / 2, (Pi / 6) + δ]

C3δ[θ_, δ_] := Which[-Pi / 18 ≤ δ ≤ 0 && Pi / 3 ≤ θ <= (Pi / 3) - δ,
  r1[θ, δ], -Pi / 18 <= δ ≤ 0 && (Pi / 3) - δ < θ <= (Pi / 2) + δ,
  r2[θ, δ], -Pi / 18 ≤ δ ≤ 0 && (Pi / 2) + δ < θ <= (Pi / 2),
```

[redacted]

Figure B.5: Program code V. This code defines the correlation function for colouring 3_δ.

```
Column[Table[C2[k (Pi)], {k, 0, 0.5, 0.005}]]
Column[Table[C3[k (Pi)], {k, 0, 0.5, 0.005}]]
Column[Table[C4[k (Pi)], {k, 0, 0.5, 0.005}]]

Column[Table[C3δ[k (Pi), -0.046 (Pi)], {k, 1 / 3, 1 / 2, 1 / 600}]]
Column[Table[C3δ[k (Pi), -0.038 (Pi)], {k, 1 / 3, 1 / 2, 1 / 600}]]
Column[Table[C3[k (Pi)], {k, 1 / 3, 1 / 2, 1 / 600}]]

Column[Table[C2Δ[k (Pi), 0.035 (Pi)], {k, 0.3, 0.5, 0.002}]]
Column[Table[C2[k (Pi)], {k, 0.3, 0.5, 0.002}]]
```

Figure B.6: Program code VI. This code computes the correlations. The first three lines output the correlations plotted in Figure 2.5. The next three lines output the correlations plotted in Figure 2.6. The last two lines output the correlations plotted in Figure 2.7.

Appendix C

Details of the Primed PBT Protocol

We provide specific details of the *primed* PBT protocol described in section 3.5, which achieves success probability q_j and satisfies Equation (3.8) for the corresponding primed states,

$$\eta'_j = \gamma'_{j,i} = \frac{I}{2^n}. \tag{C.1}$$

We use the following identity satisfied for any quantum state ρ of dimension 2^n:

$$\frac{I}{2^n} \equiv \frac{1}{4^n} \sum_{l=1}^{4^n} V_l \rho V_l^\dagger; \tag{C.2}$$

where we define the set of unitary operations $\{V_l\}_{l=1}^{4^n} \equiv \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}^{\otimes n}$, σ_0 is the identity acting on $\mathbb{C}^2$, and $\{\sigma_i\}_{i=1}^3$ are the Pauli matrices.

The following, *primed*, PBT protocol achieves success probability q_j and satisfies (C.1).

Firstly, consider the stage previous to the implementation of PBT in which the resource state is prepared and distributed to Alice and Bob. An ancilla a' with Hilbert space $\mathcal{H}_{a'}$ of dimension 4^n is prepared in the state $|\phi\rangle \equiv \frac{1}{2^n} \sum_{l=1}^{4^n} |\mu_l\rangle$, where $\{|\mu_l\rangle\}_{l=1}^{4^n}$ is an orthonormal basis of $\mathcal{H}_{a'}$. Consider the resource state

$|\xi\rangle_{AB}$ for the PBT protocol defined by (3.3) – (3.5). In the primed protocol, the controlled unitary $\sum_{l=1}^{4^n}(|\mu_l\rangle\langle\mu_l|)_{a'}\bigotimes_{i=1}^{N}(V_l)_{B_i}$ is applied on $|\phi\rangle_{a'}|\xi\rangle_{AB}$ in order to prepare the new resource state

$$|\xi'\rangle_{a'AB} \equiv \frac{1}{2^n}\sum_{l=1}^{4^n}\bigotimes_{i=1}^{N}(V_l)_{B_i}|\mu_l\rangle_{a'}|\xi\rangle_{AB}, \tag{C.3}$$

where $(V_l)_{B_i}$ acts on $\mathcal{H}_{B_i}$ only. Recall that $B \equiv B_1B_2\cdots B_N$. The system $a'A$ is sent to Alice and the system B is sent to Bob. In this protocol, the initial state of the system B_j is $\eta'_j \equiv \mathrm{Tr}_{a'A\tilde{B}_j}(|\xi'\rangle\langle\xi'|)_{a'AB}$. From the definitions of η'_j, $|\xi'\rangle$ and η_j (Equation (3.31)), the identity (C.2), and the fact that η_j is independent of $|\psi\rangle$, it is straightforward to obtain that

$$\eta'_j = \frac{1}{4^n}\sum_{l=1}^{4^n} V_l\eta_j V_l^\dagger = \frac{I}{2^n}, \tag{C.4}$$

as claimed.

Now consider the implementation of the primed PBT protocol. Alice applies the unitary operation $W_{aa'} \equiv \sum_{l=1}^{4^n}(V_l^\dagger)_a \otimes (|\mu_l\rangle\langle\mu_l|)_{a'}$ on the system aa', as the notation suggests. The global state transforms into

$$W_{aa'}|\psi\rangle_a|\xi\rangle_{a'AB} = \frac{1}{2^n}\sum_{l=1}^{4^n}(V_l^\dagger)_a\bigotimes_{i=1}^{N}(V_l)_{B_i}|\psi\rangle_a|\mu_l\rangle_{a'}|\xi\rangle_{AB}. \tag{C.5}$$

Then, Alice applies her operations corresponding to the PBT protocol defined by (3.3) – (3.5) on the system aA only. With probability q_j, Alice obtains outcome $k = j \neq 0$. Due to the linearity of unitary evolution, it is not difficult to obtain that, in this case, the global state transforms into

$$|G'_j\rangle_{a'aAB} = \frac{1}{2^n}\sum_{l=1}^{4^n}\bigotimes_{\substack{i=1\\ i\neq j}}^{N}(V_l)_{B_i}|\mu_l\rangle_{a'}|\psi\rangle_{B_j}|R_j\rangle_{aA\tilde{B}_j}. \tag{C.6}$$

Thus, we see that the state $|\psi\rangle$ is teleported to port B_j, as required. This protocol works because, as we can see from (C.5), the operations on the system B commute with the operations performed by Alice on aA, which is necessary for satisfaction of the no-signalling principle. Therefore, this protocol is equivalent to the following: conditioned on a' being in the state $|\mu_l\rangle_{a'}$, if an outcome $k = j \neq 0$ is obtained, the state $V_l^\dagger|\psi\rangle$ is teleported to the port B_j; then, Bob applies $\bigotimes_{i=1}^{N}(V_l)_{B_i}$, after which, the state of the system B_j transforms into $|\psi\rangle$, as desired.

The state of the system B_j, after an outcome $k = i \notin \{0, j\}$ is obtained, is $\gamma'_{j,i} \equiv \mathrm{Tr}_{a'aA\tilde{B}_j}(|G'_i\rangle\langle G'_i|)_{a'aAB}$. From the definitions of $\gamma'_{j,i}$ and $\gamma_{j,i}$ (Equation (3.32)), the identity (C.2), and the fact that $\gamma_{j,i}$ is independent of $|\psi\rangle$, it can easily be obtained that

$$\gamma'_{j,i} = \frac{1}{4^n}\sum_{l=1}^{4^n} V_l \gamma_{j,i} V_l^\dagger = \frac{I}{2^n}, \tag{C.7}$$

as claimed.

If Alice obtains the outcome $k = 0$, the final global state is

$$|G'_0\rangle_{a'aAB} = \frac{1}{2^n}\sum_{l=1}^{4^n}\bigotimes_{i=1}^{N}(V_l)_{B_i}|\mu_l\rangle_{a'}|F^{(\psi_l)}\rangle_{aAB}, \tag{C.8}$$

where ψ_l refers to dependence on the state $V_l^\dagger|\psi\rangle$. In this case, the final state of the system B_j is $\omega_j^{\prime(\psi)} \equiv \mathrm{Tr}_{a'aA\tilde{B}_j}\left(|G'_0\rangle\langle G'_0|\right)_{a'aAB}$. From the previous definition of $\omega_j^{\prime(\psi)}$ and that one of $\omega_j^{(\psi)}$, given by (3.33), it is straightforward to obtain the expression (3.36):

$$\omega_j^{\prime(\psi)} = \frac{1}{4^n}\sum_{l=1}^{4^n} V_l \omega_j^{(\psi_l)} V_l^\dagger. \tag{C.9}$$

Appendix D

Bound for Nonlocal Strategies in the IC-2 Game

Recall the nonlocal strategies in the IC-2 game presented in section 4.5.3. We show the bound (4.60):

$$Q \leq Q', \tag{D.1}$$

where $Q' \equiv \frac{1}{4}\left(1+\frac{3}{\sqrt{n}}\right)$ and $Q = \frac{1}{n}\sum_{k=0}^{n-1} P\left(y_k^0 = x_k^0, y_k^1 = x_k^1\right)$ is the success probability. The proof is an extension of the one given in [108] for the IC-1 game. It requires several steps. Firstly, we define the quantity $E_{\vec{x},k} \equiv (-1)^{x_k^0+x_k^1}\langle\psi|\hat{A}_{\vec{x}}\hat{B}_k|\psi\rangle$ in terms of the Hermitian operators:

$$\begin{aligned}
\hat{A}_{\vec{x}} &\equiv \sum_{r=0}^{1}\sum_{s=0}^{1}(-1)^{r+s}|\nu_{r,s}^{\vec{x}}\rangle\langle\nu_{r,s}^{\vec{x}}|, \\
\hat{B}_k &\equiv \sum_{t=0}^{1}\sum_{u=0}^{1}(-1)^{t+u}|w_{t,u}^{k}\rangle\langle w_{t,u}^{k}|,
\end{aligned}$$

which act on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. We write the state $|\psi\rangle$ in the basis $\{|\nu_{r,s}^{\vec{x}}\rangle|w_{t,u}^{k}\rangle\}$, we use that $y_k^j = a_k^j \oplus b_k^j$, for $j = 0, 1$, and we use the fact that $\vec{x}$ is

a random variable of 4^n possible values to obtain that

$$\frac{1}{n}\sum_{k=0}^{n-1}\left[P\left(y_k^0=x_k^0,y_k^1=x_k^1\right)+P\left(y_k^0\neq x_k^0,y_k^1\neq x_k^1\right)\right]=\frac{1}{2}\left(1+\frac{1}{n4^n}\sum_{k=0}^{n-1}\sum_{\vec{x}}E_{\vec{x},k}\right). \tag{D.2}$$

Then, we show that

$$\frac{1}{2}\left(1+\frac{1}{n4^n}\sum_{k=0}^{n-1}\sum_{\vec{x}}E_{\vec{x},k}\right)\leq\frac{1}{2}\left(1+\frac{1}{\sqrt{n}}\right), \tag{D.3}$$

which from (D.2) implies

$$\frac{1}{n}\sum_{k=0}^{n-1}\left[P\left(y_k^0=x_k^0,y_k^1=x_k^1\right)+P\left(y_k^0\neq x_k^0,y_k^1\neq x_k^1\right)\right]\leq\frac{1}{2}\left(1+\frac{1}{\sqrt{n}}\right). \tag{D.4}$$

We follow a similar procedure to obtain

$$\frac{1}{n}\sum_{k=0}^{n-1}\left[P\left(y_k^0=x_k^0,y_k^1=x_k^1\right)+P\left(y_k^0=x_k^0,y_k^1\neq x_k^1\right)\right]\leq\frac{1}{2}\left(1+\frac{1}{\sqrt{n}}\right), \tag{D.5}$$

$$\frac{1}{n}\sum_{k=0}^{n-1}\left[P\left(y_k^0=x_k^0,y_k^1=x_k^1\right)+P\left(y_k^0\neq x_k^0,y_k^1=x_k^1\right)\right]\leq\frac{1}{2}\left(1+\frac{1}{\sqrt{n}}\right). \tag{D.6}$$

Adding (D.4) – (D.6), using normalization of probabilities and arranging terms we have that

$$\frac{1}{n}\sum_{k=0}^{n-1}P\left(y_k^0=x_k^0,y_k^1=x_k^1\right)\leq\frac{1}{4}\left(1+\frac{3}{\sqrt{n}}\right),$$

as claimed in (D.1).

We show Equation (D.2). Writing $|\psi\rangle$ in the basis $\{|\nu_{r,s}^{\vec{x}}\rangle|w_{t,u}^k\rangle\}$, we have

$$|\psi\rangle=\sum_{r,s,t,u\in\{0,1\}}C_{r,s,t,u}^{\vec{x},k}|\nu_{r,s}^{\vec{x}}\rangle|w_{t,u}^k\rangle.$$

From the definition of $E_{\vec{x},k}$, it follows that

$$\begin{aligned}
E_{\vec{x},k} &= (-1)^{x_k^0+x_k^1} \sum_{r,s,t,u\in\{0,1\}} (-1)^{r+s+t+u} |C^{\vec{x},k}_{r,s,t,u}|^2. \\
&= (-1)^{x_k^0+x_k^1} \sum_{a_k^0,a_k^1,b_k^0,b_k^1\in\{0,1\}} (-1)^{a_k^0\oplus b_k^0} (-1)^{a_k^1\oplus b_k^1} P(a_k^0, a_k^1, b_k^0, b_k^1|\vec{x}) \\
&= (-1)^{x_k^0+x_k^1} \sum_{y_k^0,y_k^1\in\{0,1\}} (-1)^{y_k^0+y_k^1} P(y_k^0, y_k^1|\vec{x}) \\
&= P\left(y_k^0 = x_k^0, y_k^1 = x_k^1|\vec{x}\right) + P\left(y_k^0 \neq x_k^0, y_k^1 \neq x_k^1|\vec{x}\right) \\
&\qquad -P\left(y_k^0 = x_k^0, y_k^1 \neq x_k^1|\vec{x}\right) - P\left(y_k^0 \neq x_k^0, y_k^1 = x_k^1|\vec{x}\right).
\end{aligned}$$

Using normalization of probabilities and arranging terms, we obtain

$$P\left(y_k^0 = x_k^0, y_k^1 = x_k^1|\vec{x}\right) + P\left(y_k^0 \neq x_k^0, y_k^1 \neq x_k^1|\vec{x}\right) = \frac{1}{2}(1 + E_{\vec{x},k}).$$

Since each possible value of $\vec{x}$ occurs with probability 4^{-n}, multiplying the previous equation by $n^{-1}4^{-n}$ and summing over all possible values of $\vec{x}$ and k, we obtain Equation (D.2).

Now we show Equation (D.3). We define the normalized states:

$$\begin{aligned}
|A\rangle &= \frac{1}{\sqrt{4^n}} \sum_{\vec{x}} \hat{A}_{\vec{x}}|\psi\rangle \otimes |\vec{x}\rangle, \\
|B_k\rangle &= \frac{1}{\sqrt{4^n}} \sum_{\vec{x}} (-1)^{x_k^0+x_k^1} \hat{B}_k|\psi\rangle \otimes |\vec{x}\rangle,
\end{aligned}$$

where the set of states $|\vec{x}\rangle$ is orthonormal. We have that $\langle A|B_k\rangle = E_k$, where $E_k \equiv \frac{1}{4^n}\sum_{\vec{x}} E_{\vec{x},k}$. Since the states $|B_k\rangle$ satisfy $\langle B_{k'}|B_k\rangle = \delta_{k',k}$, $\sum_k |B_k\rangle\langle B_k|$ satisfies $\left(\sum_k |B_k\rangle\langle B_k|\right)^2 = \sum_k |B_k\rangle\langle B_k|$ and $\left(\sum_k |B_k\rangle\langle B_k|\right)^\dagger = \sum_k |B_k\rangle\langle B_k|$, hence,

$\sum_k |B_k\rangle\langle B_k|$ is a projector. Thus, we obtain

$$\begin{aligned}\sum_{k=0}^{n-1} E_k^2 &= \sum_{k=0}^{n-1} \langle A|B_k\rangle^2 \\ &= \langle A| \left(\sum_{k=0}^{n-1} |B_k\rangle\langle B_k| \right) |A\rangle \\ &\leq 1. \end{aligned} \tag{D.7}$$

Since the root mean square is not smaller than the average value, we have

$$\begin{aligned}\frac{1}{n}\sum_{k=0}^{n-1} E_k &\leq \sqrt{\frac{1}{n}\sum_{k=0}^{n-1} E_k^2} \\ &\leq \frac{1}{\sqrt{n}}, \end{aligned} \tag{D.8}$$

where in the second line we have used (D.7). Equation (D.3) follows from (D.8) and the definition of E_k.

We adopt a similar procedure to show Equation (D.5). We define $E^0_{\vec{x},k} \equiv (-1)^{x^0_k} \langle\psi|\hat{A}^0_{\vec{x}}\hat{B}^0_k|\psi\rangle$ in terms of the Hermitian operators:

$$\begin{aligned}\hat{A}^0_{\vec{x}} &\equiv \sum_{r=0}^{1}\sum_{s=0}^{1} (-1)^r |\nu^{\vec{x}}_{r,s}\rangle\langle\nu^{\vec{x}}_{r,s}|, \\ \hat{B}^0_k &\equiv \sum_{t=0}^{1}\sum_{u=0}^{1} (-1)^t |w^k_{t,u}\rangle\langle w^k_{t,u}|. \end{aligned}$$

It follows that

$$\begin{aligned}E^0_{\vec{x},k} &= (-1)^{x^0_k} \sum_{a^0_k,a^1_k,b^0_k,b^1_k\in\{0,1\}} (-1)^{a^0_k \oplus b^0_k} P(a^0_k, a^1_k, b^0_k, b^1_k|\vec{x}) \\ &= (-1)^{x^0_k} \sum_{y^0_k=0}^{1} (-1)^{y^0_k} P(y^0_k|\vec{x}) \\ &= P\left(y^0_k = x^0_k|\vec{x}\right) - P\left(y^0_k \neq x^0_k|\vec{x}\right). \end{aligned}$$

From the previous equation, it is straightforward to obtain that

$$\frac{1}{n}\sum_{k=0}^{n-1}\left[P\left(y_k^0=x_k^0,y_k^1=x_k^1\right)+P\left(y_k^0=x_k^0,y_k^1\neq x_k^1\right)\right]=\frac{1}{2}\left(1+\frac{1}{n4^n}\sum_{k=0}^{n-1}\sum_{\vec{x}}E_{\vec{x},k}^0\right). \tag{D.9}$$

We define the normalized states:

$$\begin{aligned}|A^0\rangle &= \frac{1}{\sqrt{4^n}}\sum_{\vec{x}}\hat{A}_{\vec{x}}^0|\psi\rangle\otimes|\vec{x}\rangle,\\ |B_k^0\rangle &= \frac{1}{\sqrt{4^n}}\sum_{\vec{x}}(-1)^{x_k^0}\hat{B}_k^0|\psi\rangle\otimes|\vec{x}\rangle.\end{aligned}$$

We have that $\langle A^0|B_k^0\rangle=E_k^0$, where $E_k^0\equiv\frac{1}{4^n}\sum_{\vec{x}}E_{\vec{x},k}^0$. Similar to (D.8), we obtain

$$\frac{1}{n}\sum_{k=0}^{n-1}E_k^0\leq\frac{1}{\sqrt{n}}. \tag{D.10}$$

From the definition of E_k^0 and Equations (D.9) and (D.10), we obtain (D.5).

In a similar way, Equation (D.6) can be shown using $E_{\vec{x},k}^1\equiv(-1)^{x_k^1}\langle\psi|\hat{A}_{\vec{x}}^1\hat{B}_k^1|\psi\rangle$ in terms of the Hermitian operators:

$$\begin{aligned}\hat{A}_{\vec{x}}^1 &\equiv \sum_{r=0}^{1}\sum_{s=0}^{1}(-1)^s|\nu_{r,s}^{\vec{x}}\rangle\langle\nu_{r,s}^{\vec{x}}|,\\ \hat{B}_k^1 &\equiv \sum_{t=0}^{1}\sum_{u=0}^{1}(-1)^u|w_{t,u}^k\rangle\langle w_{t,u}^k|,\end{aligned}$$

and noticing that $\langle A^1|B_k^1\rangle=E_k^1$, for $E_k^1\equiv\frac{1}{4^n}\sum_{\vec{x}}E_{\vec{x},k}^1$ and the states

$$\begin{aligned}|A^1\rangle &= \frac{1}{\sqrt{4^n}}\sum_{\vec{x}}\hat{A}_{\vec{x}}^1|\psi\rangle\otimes|\vec{x}\rangle,\\ |B_k^1\rangle &= \frac{1}{\sqrt{4^n}}\sum_{\vec{x}}(-1)^{x_k^1}\hat{B}_k^1|\psi\rangle\otimes|\vec{x}\rangle.\end{aligned}$$

References

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.

[2] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964. Reprinted in [121], pages 14–21.

[3] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3-4):379–423,623–656, 1948.

[4] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer, Berlin, 1932. English translation by R. T. Beyer. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, NJ, 1955.

[5] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[6] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[7] A. S. Kholevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3):177–183, 1973. Translated from *Problemy Peredachi Informatsii*, 9(3):3–11,1973.

[8] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature (London)*, 299:802–803, 1982.

[9] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982.

[10] R. Jozsa. A stronger no-cloning theorem. E-print arXiv:quant-ph/0204153, 2002.

[11] R. Jozsa. Illustrating the concept of quantum information. E-print arXiv:quant-ph/0305114, 2003.

[12] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.

[14] B. Schumacher. Quantum coding. *Physical Review A*, 51(4):2738–2747, 1995.

[15] A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265, 1937.

[16] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, 1980.

[17] P. Benioff. Quantum mechanical Hamiltonian models of Turing machines. *Journal of Statistical Physics*, 29(3):515–546, 1982.

[18] P. Benioff. Quantum mechanical models of Turing machines that dissipate no energy. *Physical Review Letters*, 48(23):1581–1585, 1982.

[19] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982.

[20] R. P. Feynman. Quantum mechanical computers. *Foundations of Physics*, 16(6):507–531, 1986. Originally appeared in *Optics News*, February 1985.

[21] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400(1818):97–117, 1985.

[22] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A*, 439(1907):553–558, 1992.

[23] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Los Alamitos, California, 1994. IEEE Computer Society Press.

[24] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in cryptology: Proceedings of CRYPTO 82*, pages 267–275, New York, 1983. Plenum Press.

[25] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, 1984. IEEE.

[26] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[27] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, 2005.

[28] O. E. Lanford and D. W. Robinson. Mean entropy of states in quantum-statistical mechanics. *Journal of Mathematical Physics*, 9(7):1120–1125, 1968.

[29] H. Araki and E. H. Lieb. Entropy inequalities. *Communications in Mathematical Physics*, 18(2):160–170, 1970.

[30] L. Henderson and V. Vedral. Classical, quantum and total correlations. *Journal of Physics A: Mathematical and General*, 34(35):6899, 2001.

[31] H. Ollivier and W. H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Physical Review Letters*, 88(1):017901, 2001.

[32] B. Groisman, S. Popescu, and A. Winter. Quantum, classical, and total amount of correlations in a quantum state. *Physical Review A*, 72(3):032317, 2005.

[33] J. Barrett. Information processing in generalized probabilistic theories. *Physical Review A*, 75(3):032304, 2007.

[34] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844–1852, 1996.

[35] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin. Optimal universal and state-dependent quantum cloning. *Physical Review A*, 57(4):2368–2378, 1998.

[36] N. Gisin and S. Massar. Optimal quantum cloning machines. *Physical Review Letters*, 79(11):2153–2156, 1997.

[37] N. Gisin. Quantum cloning without signaling. *Physics Letters A*, 242(1-2):1–3, 1998.

[38] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín. Quantum cloning. *Review of Modern Physics*, 77(4):1225–1256, 2005.

[39] R. F. Werner. Optimal cloning of pure states. *Physical Review A*, 58(3):1827–1832, 1998.

[40] M. Keyl and R. F. Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7):3283, 1999.

[41] D. Bohm. *Quantum Theory*. Prentice-Hall, New York, 1951.

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

[43] J. S. Bell. Introduction to the hidden-variable question. In *Foundations of Quantum Mechanics. Proceedings of the International School of Physics 'Enrico Fermi', course IL*, pages 171–181, New York, 1971. Academic. Reprinted in [121], pages 29–39.

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

[45] S. L. Braunstein and C. M. Caves. Wringing out better Bell inequalities. *Annals of Physics*, 202(1):22–56, 1990.

[46] S. Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Physical Review A*, 73(2):022110, 2006.

[47] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, 47(7):460–463, 1981.

[48] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment* : A new violation of Bell's inequalities. *Physical Review Letters*, 49(2):91–94, 1982.

[49] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time- varying analyzers. *Physical Review Letters*, 49(25):1804–1807, 1982.

[50] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of Bell inequalities by photons more than 10 km apart. *Physical Review Letters*, 81(17):3563–3566, 1998.

[51] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters*, 81(23):5039–5043, 1998.

[52] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature (London)*, 409:791–794, 2001.

[53] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe. Bell inequality violation with two remote atomic qubits. *Physical Review Letters*, 100(15):150404, 2008.

[54] D. Salart, A. Baas, J. A. W. van Houwelingen, N. Gisin, and H. Zbinden. Spacelike separation in a Bell test assuming gravitationally induced collapses. *Physical Review Letters*, 100(22):220404, 2008.

[55] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger. Bell violation using entangled photons without the fair-sampling assumption. *Nature (London)*, 497:227–230, 2013.

[56] J. F. Clauser and M. A. Horne. Experimental consequences of objective local theories. *Physical Review D*, 10(2):526–535, 1974.

[57] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Physical Review A*, 47(2):R747–R750, 1993.

[58] J. S. Bell. Bertlmann's socks and the nature of reality. *Journal de Physique*, 42(3):C2 41–61, 1981. Reprinted in [121], pages 139–158.

[59] E. Santos. Constraints for the violation of the Bell inequality in Einstein-Podolsky-Rosen-Bohm experiments. *Physics Letters A*, 200(1):1–6, 1995.

[60] P. M. Pearle. Hidden-variable example based upon data rejection. *Physical Review D*, 2(8):1418–1425, 1970.

[61] A. Kent. Causal quantum theory and the collapse locality loophole. *Physical Review A*, 72(1):012107, 2005.

[62] N. Gisin and H. Zbinden. Bell inequality and the locality loophole: Active versus passive switches. *Physics Letters A*, 264(2-3):103–107, 1999.

[63] A. Garg and N. D. Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Physical Review D*, 35(12):3831–3835, 1987.

[64] L. Diósi. A universal master equation for the gravitational violation of quantum mechanics. *Physics Letters A*, 120(8):377–381, 1987.

[65] L. Diósi. Models for universal reduction of macroscopic quantum fluctuations. *Physical Review A*, 40(3):1165–1174, 1989.

[66] R. Penrose. On gravity's role in quantum state reduction. *General Relativity and Gravitation*, 28(5):581–600, 1996.

[67] A. Kent. A proposed test of the local causality of spacetime. In *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, pages 369–378. Springer, 2009. E-print arXiv:gr-qc/0507045.

[68] D. Bohm. *The Special Theory of Relativity*. W. A. Benjamin, New York, 1965.

[69] G. C. Ghirardi, A. Rimini, and T. Weber. A general argument against superluminal transmission through the quantum mechanical measurement process. *Lettere al Nuovo Cimento*, 27(10):293–298, 1980.

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

[71] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nature (London)*, 461:1101–1104, 2009.

[72] A. Kent. Quantum nonlocal correlations are not dominated. E-print arXiv:1308.5009, 2013.

[73] J. Bae, W.-Y. Hwang, and Y.-D. Han. No-signaling principle can determine optimal quantum state discrimination. *Physical Review Letters*, 107(17):170403, 2011.

[74] A. Kent. A no-summoning theorem in relativistic quantum theory. *Quantum Information Processing*, 12(2):1023–1032, 2013. E-print arXiv:1101.4612.

[75] A. Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13:113015, 2011.

[76] A. Kent. Location-oblivious data transfer with flying entangled qudits. *Physical Review A*, 84(1):012328, 2011.

[77] Y. Aharonov and D. Z. Albert. States and observables in relativistic quantum field theories. *Physical Review D*, 21(12):3316–3324, 1980.

[78] Y. Aharonov and D. Z. Albert. Can we make sense out of the measurement process in relativistic quantum mechanics? *Physical Review D*, 24(2):359–370, 1981.

[79] Y. Aharonov and D. Z. Albert. Is the usual notion of time evolution adequate for quantum-mechanical systems? I. *Physical Review D*, 29(2):223–227, 1984.

[80] Y. Aharonov and D. Z. Albert. Is the usual notion of time evolution adequate for quantum-mechanical systems? II. Relativistic considerations. *Physical Review D*, 29(2):228–234, 1984.

[81] B. Groisman and B. Reznik. Measurements of semilocal and nonmaximally entangled states. *Physical Review A*, 66(2):022110, 2002.

[82] L. Vaidman. Instantaneous measurement of nonlocal variables. *Physical Review Letters*, 90(1):010402, 2003.

[83] B. Groisman, B. Reznik, and L. Vaidman. Instantaneous measurements of nonlocal variables. *Journal of Modern Optics*, 50(6-7):943–949, 2003.

[84] S. R. Clark, A. J. Connor, D. Jaksch, and S. Popescu. Entanglement consumption of instantaneous nonlocal quantum measurements. *New Journal of Physics*, 12:083034, 2010.

[85] S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13:093036, 2011.

[86] A. P. Kent, W. J. Munro, T. P. Spiller, and R. G. Beausoleil. Tagging systems. US Patent No. 7,075,438, 2006.

[87] R. A. Malaney. Location-dependent communications using quantum entanglement. *Physical Review A*, 81(4):042319, 2010.

[88] R. A. Malaney. Quantum location verification in noisy channels. E-print arXiv:1004.4689, 2010.

[89] A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011.

[90] H.-K. Lau and H.-K. Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):012322, 2011.

[91] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: Impossibility and constructions. E-print arXiv:1009.2490, 2011.

[92] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158, New York, 2013. ACM.

[93] A. Kent. Quantum tagging for tags containing secret classical data. *Physical Review A*, 84(2):022335, 2011.

[94] A. Kent and D. Pitalúa-García. Sphere colourings and Bell inequalities. E-print arXiv:1307.6839, 2013.

[95] N. Aharon, S. Machnes, B. Reznik, J. Silman, and L. Vaidman. Continuous input nonlocal games. *Natural Computing*, 12(1):5–8, 2013.

[96] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, 1989.

[97] B. Bukh. Measurable sets with excluded distances. *Geometric and Functional Analysis*, 18(3):668–697, 2008.

[98] F. M. de Oliveira Filho and F. Vallentin. Fourier analysis, linear programming, and densities of distance avoiding sets in $\mathbb{R}^n$. *Journal of the European Mathematical Society*, 12(6):1417–1428, 2010.

[99] D. Pitalúa-García. Deduction of an upper bound on the success probability of port-based teleportation from the no-cloning theorem and the no-signaling principle. *Physical Review A*, 87(4):040303(R), 2013.

[100] S. Ishizaka and T. Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical Review Letters*, 101(24):240501, 2008.

[101] S. Ishizaka and T. Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79(4):042306, 2009.

[102] M. A. Nielsen and I. L. Chuang. Programmable quantum gate arrays. *Physical Review Letters*, 79(2):321–324, 1997.

[103] S. Strelchuk, M. Horodecki, and J. Oppenheim. Generalized teleportation and entanglement recycling. *Physical Review Letters*, 110(1):010505, 2013.

[104] D. Pitalúa-García. Quantum information causality. *Physical Review Letters*, 110(21):210402, 2013.

[105] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

[106] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols. Quantum random access codes with shared randomness. E-print arXiv:0810.2937, 2009.

[107] M. Pawłowski and M. Żukowski. Entanglement-assisted random access codes. *Physical Review A*, 81(4):042326, 2010.

[108] S. W. Al-Safi and A. J. Short. Information causality from an entropic and a probabilistic perspective. *Physical Review A*, 84(4):042323, 2011.

[109] M. Pawłowski and V. Scarani. Information causality. E-print arXiv:1112.1142, 2011.

[110] J. Allcock, N. Brunner, M. Pawłowski, and V. Scarani. Recovering part of the boundary between quantum and nonquantum correlations from information causality. *Physical Review A*, 80(4):040103(R), 2009.

[111] D. Cavalcanti, A. Salles, and V. Scarani. Macroscopically local correlations can violate information causality. *Nature Communications*, 1:136, 2010.

[112] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués. Quantum correlations require multipartite information principles. *Physical Review Letters*, 107(21):210403, 2011.

[113] T. H. Yang, D. Cavalcanti, M. L. Almeida, C. Teo, and V. Scarani. Information-causality and extremal tripartite correlations. *New Journal of Physics*, 14:013061, 2012.

[114] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Reviews of Modern Physics*, 84(4):1655–1707, 2012.

[115] L. Hardy. Quantum theory from five reasonable axioms. E-print arXiv:quant-ph/0101012, 2001.

[116] H. Barnum, J. Barrett, M. Leifer, and A. Wilce. Generalized no-broadcasting theorem. *Physical Review Letters*, 99(24):240501, 2007.

[117] A. J. Short and S. Wehner. Entropy in general physical theories. *New Journal of Physics*, 12:033023, 2010.

[118] H. Barnum, J. Barrett, L. O. Clark, M. Leifer, R. Spekkens, N. Stepanik, A. Wilce, and R. Wilke. Entropy and information causality in general probabilistic theories. *New Journal of Physics*, 12:033024, 2010.

[119] O. C. O. Dahlsten, D. Lercher, and R. Renner. Tsirelson's bound from a generalized data processing inequality. *New Journal of Physics*, 14:063024, 2012.

[120] L. Masanes, M. P. Mueller, R. Augusiak, and D. Perez-Garcia. A digital approach to quantum theory. E-print arXiv:1208.0493, 2012.

[121] J. S. Bell. *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, Cambridge, 1987.