HELSINKI INSTITUTE OF PHYSICS INTERNAL REPORT SERIES

HIP-2001-07

QUANTUM INFORMATION PROCESSING AND ITS LINEAR OPTICAL IMPLEMENTATION

John Calsamiglia

Helsinki Institute of Physics
University of Helsinki
Helsinki, Finland

Academic dissertation
To be presented, with the permission of the Faculty of Science of the University of Helsinki, for public criticism in Auditorium E204 in the Physicum on December 21, 2001, at 12 o'clock a.m.

Helsinki 2001

ISBN 951-45-8932-7 (print)
ISBN 951-45-8933-5 (PDF)
http://ethesis.helsinki.fi
ISSN 1455-0563
Helsinki 2001
Yliopistopaino

Acknowledgments

In front of me lies a text followed by some research papers: the compound of pieces of discussions, reading, hoping, failing and succeeding. Surprisingly it has the form of a dissertation.

Of course, I could have not possibly done this work alone. My very first words of gratefulness should go to Kalle-Antti Suominen, my supervisor. He helped me invaluably providing me at every moment with the best environment. His knowledge, manners, efficiency and smoothness made easy every step of my stay here. I want to express my warmest gratitude to Norbert Lütkenhaus, who constantly, during and after his stay in Helsinki, has supported and advised me, and thanks to whom I struggled to formalize my inner intuitions. My deepest appreciation to Steve Barnett for his ability to make interesting problems out of inprecise or fuzzy questions. I also gratefully acknowledge my other collaborators Dagmar Bruss and Matt Mackie. I would like to heartfully thank Martin Plenio for his hospitality during my stay in London, and for being always available and disposed to share his knowledge. For making my years in Helsinki unforgettable I should thank all my friends and colleagues here.

Finally, I would like to thank my huge family —specially Xavier and Mariona for loving each other so much, and for being comprehensive, brave, and loving parents —and my friends all over the world.

To Marta thanks here and everywhere.

Helsinki, December 5, 2001
John Calsamiglia Costa

Abstract

This dissertation includes results on applied and theoretical aspects of Quantum Information theory.

The central topic in this thesis is the quantum information processing capabilities of linear optical elements. Photons are the number one candidates for the implementation of quantum communication protocols, since they are readily transported and have low decoherence rates. However, the lack of strong interactions between photons hinders the implementation of non-local quantum operations. Here I discuss the possibility of exploiting the indistinguishability of the photons and the implied interference and particle statistics effects to perform non-local operations on photonic qubits using only linear optical elements. Special attention is drawn to the Bell-measurement, for which a general no-go theorem is proven. The optimal efficiency of an incomplete Bell-measurement is found to be one half. Also the general form of the two-qubit POVMs that can be implemented with only linear elements and particle detectors is given.

A very simple linear optical scheme is proposed to remove a given number of photons from a field mode and its application to a quantum key distribution eavesdropping attack is analyzed.

As side topics, the universal cloning transformation is analyzed in terms of the effective POVMs on the input realized by measuring the output subsystems; and photoassociation of an atomic degenerate gas is proposed as the means to create a superposition of a macroscopic number of atoms and molecules.

Contents

List of Publications

This thesis consists of an introductory part, followed by seven research publications. The introductory part includes some previously unpublished material.

I *Quantum cloning and distributed measurements*
D. Bruss, J. Calsamiglia, and N. Lütkenhaus
Physical Review A **63**, 042308 (2001).

II *Bell measurements for teleportation*
N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen
Physical Review A **59**, 3295-3300 (1999).

III *Maximum efficiency of a linear-optical Bell-state analyzer*
J. Calsamiglia and N. Lütkenhaus
Applied Physics B-Lasers and Optics **72**, 67-71 (2001).

IV *Generalized quantum measurements by linear elements*
J. Calsamiglia
to appear in Physical Review A (February 2002); quant-ph/0108108.

V *Removal of a single photon by adaptive absorption*
J. Calsamiglia, N. Lütkenhaus, S. M. Barnett and K-A. Suominen
Physical Review A **64**, 043814 (2001); quant-ph/0106086.

VI *Conditional beam splitting attack on quantum key distribution*
J. Calsamiglia, N. Lütkenhaus and S. M. Barnett
to appear in Physical Review A (December 2001); quant-ph/0107148.

VII *Superposition of macroscopic numbers of atoms and molecules*
J. Calsamiglia, M. Mackie and K-A. Suominen
Physical Review Letters **87**, 160403 (2001).

1 Introduction to the Dissertation

Quantum Information Theory is a new research field that brings together disciplines of physics and computer science with the aim of understanding how the laws of quantum mechanics can be used to dramatically improve the acquisition, transmission, and processing of information. Quantum Information Theory provides a completely new and enlightening way of describing the foundations of quantum phenomena. However, what gave a lasting boost to the field was the early discovery of tasks that are facilitated by quantum mechanics: Quantum cryptography guarantees fundamentally secure communication, Shor's quantum factoring algorithm gives an exponential speed-up with respect to any classical algorithm, and teleportation transmits an unknown quantum state without actually sending any particle through the channel. Many applications are following, bringing about technological and scientific revolutions even in other fields, and warranting further research in Quantum Information Theory.

A topic of interest in this dissertation is the spreading of information and appearance of quantum correlations when an initial quantum state is coupled to an auxiliary system. Some results have been applied to the universal quantum cloning transformation. By drawing a correspondence between measurements at the output subsystems (i.e. clones and ancillae) and the *effective measurements* on the unknown input state we have elucidated how all information contained in the input state is distributed over the entangled state of the output, thus bringing out properties of the universal cloner which might make it a useful concept in quantum information processing. The cloning transformation serves also as a perfect ground to show how the ideas of sharp measurements, accessible information, and ideal channels are interconnected.

My primary interest has been to study the possibilities of encoding and processing quantum information with linear optics. The immediate and practical motivation of this study is its relevance in quantum communication tasks, where photons are by now the only serious candidates for qubit carriers. Photons are readily transported through free space or optical fibers. Their very weak interaction strengths subside decoherence effects, but at the same time render rather difficult the implementation of quantum gates. On the other hand, photonic realizations of qubits allow for other ways of processing and extracting the represented quantum information. The qubits are now indistinguishable particles. This brings into play interference and particle statistics effects in our qubit carriers. In order to

exhibit this effects, it suffices to use linear optical elements such as beam splitters and phase shifters that are about the simplest optical devices. Hitherto research in this topic has led my collaborators and me to two main results concerning ability to perform Bell-measurements and other generalized quantum measurements using linear optical elements. For this, we formalized the use of interference by the definition of a simple class of operations which include linear optical elements, auxiliary photonic states and conditional operations. Conditional operations are realized through the monitoring of some modes with photodetectors. This introduces a very particular type of non-linearity which is easy to realize, but together with the linear mapping of modes provides a way to perform highly non-trivial operations on the initial qubits.

The idea of conditional measurements has been further investigated in a slightly different context, that of quantum feedback control. The result of a weak measurement is used to modify the future dynamics of the system under observation. This typically leads to highly non-Markovian systems with very rich dynamics. An application of this type of evolution has brought us to a novel eavesdropping attack on quantum key distribution (QKD): Conditional beam splitting attack. Signals used in all current implementations of QKD are weak coherent pulses instead of single photons. This modification of the signals together with the large losses in long distance transmissions open a security gap. The basic idea behind the conditional beam splitting attack is to extract one single photon from the transmitted signal. This should provide the eavesdropper with the secret key whenever she succeeds in extracting a photon from the multiphoton part of the signal. The implementation of this attack consists in applying a series of very weak beam splitters with a photodetector in the weakly-coupled output arm. As soon as one detector fires, the coupling is switched off, i.e. no further beam splitters are applied. This very simple feedback mechanism offers a QKD attack which is much more efficient than the conventional beam spitting attack and, unlike the photon number splitting attack, is feasible with the current technology.

We have also explored the possibility of studying quantum phenomena using non-linear interactions. For this purpose, instead of photons, we have studied degenerate atom-molecule systems where much stronger nonlinearities are available. In particular we have proposed the means of creating a very particular "Schrödinger cat". We show that by suitably shining two-color photoassociation lasers on a non-ideal atomic Bose-Einstein condensate one can obtain a superposition of a molecular degenerate gas and

an atomic degenerate gas. Beyond the usual macroscopic superposition of two states of a given object, photoassociation actually leads to a more counterintuitive situation since, like (say) protons and quarks, molecules and atoms are different objects. Analogously, second-harmonic generation could lead to a macroscopic superposition of a bunch of red photons and bunch of blue photons.

This work is organized in two main parts. In the first part I give a rather dense presentation of quantum information theory. This includes the basic formalism and most relevant applications of this work. The second part concerns the physical implementations of quantum information processing. Special attention is drawn to the linear-optical implementations which form the bulk of the research presented here. The second part also contemplates the possibility of exploiting the non-linearities present in atomic systems to create a superposition of a macroscopic number of atoms and molecules. Since the papers included in this thesis are mostly self-contained, and many important concepts are already presented in the first part, the second part is restricted to presenting only the specifics of the implementations.

2 Quantum Information: Theory

2.1 Quantum Information and the Qubits

If one looks at the works of information theorists it is quite difficult to find any reference to the physical system used as information-carrier. Instead, one finds *bits* as building blocks of their theory. This abstraction is founded on the idea that signals can be converted from one physical form to another without any loss of information. For example, the message "I'll be home for Xmas" can be sent by tapping a finger, which produces a series of electric impulses that travel through a copper cable and are subsequently converted into marks in a piece of paper or sound waves that can be translated back into the original message. Notice that during these series of conversions the *same* information does not only change its physical support, but also its encoding. In the late 40's Shannon presented the *Noiseless Channel Coding* theorem [122] that quantified the minimal resources needed to hold all the information contained in a signal. With this, he gave the first mathematical definition of information. The basic units of information are what we know as *bits* and are binary variables valued either 0 or 1. According to Shannon's first coding theorem any signal encoded by a set of "letters" $X = \{x_1 \dots x_n\}$ occurring with probabilities $\vec{p} \equiv \{p_1 \dots p_n\}$, can be faithfully encoded in a binary string consisting of $H(\vec{p})$ bits. $H(\vec{p})$ is the *Shannon Information* of

the signal X and is given by

$$H(\vec{p}) = -\sum_{i=1}^{n} p_i \log_2(p_i). \tag{1}$$

Information and physics never met again till Landauer reminded us that *information is physical* [87, 88] by realizing that the erasure of information is always accompanied by generation of heat; thus bridging information theory with thermodynamics. Landauer's principle served to solve the conflict between Maxwell's demon and the second law of thermodynamics [6] and to show how physics constrains information processing [12]. However, the first steps towards merging physics and information, that eventually gave rise to the field of Quantum Information, were taken from quantum mechanics. A relatively small group of researchers started, already in the 60's, to investigate the transmission of classical information through quantum channels (for a good account see [82, 64, 66]). The basic tools used currently to describe quantum channels and quantum measurements, which we will review in the forthcoming sections, were developed back then. The first important result that marked a clear difference between classical and quantum information was the no-cloning theorem [46, 143] that states that, unlike classical data, the quantum information held in an unknown quantum state (see below and in Section 2.3.2) cannot be copied. Among other things, this implies that one cannot access all the information describing a quantum state by measuring it. This looks more like a drawback, but it was soon realized that this fact opened the doors for something impossible to realize by classical means [123]: quantum cryptography guaranteed fundamentally secure communication [140, 7]. The subsequent discovery of quantum computation [5, 51, 45], quantum algorithms [124, 62], quantum teleportation [8], quantum dense coding [13] and quantum error correction [125, 130] made it clear that quantum mechanics offered new ways of encoding, processing and decoding information, and the field of quantum information was founded.

According to the *first postulate* of quantum mechanics (see e.g. [41]) every isolated physical system is associated to a Hilbert space $\mathcal{H}$ in such a way that the system is completely described by a normalized ray called *state vector*. The state vector provides us with the most complete description of the system. It gives us all the information that can be obtained by any conceivable measurement on the system. In practice this situation only happens after a preparation procedure. The actual meaning or "reality status" attributed to the state vector is not well settled among the

physicist community (see for example [107, 63], [85] and references therein). Leaving these ontological matters aside, there is consensus on the actual praxis of quantum mechanics and we can go on turning the crank of this mind-puzzling machinery with the comfort that this centennial theory produces results with unprecedented experimental agreement. I do not declare myself an instrumentalist, but it falls out of the scope of this thesis to elaborate more on this idea and I could not give any original insights other than expressing my hopes that by turning the crank and keeping a "scientific attitude" one can acquire a deeper understanding of the intricate relations between the quantum world, the classical world and ourselves. In my opinion a scientist has not only to be able to describe the behavior of physical objects, but also to inquire about the origin of this behavior. It is the urge to *explain*[1] things which keeps science moving. This inquiring aspect of a scientist is what I miss in any instrumentalist attitude towards quantum mechanics. That is why I do not immediately disqualify interpretations of quantum mechanics which try to explain, though so far I did not find any that has presented itself "clear and distinctly before my mind" as a satisfactory explanation.

The most simple non-trivial quantum system is a two level system and has a two-dimensional state space. Two orthonormal vectors $|0\rangle$ and $|1\rangle$, representing for example the horizontal and vertical polarizations of a photon, an electron or nucleus spin up and spin down along a particular axis or the ground and excited states of an atom, can be chosen to form the *computational basis*. In this basis, a generic state of the system can be written as

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2}$$

where α and β are complex numbers satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. This elemental 2-level quantum system was dubbed *qubit* (quantum bit) by Ben Schumacher when presenting the quantum analog of the noiseless channel coding theorem [75, 120]. By inspecting Eq. (2) one realizes that in order to give a complete description of the state of the qubit one needs to specify the value of two real numbers (the global phase does not have any physical relevance). This means that a single qubit holds an infinite amount of classical information, i.e. an infinite number of bits. On the other hand, a measurement will only give two possible complementary

[1] Unluckily, I lack of strict definition of an "explanation" in absolute terms. It looks like in quantum mechanics we have reached the bottom.

answers revealing at most one bit of that information[2]. It is clear that we need different elementary units for classical and quantum information. The *qubit* presents itself as a good candidate for the basic unit of quantum information and the *quantum noiseless channel theorem* makes this definition sound. Briefly, the quantum version of Shannon's first coding theorem says that any quantum signal characterized by the "quantum letters" $\{|\varphi_1\rangle, \ldots, |\varphi_n\rangle\}$ occurring with probabilities $\vec{p} \equiv \{p_1, \ldots, p_n\}$ can be reliably encoded in an amount of qubits per source "letter" equal to the *von Neumann entropy*,

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho) \;\; \text{where } \rho = \sum_{i=1}^{n} p_i |\varphi_i\rangle\langle\varphi_i|, \tag{3}$$

and the states $|\varphi_i\rangle$ might live in a higher dimensional Hilbert space ($d \geq 2$) and do not need to be mutually orthogonal. Here, we have also introduced a new mathematical construction ρ called *density operator* or *density matrix*. The density operator formalism allows to describe states on which we do not have complete knowledge. This situation arises for example when we allow for some classical uncertainty in the preparation procedure or when a well determined system interacts with a second system such as the environment. The density operator is a *positive*[3] and unit trace ($\mathrm{Tr}\rho = 1$) operator. Density operators form a convex set since if ρ_0 and ρ_1 are density operators, then the state corresponding to the statistical mixture $p\rho_0 + (1-p)\rho_1$ ($0 \leq p \leq 1$) is a density operator as well. A given density matrix can always be written as convex sum like in Eq. (3). This allows for an *ensemble interpretation* of the density matrix ρ as a description of a system that is in one of the states $\{|\varphi_i\rangle\}$ with respective probabilities $\{p_i\}$. However, a given density matrix can have many different decompositions and therefore many ensemble interpretations (or *realizations*). A density matrix $\rho = \sum_{i=1}^{n} p_i |\varphi_i\rangle\langle\varphi_i| = \sum_{i=1}^{m} q_i |\phi_i\rangle\langle\phi_i|$ can be realized by drawing the states $\{|\varphi_i\rangle\}_{i=1}^{n}$ according to a probability distribution $\{p\}_{i=1}^{n}$ but also by drawing a state from a different set $\{|\phi_i\rangle\}_{i=1}^{m}$ with probabilities $\{q\}_{i=1}^{m}$. The equivalence of two realizations can be checked using the theorem [70],

$$\sum_{i=1}^{n} |\tilde{\varphi}_i\rangle\langle\tilde{\varphi}_i| = \sum_{i=1}^{m \leq n} |\tilde{\phi}_i\rangle\langle\tilde{\phi}_i| \Longleftrightarrow |\tilde{\varphi}_i\rangle = \sum_{j=1}^{n} U_{ij} |\tilde{\phi}_j\rangle \text{ where } U \text{ is unitary}, \tag{4}$$

[2] A strict version of this argument is given by Holevo's bound. See Eq. (41) in Section 2.3.1.

[3] A is positive $A \geq 0 \Leftrightarrow \langle\varphi|A|\varphi\rangle \geq 0 \; \forall |\varphi\rangle$. It is also conventional to use the term *positive semi-definite* to designate such an operator, and *positive definite* when the previous inequalities become strict inequalities ($>$).

the tilde denotes that the states are not normalized, and $|\tilde{\phi}_j\rangle \equiv 0$ for $j > m$. *Pure states*, e.g. $|\varphi\rangle\langle\varphi|$, are the extreme points of the convex set of density matrices and allow only one possible ensemble interpretation since they have a unique decomposition with a single term ($p_1 = 1$). Pure states correspond to the maximal state of knowledge described earlier by the state vector $|\varphi\rangle$. On the contrary, *mixed states* are density operators with higher rank and correspond to states with less than maximal knowledge. There is a simple purity criterion: ρ is pure iff $\mathrm{Tr}\rho^2 = 1$. But, how do we quantify the mixedness or disorder of a given density matrix? Classically the most natural measure is the Shannon information (or Shannon entropy depending on the context) given by Eq. (1). It quantifies the average information gained when sampling a given probability distribution. The more disordered the source is, the more information we gain when sampling its outcome. In the quantum case things get bit more tricky because a given density matrix has an infinite number of realizations associated to different probability distributions. In order to make the measure "interpretation-independent" and get rid of any disorder introduced by a bad choice decomposition, one defines the measure as the minimum Shannon information taken over all possible ensemble interpretations of ρ

$$S(\rho) \equiv \min_{\{p_i\}} H(\vec{p}), \tag{5}$$

where $\vec{p} = \{p_i\}$ defines the probability distributions associated to the possible realizations of ρ. It is easy to show that the minimum of $H(\vec{p})$ is achieved by the probability distribution defined by the eigenvalues $\{\lambda_i\}$ of ρ. This implies that the measure of disorder or mixedness for a quantum state ρ is its von Neumann entropy introduced in Eq. (3).

Before passing to composite systems let me briefly introduce a very convenient parametrization of the single system density matrices. A density matrix on a d-dimensional Hilbert space (also called a *qu**d**it*) is a Hermitian operator and can therefore be written in the form

$$\rho = \frac{1}{d}(\mathbb{1} + \vec{\lambda} \cdot \vec{\tau}), \tag{6}$$

where $\vec{\tau} = \{\tau_i\}$ are the $d^2 - 1$ generators of $SU(d)$ that obey $\mathrm{Tr}(\tau_i \tau_j) = 2\delta_{ij}$ and the *coherence vector* $\vec{\lambda}$ is a real-valued vector with components $\lambda_i = \mathrm{Tr}(\tau_i \rho)$. The positivity of the density matrix implies that $|\vec{\lambda}|^2 \leq \frac{d(d-1)}{d}$ but only for $d = 2$ this is also a sufficient condition for positivity. For qubits the coherence vector is called *Bloch vector* and its usually denoted by $\vec{s} = \{s_x, s_y, s_z\}$ and the $SU(2)$ generators are the ubiquitous Pauli operators

$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ and $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. In this representation the whole set of qubit density matrices is represented by a unit-ball: the vectors reaching the surface of the ball are the pure states ($Tr(\rho^2) = 1 \Rightarrow |\vec{s}| = 1$) and all their convex combinations represent the mixed states ($|\vec{s}| < 1$). The maximally mixed state corresponds to the center of the ball ($|\vec{s}| = 0$).

The total Hilbert space associated to a system composed of N subsystems, such as the qubits in a quantum computer register, is the tensor product of the Hilbert spaces of the individual subsystems $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N$. An important concept that appears in this context is that of the *partial trace*. Imagine that a composite system is described by a state ρ_{AB} on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. This density matrix reflects all the knowledge that we have on the system in the sense that it gives us the maximal predictive power on the outcomes of any measurement done on the composite system. What happens if we restrict ourselves to measurements on, say, subsystem A? The density matrix ρ_A of this subsystem should similarly provide us with the outcome statistics of any conceivable measurement[4] performed on it. It should be no surprise that this density matrix ρ_A can be obtained from our knowledge on the total system, i.e. from ρ_{AB}. It is easy to show that the *partial trace* over the remaining part of system, $\mathrm{Tr}_B(\rho_{AB})$, does precisely this job and is defined as follows

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) \equiv \sum_{i=1}^{d_B} \langle e_i|\rho_{AB}|e_i\rangle, \tag{7}$$

where $\{|e_i\rangle\}_{i=1}^{d_B}$ is an orthonormal basis of $\mathcal{H}_B$. The state left after doing the partial trace is called *reduced density matrix*, and one says that the system B has been *traced out*. Notice that the partial trace is a linear operation and therefore an ensemble interpretation of the total system is consistent with the ensemble of reduced density matrices of the subsystem.

A composite system is said to be in a *product state* if the description of the isolated subsystems is equivalent to the description of the total system. Explicitly,

$$\rho_{AB} = \rho_A \otimes \rho_B \text{ where } \rho_A = \mathrm{Tr}_B(\rho_{AB}) \text{ and } \rho_B = \mathrm{Tr}_A(\rho_{AB}). \tag{8}$$

Product states exhibit no correlations whatsoever between the subsystems. However, quantum mechanics allows for different sorts of correlations. A

[4]See next section for a precise definition of quantum measurement.

state acting on $\mathcal{H}_{AB}$ is called *separable*[5] if it can be written in the form,

$$\rho = \sum_{i=1}^{m} p_i \rho_i \otimes \tilde{\rho}_i, \tag{9}$$

where ρ_i and $\tilde{\rho}_i$ are states on $\mathcal{H}_A$ and $\mathcal{H}_B$ and the p_i's define a probability distribution. This state has only classical correlations (except for $p_i = \delta_{i1}$), thus it can be prepared by *LOCC* (**L**ocal **O**perations and **C**lassical **C**ommunication). If a state *cannot* be written in the above form, Eq. (9), then it is called *entangled* and it exhibits genuine quantum correlations. Historically, entanglement was first recognized by Einstein, Podolsky and Rosen (EPR) in their famous paper [50] where they skeptically unveiled the non-local nature of quantum mechanics, and by Schrödinger [119, 139] who realized that entanglement —or *verschränkung* as he called it—gave rise to situations where the "best possible knowledge of a whole does *not* include the best possible knowledge of its parts..." [119, 139]. Indeed, the paradigmatic entangled state, the singlet[6]

$$|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{10}$$

is a pure sate, and therefore describes a state of maximal knowledge, but each of its subsystems is described by the *maximally mixed state* $\rho_A = \rho_B = \frac{1}{2}\mathbb{1}$, which describes a completely unknown state. We will refer to pure states with this property as *maximally entangled* or *EPR* states. Later, Bell [4] brought out the conflict between local realistic theories and quantum mechanics. As we will see, entanglement is a crucial ingredient in many quantum information protocols. Such is the relevance of entanglement that a great part of the current research efforts in the field of quantum information theory are devoted to the characterization and quantification of entanglement. In particular, this entails: A) Finding criteria to determine whether a state is separable or entangled. In the later case, determine also if the entanglement is distillable or not, i.e. if it can be transformed into singlet states, which are the "fuel" for many quantum information protocols. B) Find measures of entanglement. Entanglement is a new sort of quantum information that cannot be embodied in a single qubit. The basic unit of entanglement is the singlet $|\psi^-\rangle$ introduced in Eq. (10). For an increasing number of subsystems (also called *parties*) new sorts of quantum

[5] For infinite dimensional Hilbert spaces this definition has to be slightly modified [136].

[6] Throughout this work I will use the notation $|\phi\varphi\rangle \equiv |\phi\rangle|\varphi\rangle \equiv |\phi\rangle \otimes |\varphi\rangle$.

correlations appear that cannot be reduced to bipartite entanglement. New basic units of quantum information are therefore expected to appear.

In this work entanglement will mostly appear in bipartite systems. For such systems it is very useful to exploit (see papers III and IV) the isomorphism between the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and the Hilbert space spanned by the complex $d_A \times d_B$ matrices. A general vector in $\mathcal{H}_A \otimes \mathcal{H}_B$, $|\Psi\rangle = \sum_{i,j=1}^{d_A,d_B} C_{ij}|i\rangle|j\rangle$, corresponds to a matrix C with matrix elements C_{ij}, and the inner product is accordingly defined as $\langle C|C'\rangle = \mathrm{Tr}(C^\dagger C')$.

> Throughout this work I will make use of this isomorphism and use the *notation* $|C\rangle$ for any matrix C to denote the bipartite pure state $|C\rangle = \sum_{i,j=1}^{d_A,d_B} C_{ij}|i\rangle|j\rangle$.

Some useful relations between both representations are

$$A \otimes B|C\rangle = |ACB^T\rangle, \tag{11}$$

$$\mathrm{Tr}_A(|A\rangle\langle B|) = AB^\dagger \text{ and } \mathrm{Tr}_B(|A\rangle\langle B|) = A^T B^*. \tag{12}$$

The matrix representation allows one to import many tools and theorems from matrix analysis theory [67, 14] for the analysis of bipartite quantum systems. For instance, the SVD (**S**ingular **V**alue **D**ecomposition) provides a canonical form of writing a general bipartite pure state from where all the non-local properties can be easily read:

> Every pure state $|\Psi\rangle$ in $\mathcal{H}_A \otimes \mathcal{H}_B$ has a *Schmidt decomposition* [111], i.e. there exists basis $\{|e_i\rangle\}_{i=1}^{d_A}$ and $\{|\tilde{e}_i\rangle\}_{i=1}^{d_B}$ in $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively such that,
>
> $$|C\rangle = \sum_{i=1}^{n} \sqrt{\lambda_i}|e_i\rangle|\tilde{e}_i\rangle \tag{13}$$
>
> where $n = \min\{d_A, d_B\}$ and the *Schmidt coefficients* $\lambda_1 \geq \ldots \geq \lambda_n \geq 0$ are non-negative real numbers and satisfy $\sum_i \lambda_i = 1$.
> *Proof:* The SVD of a general complex matrix is $C = U\Lambda V^\dagger$, where Λ is a diagonal matrix whose elements are the non–negative square roots of the eigenvalues of $C^\dagger C$ (called singular values) entered in decreasing order, and U and V are unitary matrices which ith columns are the eigenvectors corresponding to the ith eigenvalue of $CC^\dagger$ and $C^\dagger C$ respectively. Making use of the SVD and applying Eq. (11) we arrive to $|C\rangle = |U\Lambda V^\dagger\rangle = U \otimes V^*|\Lambda\rangle$ that leads to the desired result after identifying the new basis $|e_i\rangle = U|i\rangle$ and $|\tilde{e}_i\rangle = V^*|i\rangle$.

From this proof and Eq. (12) one realizes that the Schmidt decomposition of a state $|C\rangle_{AB}$ is determined by the reduced density matrices $\rho_A = CC^\dagger$ and $\rho_B = C^T C^*$ of the subsystems. The Schmidt coefficients λ_i's are their eigenvalues and $\{|e_i\rangle\}_{i=1}^{d_A}$ and $\{|\tilde{e}_i\rangle\}_{i=1}^{d_B}$ are the basis that diagonalize them respectively. In the case of degenerate eigenvalues, as in (10), there is ambiguity on the local basis used to find the Schmidt decomposition. In any case, what is important is that all the non-local properties of a state come into view thanks to the Schmidt decomposition. The Schmidt decomposition formalizes the relation between the entanglement of a pure bipartite state and the mixedness of its reduced density matrices. According to the previous definition, a state is entangled iff the number of non-vanishing Schmidt coefficients, the *Schmidt rank*, is bigger than one. This is equivalent to saying that the subsystems are in a mixed state. For a maximally entangled state, the subsystems are found to be in a maximally mixed state. In fact, the degree of mixedness of this density matrix, given by the von Neumann entropy, is a valid measure of entanglement and hence also called *entropy of entanglement* of the bipartite state.

A *purification* of a mixed state ρ_A is said to be the bipartite pure state $|\Psi\rangle_{AB}$ such that by tracing out the auxiliary system B we obtain the mixed state ρ_A. The Schmidt rank gives the minimal dimension of the purification's subsystems.

An extension of the notion of Schmidt rank of bipartite pure states to density matrices is the *Schmidt number* [132]. A density matrix ρ has Schmidt number k if *i)* for any realization of $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$ at least one of the states $|\varphi_i\rangle$ has Schmidt rank k and *ii)* there exists a realization with all vectors $\{|\varphi_i\rangle\}$ with Schmidt rank at most k. As the Schmidt rank, the Schmidt number has the property that it cannot increase under LOCC and serves to induce a gross classification of density matrices. However, for mixed states, it is clear that the mixedness of the subsystems does not serve as an indicator of the quantum correlations and separability criteria are then usually based on how the states transform under certain maps (see next section).

2.2 Quantum Operations and Measurements

In the previous section I introduced the density operator as the most general way to describe a quantum state. In this section we will study how quantum systems evolve. Of course, this whole description only makes sense when we have the means to get to know those states, and in quantum mechanics this is known to be a non-trivial task. Thus, the density matrix and evolution

formalism has to go hand in hand with a formalization of the measurement process.

Postulates two to six of quantum mechanics (see e.g. [41]) give us quite a primitive toolbox to describe the dynamics of quantum states. For completeness I summarize it as follows.

1. Measurement (Postulates 2-5). Every measurable physical quantity is associated to a Hermitian operator A. The result of measuring the observable A on $|\varphi\rangle$ can only produce one of the eigenvalues a_i of A with probability,

$$p(i|\varphi) = |\Pi_i|\varphi\rangle|^2 \quad \text{where} \quad A = \sum_{i=1}^{d} a_i \Pi_i, \tag{14}$$

   and Π_i is the projector associated to the outcome a_i, and satisfy $\Pi_i \Pi_j = \delta_{ij}\Pi_i$ and $\sum_{i=1}^{d} \Pi_i = \mathbb{1}$. After the measurement is performed the state of the system collapses to the state

$$|\varphi_i\rangle = \frac{\Pi_i|\varphi\rangle}{|\Pi_i|\varphi\rangle|}. \tag{15}$$

2. Unitary evolution (Postulate 6). The evolution of a closed system is given by Schrödinger's equation $i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\varphi(t)\rangle = H(t)|\varphi(t)\rangle$. The evolution is therefore always *unitary*,

$$|\varphi(t)\rangle = U|\varphi(0)\rangle. \tag{16}$$

The measurement expressed in the first postulates (14) is usually known as *von Neumann* or *projective measurement*. As indicated by the limitation on the number of measurement outcomes to the dimension d of the Hilbert space, the notion of projective measurement is too restrictive. In general *a quantum measurement is any physical process on a state that generates a probability distribution for some outcomes*[7]. Equation (14) captures the essence of a quantum measurement: it gives a mapping between an initial state and a positive number that is the probability of obtaining the measurement outcome represented by the projector Π_i. In a similar way, a *generalized measurement* is defined by a set of positive operators $\{E_i\}_{i=1}^{n}$

[7] See [24] for an introduction to mathematical and conceptual aspects of quantum measurement

that satisfy the completeness relation $\sum_{i=1}^{n} E_i = \mathbb{1}$. These conditions are enough to guarantee that the mapping

$$p(i|\rho) = \mathrm{Tr}(\rho E_i) \tag{17}$$

defines a probability distribution, i.e. $0 \leq p_i \leq 1$ and $\sum_{i=1}^{n} p_i = 1$, for all possible input states ρ. A generalized measurement is therefore characterized by the set of¡ operators $\{E_i\}_{i=1}^{n}$ called *POVM* (**P**ositive **O**perator-**V**alued **M**easure). For every measurement outcome there is a *POVM-element* E_i that gives the probability of this outcome for every input state. POVM's are as fundamental as von Neumann measurements: their appearance in quantum mechanics is postulated. However, *Neumark's theorem* [101, 111] lets one reduce the former from the latter.

> Any POVM $\{E_i\}_{i=1}^{n}$ on a Hilbert space $\mathcal{H}$ can be realized by performing a von Neumann measurement on an extended Hilbert space $\mathcal{H} \oplus \mathcal{H}'$.

In the context of quantum information, however, one usually deals with systems of qubits, hence the direct sum extension of the Hilbert space does not appear naturally. To provide an extended Hilbert space one usually has to add, as shown in Figure 1, an auxiliary system —rather politically incorrectly referred to as *ancilla*[8]. A unitary evolution of the system and ancilla followed by a projection measurement $\{\Pi_i\}_{i=1}^{n}$ on the ancilla leads to the following outcome probabilities,

$$\begin{aligned} p(i|\rho) &= \mathrm{Tr}[U(\rho \otimes \sigma)U^\dagger(\mathbb{1} \otimes \Pi_i)] = \mathrm{Tr}[(\rho \otimes \mathbb{1})(\mathbb{1} \otimes \sigma)U^\dagger(\mathbb{1} \otimes \Pi_i)U] \\ &= \mathrm{Tr}_s \left[\rho \, \mathrm{Tr}_{\mathrm{anc}}[(\mathbb{1} \otimes \sigma)U^\dagger(\mathbb{1} \otimes \Pi_i)U]\right]. \end{aligned} \tag{18}$$

where in the first equality we have used the cyclic property of the trace and last equality can be reached by writing the total trace in a separable basis, i.e. as the partial traces of the system and ancilla. Comparing (18) with the definition in (17), we find that every outcome Π_i of the projective measurement on the ancilla is associated to a POVM element E_i over the system state ρ,

$$E_i \equiv \mathrm{Tr}_{\mathrm{anc}} \left((\mathbb{1} \otimes \sigma)U^\dagger(\mathbb{1} \otimes \Pi_i)U\right). \tag{19}$$

It is straightforward to check the positivity and completeness relation of this POVM. With this we have shown that the unitary coupling of the

[8] In latin, a female slave.

system to the ancilla followed by a projection measurement $\{\Pi_i\}_{i=1}^n$ on the ancilla leads to a POVM $\{E_i\}_{i=1}^n$ on the input state ρ. The reverse can also be shown to be true: for every POVM we can always find an ancilla state σ and a unitary operator U that realizes it in the prescribed way [82, 105].

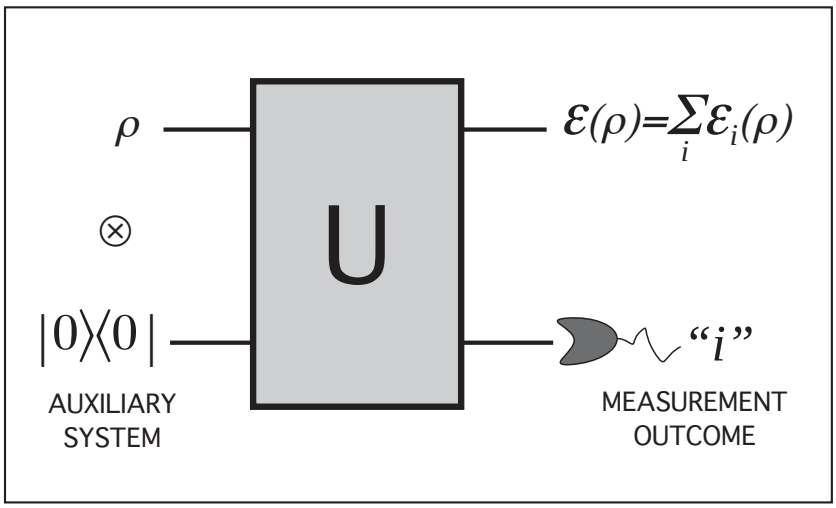

Figure 1: Any generalized measurement or quantum operation (see below) can be realized by unitarily coupling the system to an auxiliary system and performing projection measurements on the the auxiliary system.

Equations (15, 16) in the postulates of quantum mechanics give us a mapping between the states before and after the measurement and the free evolution. We can now try to generalize the idea of state transformations to arrive to the notion of *quantum operation*. We want to find the most general form of the map $\mathcal{E}$ that takes an input state ρ to an output state $\rho' = \mathcal{E}(\rho)$, where input and output Hilbert spaces do not have to be necessarily the same. This map has to send density matrices to density matrices. This implies that,

0) $\mathcal{E}(\rho)$ preserves positivity: $\rho \geq 0 \Rightarrow \mathcal{E}(\rho) \geq 0$

1)* $\mathcal{E}(\rho)$ is trace preserving: $\mathrm{Tr}\rho = 1 \Rightarrow \mathrm{Tr}(\mathcal{E}(\rho)) = 1$

In order to cope with non-deterministic dynamics, we can relax condition *1*)* to *1)* $\mathrm{Tr}(\mathcal{E}(\rho)) \leq 1$, and adopt the convention that $\mathrm{Tr}(\mathcal{E}(\rho))$ is the probability of the particular process $\mathcal{E}$ occurring for an initial state ρ, so

that the properly normalized output state is $\rho' = \frac{\mathcal{E}(\rho)}{\mathrm{Tr}(\mathcal{E}(\rho))}$. For deterministic dynamics condition *1*)* still applies.

Consistent with the ensemble interpretation of a density matrix we also demand that if a system is either in state ρ_0 with probability p or in state ρ_1 with probability $(1-p)$, then the output state should be either in $\mathcal{E}(\rho_0)$ or $\mathcal{E}(\rho_1)$ with the same probabilities. This means that a quantum operation has to be linear on the set of density matrices,

2) $\mathcal{E}(\sum_i p_i \rho_i) = \sum_i p_i \mathcal{E}(\rho_i)$.

The last condition we will impose on quantum operations is that any extension to a larger Hilbert space has to be a positive map.

3) $\mathcal{E}(\rho)$ is *completely positive*: $\rho_{AB} \geq 0 \Rightarrow (\mathcal{I}_A \otimes \mathcal{E}_B)\rho_{AB} \geq 0$,

where $\mathcal{I}_A$ is the identity map on subsystem A. This requirement is based on the very natural idea that if for some reason the system under study is part of a larger system, then the total state of the system should still be a density matrix after the operation. This looks like a physically sound and innocuous extension of condition *0)*, but it turns out to be one of key concepts in quantum information. Positive maps that are not completely positive transform separable states into positive density matrices. It is only for entangled states that these maps may render unphysical outcomes, i.e. not density operators. A composite system in a separable state will remain physical no matter what local transformations we do on each of its parts. Each part is independent of the other —even their time arrows are uncorrelated. However, if we apply time-reversal[9] or inversion to *only one* subsystem of, say, a singlet state, then the total system becomes unphysical. Hence, time–reversal and inversion, as all the positive but not completely positive maps, can be used to identify entangled states. The *partial transposition* defined as

$$\rho = \sum_{i,j,\mu,\nu} \rho_{j\nu,i\mu} |j\nu\rangle\langle i\mu| \text{ on } \mathcal{H}_A \otimes \mathcal{H}_B \xrightarrow{T_A} \rho^{T_A} = \sum_{i,j,\mu,\nu} \rho_{i\nu,j\mu} |j\nu\rangle\langle i\mu|, \quad (20)$$

is another positive, but not completely positive, map. The positivity of the partial transposition (PPT) [109, 68] provides a necessary condition for the separability of *any* composite system (in a pure or mixed state!) that can be easily checked. The Horodecki family proved in [68] that a state is separable if and only if *for any* positive map Δ, $\mathbb{1} \otimes \Delta\rho \geq 0$ holds.

[9]For definition see for example [111] page 258.

Unluckily, we do not have a full characterization of the set of positive maps. However, for 2×2 and 2×3 bipartite systems we know that all the positive maps can be written in terms of completely positive maps and the partial transposition, so that effectively the PPT (also called the Peres-Horodecki criterion) becomes a necessary and sufficient condition for a state to be separable.

After pointing out the relevance of completely positive maps in quantum information, we will finally see that the extension of condition *0)* to *3)* has important implications in our program of finding the most general quantum operation. The *Kraus representation theorem* [82] states that a map $\mathcal{E}(\rho)$ fulfills conditions *1), 2)* and *3) if and only if* it has an *operator–sum representation* (or *Kraus representation*) given by,

$$\mathcal{E}(\rho) = \sum_{i=1}^{m} A_i \rho A_i^\dagger \text{ where } \sum_{i=1}^{m} A_i^\dagger A_i \leq \mathbb{1}. \tag{21}$$

The equality holds only for deterministic operations, and A_i are the so-called *Kraus operators*. The proof of this theorem (see [121] for an enlightening version) strongly relies on *3)* superseding *0)*: there is no similar characterization theorem for positive maps. The operator–sum representation is a very important tool in quantum information to study the viability or optimality of different quantum information processing tasks without detour on the actual physical operations. However, it is reassuring to know that, once we find the best fitted quantum operation for our purpose, it is always possible to implement it by coupling our system to an auxiliary system as in Figure 1. Let us suppose that our system and ancilla are initially[10] in a state $\rho\otimes|0\rangle\langle0|$ on $\mathcal{H}_s\otimes\mathcal{H}_{aux}$ and that we couple them through a unitary interaction defined by U resulting in the state $U\rho\otimes|0\rangle\langle0|U^\dagger$. The transformation of our initial system can be obtained by tracing out, i.e. doing the partial trace over, the auxiliary system:

$$\mathcal{E}(\rho) = \mathrm{Tr}_{aux}(U\rho\otimes|0\rangle\langle0|U^\dagger) = \sum_{i=i}^{d_{aux}} \langle e_i|U\rho\otimes|0\rangle\langle0|U^\dagger|e_i\rangle \tag{22}$$

$$= \sum_{i=1}^{d_{aux}} A_i\rho A_i^\dagger \text{ where } A_i \equiv \langle e_i|U|0\rangle. \tag{23}$$

This coincides with the axiomatic characterization of a deterministic quantum operation in Eq. (21) since $\sum_{i=1}^{n} A_i^\dagger A_i = \sum_{i=1}^{n}\langle0|U^\dagger|e_i\rangle\langle e_i|U|0\rangle = \mathbb{1}$. It

[10]For simplicity we assume that the ancilla has been prepared in a pure state. Linearity makes the extension to mixed ancilla states straightforward.

can be proven that for any quantum operation one can find an auxiliary system and a unitary operation that realize that quantum operation[82, 105]. Referring to Eq. (23), notice that we can interpret each term in the sum as the unnormalized state of the system after performing a projective measurement on the ancilla and obtaining the outcome associated to the projector $\Pi_i = |e_i\rangle\langle e_i|$,

$$\mathcal{E}_i(\rho) = A_i \rho A_i^\dagger. \tag{24}$$

Each Kraus operator A_i is associated to a measurement outcome and maps the initial state to the state of the system after the measurement. Moreover, by definition the norm of the resulting state is the probability of the process $\mathcal{E}_i$ to occur,

$$p(i|\rho) = \mathrm{Tr}(\mathcal{E}_i(\rho)) = \mathrm{Tr}(A_i^\dagger, A_i \rho) = \mathrm{Tr}(E_i \rho) \tag{25}$$

where the operator $E_i = A_i^\dagger A_i$ has all the ingredients to be considered as a POVM element. Thus, to no surprise, we see that quantum operations also formalize the most general measurement process. In many situations the state after the measurement will be irrelevant to the problem and it will pay off in simplicity to use POVM formalism described above.

Had we taken in Eq. (23) the partial trace using another base for the ancilla Hilbert space $\{|f_i\rangle = V^\dagger |e_i\rangle\}$, the quantum operation would obviously remain untouched, but the operator-sum representation will be given by the Kraus operators,

$$\tilde{A}_i = \langle f_i|U|0\rangle = \sum_{j=1}^{m} V_{ij} A_j \text{ where } V \text{ is unitary.} \tag{26}$$

Each new Kraus operator $\tilde{A}_i$ corresponds to the measurement outcome $|f_i\rangle\langle f_i|$. It turns out that all the *equivalent operator-sum representations*, i.e. those that lead to the same quantum operation, satisfy the above relation between its Kraus operators. The similarity of the previous equation to Eq. (4) describing the relation between different realizations of a density matrix is not casual: the state after the coupling unitary transformation corresponds to a purification of $\mathcal{E}(\rho)$ and each different measurement on the ancilla leads to a different ensemble interpretation. A simple parameter count shows that maximum number of Kraus operators needed to characterize a quantum operation acting on a d_s-dimensional system is at most $m \leq d_s^2$.

Despite the Kraus representation gives an explicit characterization of the physical operations that one can do on a quantum system, there are

still a lot of open questions surrounding quantum operations. For example, it would be very convenient to derive simple criteria to determine whether or not particular state transformations are possible, or to have a characterization of constraint quantum operations such as local operations, local operations with classical communication or operations implementable by linear elements (see 3.2.2). There has been some progress in this direction using information-theoretical criteria. The theory of majorization [102] has also been proven to be of great use in characterizing pure state transformations.

Quantum operations are in general irreversible —unitary evolution is the only exception. Decoherence, or the coupling to uncontrolled degrees of freedom, fixes the arrow of time. This means that quantum operations do not define a group but a semigroup: the consecutive application of quantum operations is a quantum operation. The continuos evolution of *open systems* (systems which are coupled to an environment) has been conventionally described by a master equation for the density operator, where one includes all sorts of non-unitary effects such as damping, decoherence, and noisy driving fields. Starting from complete positivity and linearity axioms Lindblad [92] gave the general form for a Markovian semigroup master equation,

$$\dot{\rho} = -i[H, \rho] + \sum_{i=1} 2L_i \rho L_i^\dagger - L_i^\dagger L_i \rho - \rho L_i^\dagger L_i, \tag{27}$$

where L_i are called Lindblad operators. Usually, the presence of the non-reversible terms was postulated on phenomenological grounds. Solving the master equation required the use of numerical methods that basically "unraveled" the master equation for the density matrix into stochastic trajectories of state vectors [34]. The appearance of these stochastic equations called for a physical interpretation of their origin. As in the case of the "discrete" quantum operations, it turns out that a given master equation can have many different interpretations, each of them with a physical meaning. Recognizing this became of crucial importance when experimental physics (specially in the field of quantum optics) allowed one to monitor the state of the environment and therefore condition the state of the system to the measurement outcomes. For example, homodyne and heterodyne measurements of the light leaking to the environment from a quantum optical system have been seen [142, 141] to induce dynamics on the system —or, to be more legitimate, on our description of the system—associated with two different continuous state-diffusion stochastic equations [34, 58], while a direct photon-counting measurements induces a quantum-jump stochastic

equation. Based on these accurate descriptions of the conditional dynamics several feedback mechanisms have been modelled and found to result in non-trivial, and sometimes useful, manipulations of the optical system.

Despite the claimed generality of the quantum operations and Lindblad master equation (27) it is important to bear in mind their working conditions. A typical situation which leads to dynamics that cannot be described by quantum operations is when the system is initially entangled with the environment. This is somehow natural, since one can use the environment to gain information on the input and use this information to perform any kind of operation on it. For example, if by measuring the environment we can know whether the input state is in the upper or lower hemisphere of the Bloch-sphere we can invert the Bloch-vector of any input state by applying simple rotations. However, it is well known that the inversion is an anti-unitary operation which is a positive but not a completely positive operation (see Section 2.3.2). Of course, in the scenario where one can obtain a complete knowledge on the input state from the environment, one can use this information to create the most bizarre map, including non-linear maps. In some intrinsically non-linear systems[11] it is possible to find dynamics which are not completely positive but do not lead to negative probabilities [42].

The master equation (27) is only valid when the condition of no initial correlations with the environment is fulfilled at every time-step. If the system interacts with the environment at a given time (letting some information out), then it cannot interact with that "part" of the environment again[12] (the lost information cannot enter the system at future times). This is the content of the Markovian approximation. Royer [115] showed that for some cases it is still possible to treat consistently and obtain useful results while properly accounting for initial correlations. See also paper IV [30] for a simple treatable example of non-Markovian dynamics.

2.3 Applications

In the first section I gave a quick introduction on what are the quantum information carriers (quantum states) and how we can manipulate them (quantum operations). In this section, I will review some basic protocols in quantum information that illustrate how these ideas can give rise to

[11] Typically systems in which a full microscopic account is replaced by a mean field theory, where the dynamics is described by a non-linear evolution of a single quantum object, the mean field.

[12] This implies that the environment has to have "infinite" degrees of freedom.

striking applications that motivate the research presented in this work. These applications are interesting by themselves and, equally important, they provide a phenomenology that helps to develop new intuitions on quantum information.

2.3.1 State Discrimination and Optimal State Estimation

Imagine the scenario in which Alice secretly prepares a quantum system in one of the states $\{\rho_i\}_{i=1}^n$ according to the *a priori* probability distribution $\{p_i\}_{i=1}^n$. Now it is the task of an observer, Bob, to make the "best" measurement in order to establish the identity of the state. In general Bob will not be able to unambiguously identify each of the possible states, thus the notion of "best" measurement will strongly depend on what exactly Bob has to say about the state. Here we will consider three cases: *quantum hypothesis testing* where Bob is forced to make a guess on the input state after each measurement outcome, *unambiguous state discrimination* where Bob has the right to admit that he has no clue about the identity of the state for some given measurement outcomes, and the *maximization of the information gained* in the detection process.

Quantum hypothesis testing is one of the central problems in quantum detection theory advanced in the 1960s by Helstrom [64], and was part of the initial motivation to develop the theory of quantum operations and generalized measurements. In this problem, Bob has to guess the state prepared by Alice, based on the result of his experiment and with the minimal probability of error[13]. Bob's strategy can be easily formalized by a POVM $\{E_j\}$ with n elements, where the outcome E_j is taken to correspond to the guessed state ρ_j. The probability of error of this strategy is,

$$P_e = 1 - P_s = 1 - \sum_{j=1}^{n} p_j p(j|\rho_j) = 1 - \sum_{j=1}^{n} p_j \mathrm{Tr}(E_j \rho_j). \tag{28}$$

If the initial set of states is linearly independent it is always possible for Bob to find a von Neumann measurement which is optimal [76, 64]. For a set of two linearly independent states, which can be conveniently written as

$$|\varphi_\pm\rangle = \cos\theta|+\rangle \pm \sin\theta|-\rangle, \tag{29}$$

[13] *Quantum Bayes* [64] strategies are a very well studied extension of this idea in which different errors can have different costs. Bob's goal is to minimize the cost function $c = \sum_{ij} p_i C_{ij} p(E_j|\rho_i)$ for a given cost matrix C.

occurring with *a priori* probabilities p_+ and $p_- = 1 - p_+$, Helstrom [64] found the optimum value of the probability of error,

$$P_e^{opt} = \frac{1}{2}(1 - \sqrt{1 - 4p_+p_-|\langle\varphi_+|\varphi_-\rangle|^2}). \tag{30}$$

Figure 2 shows the optimal von Neumann measurement corresponding to the case $p_+ = p_- = \frac{1}{2}$ for which the probability of error reduces to

$$P_e^{opt} = \frac{1}{2}(1 - \sin 2\theta). \tag{31}$$

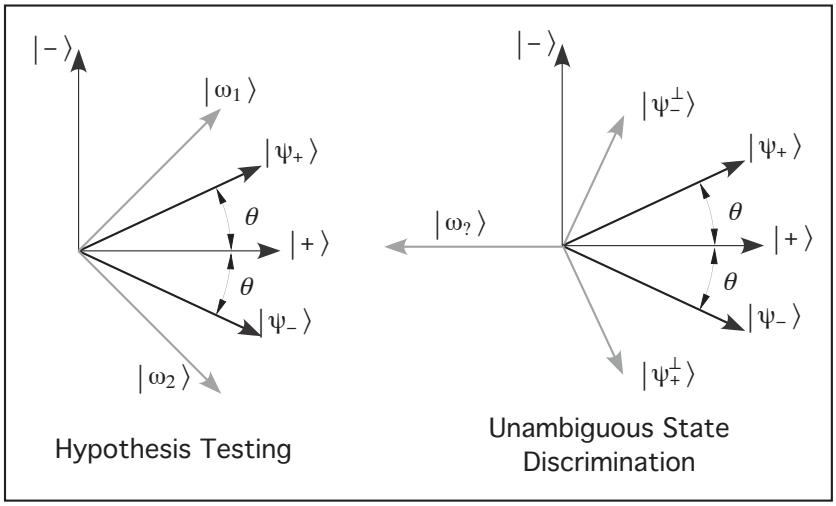

Figure 2: Optimal measurements for quantum hypothesis testing and unambiguous state discrimination for two non-orthogonal states in the real plane. The vectors in black represent the input states while the gray ones represent the projection directions of the optimal POVMs.

For a linearly dependent set of states, von Neumann measurements are not optimal and one has to minimize over all possible POVMs of n elements, which is a difficult task to do analytically. There is, however, an important class of ensembles for which one can find a general analytic solution, namely the sets of equiprobable and *symmetric* states. A set of states $\{|\varphi_j\rangle\}_{j=1}^n$ is said to be symmetric if there exists a unitary transformation U such that,

$$|\varphi_j\rangle = U^{j-1}|\varphi_1\rangle \text{ and } |\varphi_1\rangle = U|\varphi_n\rangle. \tag{32}$$

The optimal strategy for this particular type of sets consists in doing a *square root measurement* defined by the POVM elements,

$$E_j = \Phi^{-\frac{1}{2}} |\varphi_j\rangle\langle\varphi_j| \Phi^{-\frac{1}{2}} \tag{33}$$

where $\Phi = \sum_{j=1}^{n} |\varphi_j\rangle\langle\varphi_j|$. The probability of error of this optimal measurement is,

$$P_e^{opt} = 1 - \frac{1}{n} \sum_{j=1}^{n} |\langle\varphi_j| \Phi^{-\frac{1}{2}} |\varphi_j\rangle|^2. \tag{34}$$

The two-state set from Figure 2 is the simplest example of symmetric states. A non-trivial example is the symmetric set of three real states, the *trine*, which is relevant in some quantum cryptography protocols.

Unambiguous state discrimination puts the very strong demand on Bob of not permitting him any errors. All of Bob's uncertainty has to be shifted to a single measurement event associated to the POVM element $E_?$. Whenever the measurement gives this outcome, Bob says 'don't know', and in all the other cases he has to make the right guess with certainty. The figure of merit that Bob needs to minimize is the total probability of an inconclusive answer $P_? = \mathrm{Tr}(\rho E_?)$, where ρ describes the ensemble $\{p_i, |\varphi_i\rangle\}$. The *error-free* condition puts very tight restrictions on the POVM elements: $p(j|\varphi_i) = \mathrm{Tr}(\rho_i E_j) \propto \delta_{ij}$ implies that the POVM corresponding to the guess $|\varphi_j\rangle$ has to be proportional to the projector on the space orthogonal to all the other states $\{|\varphi_i\rangle\}_{i \neq j}$. It immediately follows that linearly dependent states cannot be unambiguously discriminated. In [38] Chefles proved that linear independence is also a sufficient condition for unambiguous state discrimination. The strategy for two linearly independent states, defined as in Eq. (29), follows from the error-free condition,

$$E_\pm = \frac{\gamma_\pm}{|\langle\varphi_\pm^\perp|\varphi_\mp\rangle|^2} |\varphi_\pm^\perp\rangle\langle\varphi_\pm^\perp| \text{ and } E_? = \mathbb{1} - E_+ - E_-, \tag{35}$$

where $|\varphi_\pm^\perp\rangle = \sin\theta|+\rangle \mp \cos\theta|-\rangle$ are orthogonal to $|\varphi_\pm\rangle$ and the coefficients in front of the projectors are defined so that $\gamma_\pm$ is the probability of successful discrimination conditional to the initial state being in $|\varphi_\pm\rangle$. The optimum strategy can be easily obtained by minimizing the probability of the inconclusive result $P_? = 1 - p_+\gamma_+ - p_-\gamma_-$ subject to the positivity condition $E_? \geq 0$ [73]. This was first solved [72, 108, 47] for equiprobable states ($p_+ = p_-$) resulting in an optimum inconclusive result probability,

$$P_? = |\langle\varphi_+|\varphi_-\rangle| = \cos 2\theta. \tag{36}$$

A measurement corresponding to the optimal POVM is shown in Figure 2. Notice, that after the inconclusive result both input states are mapped to the state $|+\rangle$, rendering useless any further attempts to discriminate the states. In fact, it can be shown that an inconclusive answer in optimal unambiguous state discrimination always maps the set of input states to a linearly dependent set [38]. While this implies the impossibility of any further error-free discrimination, it is still possible in many cases to get information about the input state at the price of producing some errors.

As for quantum hypothesis testing, analytical solutions for more than two states have only been found for the case of equiprobable and symmetric states [39]. A set of linearly independent states satisfying Eq. (32) can always be written as,

$$|\varphi_j\rangle = \sum_{k=1}^{n} c_k \exp\left(\frac{i2\pi jk}{n}\right)|k\rangle \tag{37}$$

where $|k\rangle$ are the eigenstates of the symmetry transformation U in Eq. (32). The minimum value for the inconclusive result probability is given by,

$$P_?^{opt} = n \min_k |c_k|^2. \tag{38}$$

A different approach was taken by Peres and Terno [110] who solved the problem of optimal unambiguous state discrimination for three arbitrary pure states with arbitrary *a priori* probabilities, and gave the recipe to solve, at least numerically, the generalization to more than three states.

Quantum hypothesis testing and unambiguous state discrimination apply to the scenario in which Bob tries to guess the state forwarded by Alice after each measurement, and his aim is to maximize the number of correct guesses. Another approach, typically adopted by information theorists, is to maximize the information gained during the measurement. We already saw that if the probabilities of a set of states $\{|\varphi_i\rangle\}$ are $\{p_i\}$, the corresponding classical information is quantified by the Shannon entropy $H(\vec{p})$ from Eq. (1). Getting a measurement outcome modifies the *a priori* probability distribution $\vec{p} \to \vec{p'}$. The amount of information gained from the measurement is the amount by which the entropy is reduced $\Delta I' = H(\vec{p}) - H(\vec{p'})$. Since different measurement outcomes will provide more information than others, Bob's goal will be to find the POVM $\{E_j\}_{k=1}^{m}$ that maximizes the

average information gain[14],

$$\Delta I = \sum_{k=1}^{m} P_k \left(\sum_{i=1}^{n} p_i \log_2 p_i - \sum_{i=1}^{n} p(i|k) \log_2 p(i|k) \right) \tag{39}$$

where $P_k = \sum_{i=1}^{n} p_i \mathrm{Tr}(E_k|\varphi_i\rangle\langle\varphi_i|)$ is the *a priori* probability of getting the outcome E_k, and $p(i|k)$ is the probability of having the state $|\varphi_i\rangle$ given the measurement outcome E_k. This conditional probability can be obtained from *Bayes' rule*,

$$p(i|k) = \frac{p_i p(k|i)}{P_k} = \frac{p_i \mathrm{Tr}(E_k|\varphi_i\rangle\langle\varphi_i|)}{\sum_{j=1}^{n} p_j \mathrm{Tr}(E_k|\varphi_j\rangle\langle\varphi_j|)}. \tag{40}$$

Note that the number of POVM elements, m, is not fixed by the number of possible states n. This, together with the fact that the average information gain is not linear, makes the problem even more difficult to treat analytically than for the previous strategies. However there are some general results worth mentioning,

- *Holevo bound* [65] on the accessible information:

$$\Delta I = H(X:Y) \leq S(\sum_i p_i \rho_i) - \sum_i p_i S(\rho_i) \tag{41}$$

  where $S(\rho)$ is the von Neumann entropy defined in Eq. (5) and equality holds when the states prepared by Alice ρ_i commute. An immediate implication is that one can transmit at most *one bit per qubit*.

- Davies' theorems [43]: *1)* The information gain can always be maximized by a POVM with m POVM elements of rank one, $d \leq m \leq d^2$, $E_i = |v_k\rangle\langle v_k|$ where $\langle v_k|v_k\rangle \leq 1$ and d is the dimension of the input Hilbert space. POVMs of this kind represent the so-called *sharp measurements*[15].
  2) If the states in the input set are equiprobable, and the set is covariant with respect to a group G with an irreducible representation $\pi_g(\rho)$ on the input space, then there exists a normalized state $|\varphi\rangle$ such that the optimal POVM is covariant and given by $E_g = \frac{d}{n}\pi_g^\dagger(|\varphi\rangle\langle\varphi|)$. This result has been extended to groups that do not act irreducibly on the whole input space [118].

[14]The average information gain is also known as the *mutual information* $H(X:Y)$ between the input signals $X = \{p_i, |\varphi_i\rangle\}$ and the detection signals $Y = \{P_k, E_k\}$, and its maximum over all possible POVM is called *accessible information*.

[15]Some authors use differently this term to denote measurements where each measurement outcome can be triggered with unit probability by choosing the appropiate input state.

- Two states: this case has the peculiarity that the POVM which maximizes the average information gain coincides with the von Neumann measurement which achieves the minimum error probability in quantum hypothesis testing, and the average information gain obtained is,

$$\Delta I_{\text{opt}} = \frac{1}{2}\left((1-\sin 2\theta)\log_2(1-\sin 2\theta) + (1+\sin 2\theta)\log_2(1+\sin 2\theta)\right).$$

The average information gained in optimal unambiguous state discrimination is equal to the gain corresponding to the successful discrimination events (the inconclusive results do not provide any information) $\Delta I_{\text{USD}} = 1 - P_? = 1 - \cos 2\theta$, which is lower than the optimal except for $\theta = \frac{\pi}{4}$. For orthogonal input states, unambiguous state discrimination, optimal information gain, and minimum error probability are achieved by projection measurement onto these states, and the Holevo bound is reached.

To finish, let us consider the scenario in which Alice instead of preparing a state from set of states known to Bob, she gives him a completely arbitrary pure state. So, effectively Bob has to discriminate a state from an infinite set of states with a flat *a priori* probability distribution. In this scenario there is no place for unambiguous state discrimination, asthe set of states is obviously linearly dependent. On the other hand, in any realistic situation the number of measurement outcomes is finite, so that one can not associate a measurement outcome to every possible input state as required in quantum hypothesis testing. There are a couple of more natural strategies to adopt here. One is to maximize the average information gain. The other one is to perform *quantum state estimation*, which I introduce here. The high-symmetry of the problem makes it possible to find analytic solutions, and even to investigate the more interesting case where Alice provides Bob with N copies of the same state. Bob's ensemble is $\{p_i, \rho_i \otimes \overset{N}{\ldots} \otimes \rho_i\}$ and for increasing N he will get closer to a *full* knowledge of the state ρ_i chosen by Alice.

Quantum state estimation was put forward by Massar and Popescu [96] formulated as a game[16]. Alice gives the unknown state $|\varphi\rangle$ to Bob who performs a POVM $\{E_i\}_{j=1}^k$ on it. For each measurement outcome he will propose a state $|\phi_j\rangle$ as his guess. Alice will then compare Bob's guess with the original state, using a previously agreed distinguishability measure $d(|\phi_j\rangle, |\varphi\rangle)$. According to this measure Bob will get more points the more

[16] See also [66].

indistinguishable his guess to the original state is. Bob's goal is to find the strategy that gives him on average the highest score, which is given by,

$$\bar{F} = \sum_{j=1}^{k} \int \mathcal{D}|\varphi\rangle p(j|\varphi) d(|\phi_j\rangle, |\varphi\rangle). \tag{42}$$

In this context, the most commonly used distinguishability measure is the *quantum fidelity*, which definition and main properties I give below[17].

Quantum Fidelity [74]: Based on the classical statistical overlap measure between two probability distributions $\vec{p} = \{p_i\}$ and $\vec{q} = \{q_i\}$ $F_c(\vec{p}, \vec{q}) = \left(\sum_i \sqrt{p_i q_i}\right)^2$ the quantum fidelity is defined as,

$$F(\rho, \sigma) = \left(\min_{\{E_i\}} \sum_i \sqrt{\mathrm{Tr}(\rho E_i)\mathrm{Tr}(\sigma E_i)} \right)^2 \tag{43}$$

where the minimum is taken over all possible POVMs. That is, the quantum fidelity is the classical fidelity of the probability distributions generated by the optimum POVM. An alternative, but equivalent, definition of the quantum fidelity is provided by Uhlmann's theorem:

$$F(\rho, \sigma) = \max_{\phi_\sigma} |\langle \varphi_\rho | \phi_\sigma \rangle|^2, \tag{44}$$

where $|\varphi_\rho\rangle$ and $|\phi_\sigma\rangle$ are purifications of ρ and σ respectively. A closed expression for $F(\rho, \sigma)$ can be found to be,

$$F(\rho, \sigma) = \left(\mathrm{Tr}\left((\sqrt{\rho}\sigma\sqrt{\rho})^{\frac{1}{2}} \right) \right)^2, \tag{45}$$

which is bound by $0 \leq F(\rho, \sigma) \leq 1$, and the lower and upper bound are reached iff the states are orthogonal ($\rho\sigma = 0$) and identical ($\rho = \sigma$) respectively. Some other useful properties of the quantum fidelity are: *i)* Invariance under unitary transformations $F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma)$. *ii)* Symmetry $F(\rho, \sigma) = F(\sigma, \rho)$. *iii)* Concavity $F(\rho, p\sigma_1 + (1-p)\sigma_2) \geq pF(\rho, \sigma_1) + (1-p)F(\rho, \sigma_2)$. *iv)* If one of the states is pure $F(\rho, |\varphi\rangle\langle\varphi|) = \langle\varphi|\rho|\varphi\rangle$ and if both are pure $F(|\varphi\rangle\langle\varphi|, |\phi\rangle\langle\phi|) = |\langle\varphi|\phi\rangle|^2$. *v)* Multiplicativity, $F(\rho \otimes \rho', \sigma \otimes \sigma') = F(\rho, \sigma)F(\rho', \sigma')$. *vi)* Monotinicity [3] $F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma)$ for *any* trace preserving quantum operation $\mathcal{E}$. Considering the partial trace as a quantum operation we recover Uhlmann's theorem.

[17] For an in depth study of this and other quantum distinguishability measures see [53].

By taking the quantum fidelity as a measure of distinguishability, i.e as the score function $d(|\phi_j\rangle, |\varphi\rangle)$ in Eq. (42), it is straightforward to realize [96] that for a single qubit in an unknown state the optimal average fidelity is $\bar{F}_1 = \frac{2}{3}$ and can be achieved by letting the unknown state go through a Stern-Gerlach apparatus, i.e. performing a von Neumann measurement, and taking the outcome as the guessed state. Massar and Popescu [96] studied what was the change in the fidelity when Alice handed Bob N copies of the unknown state. They found that the upper-bound on the average fidelity that Bob can achieve is given by,

$$\bar{F}_N^{opt} = \frac{N+1}{N+2}. \tag{46}$$

However, they could only give an explicit form of the POVM for $N = 2$, while for $N > 2$ they proposed one with an infinite number of outcomes, thus breaking with the realizable measurements for state estimation. Later, Derka *et al.* [44] gave an algorithm to find the optimal POVM (with finite number of elements) for N copies of an unknown state of arbitrary dimension. The Barcelona group [89, 135] found the *minimal optimal measurement*[18] and the corresponding optimal fidelity for N copies of a state drawn from the set of mixed states $\{f(|\vec{s}|), \rho(\vec{s})\}$, where $\vec{s}$ is the Bloch vector (6) parametrizing each state and $f(|\vec{s}|)$ is an isotropic *a priori* probability distribution (states with the same degree of mixedness are equiprobable). Bob's optimal strategy is affected by the *a priori* probability distribution only in assigning a guess to each measurement outcome: the optimal POVM itself is independent of $f(|\vec{s}|)$. As an example, and for further reference in this work, I give here the optimal minimal measurement for two copies of an unknown qubit. The POVM consists of four rank one projectors of the form

$$E_i = \frac{3}{4}|\vec{n}_i\rangle\langle\vec{n}_i| \otimes |\vec{n}_i\rangle\langle\vec{n}_i| \quad \text{with} \quad i = 1, \ldots, 4 \tag{47}$$

where $|\vec{n}_i\rangle\langle\vec{n}_i|$ are pure states with Bloch vectors $\vec{n}_i$ that point at the four vertices of a tetrahedron. This POVM is a resolution of the identity on the symmetric space of two qubits, which is the space spanned by inputs of the form $|\varphi_s\rangle|\varphi_s\rangle$. If Alice hands out to Bob states of the form $\rho(\vec{s}) \otimes \rho(\vec{s})$ following an isotropic probability distribution $f(|\vec{s}|)$, then the input states span the entire two qubit state space (symmetric and antisymmetric parts) and an extra POVM element $E_5 = |\psi^-\rangle\langle\psi^-|$ has to be added to complete the resolution of the identity $\sum_i E_i = \mathbb{1}$.

[18] POVM that optimizes the score with the minimal number of POVM elements.

By inverting the order of the sum and integration in Eq. (42) we find that the score can be written as

$$\bar{F} = \int \mathcal{D}|\varphi\rangle F_\varphi \text{ where } F_\varphi = \langle\varphi|\rho_e|\varphi\rangle, \text{ and} \tag{48}$$

$$\rho_e = \sum_{j=1}^{k} p(j|\varphi)|\phi_j\rangle\langle\phi_j| \tag{49}$$

is the expected state estimation guess corresponding to the input $|\varphi\rangle$. In state estimation the fidelity of the outcome must not depend on the input chosen by Alice. This implies that the estimated state ρ_e is of the form

$$\rho_e = \frac{1}{2}(1-\eta_e)\mathbb{1} + \eta_e|\varphi\rangle\langle\varphi| = \frac{1}{2}(\mathbb{1} + \eta_e \vec{s}_\varphi \cdot \vec{\sigma}) \tag{50}$$

where $0 \leq \eta_e \leq 1$ and is called *shrinking factor* for obvious reasons, or *Black Cow factor* for not so obvious reasons[19]. The corresponding fidelity is

$$\bar{F} = F_\varphi = \frac{1}{2}(1+\eta_e) \tag{51}$$

which for the optimal strategy results in a shrinking factor given by

$$\eta_e^{opt} = \frac{N}{N+2}. \tag{52}$$

Notice that the shrinking factor approaches one with increasing N, i.e. the average guessed state (defined by $\eta_e\vec{s}$) gets asymptotically close to the unknown input (defined by $\vec{s}$).

2.3.2 Cloning

Non-orthogonal states cannot be cloned. This phrase summarizes one of the fundamental theorems in quantum information. The *no-cloning theorem* [46, 143] states that it is not possible to make an exact copy of an unknown state $|\varphi\rangle$, i.e. there is no quantum operation $\mathcal{E}$ such that $|\varphi\rangle|\Phi\rangle \xrightarrow{\mathcal{E}} |\varphi\rangle|\varphi\rangle$ for a generic "blank" state $|\Phi\rangle$. This is a direct implication of the linearity of quantum operations since the transformation of the basis states $|0\rangle|\Phi\rangle \xrightarrow{\mathcal{E}} |0\rangle|0\rangle$ and $|1\rangle|\Phi\rangle \xrightarrow{\mathcal{E}} |1\rangle|1\rangle$ fixes the transformation of a superposition $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\Phi\rangle \xrightarrow{\mathcal{E}} \frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|1\rangle)$, which is obviously different than

[19] This factor plays an important role in the connection between quantum state estimation and universal cloning (see following section) [23]. This was established by A. Ekert, C. Macchiavello and D. Bruss following discussions at the Black Cow bar.

the desired output $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$. Notice that the cloning transformation can work on some states, as the two states $\{|0\rangle,|1\rangle\}$ above, though the states have to be orthogonal to preserve the norm of the output state.

The *no-broadcasting theorem* extended the result to mixed input states. The class of operations to consider in this case is much wider: $\rho_A \otimes |\Phi\rangle\langle\Phi|_B \xrightarrow{\mathcal{E}} \sigma_{AB}$ with the condition that the reduced density matrices are $\sigma_A = \sigma_B = \rho_A$. Barnum *et al.* [2] proved that such *broadcasting* operation is only possible if the set of input density matrices commute. They showed that the broadcasting operation acting on non-commuting density matrices would imply an increase of quantum fidelity under the partial trace operation, which is in contradiction with the monotinicity property of the quantum fidelity *(vi)* in 2.3.1). The connection between this result and the fact that the Holevo bound on the accessible information can be achieved only for commuting signal states has, to my knowledge, not been established.

The no-go theorems for cloning and broadcasting were not the last words on quantum cloners. In the following years researchers in the field started to investigate the possibilities of producing "not perfect" cloners. It turns out that by relaxing a little the conditions of the ideal cloning machine, it is possible to copy unknown states. This can be done, basically, in two ways. The first one is to allow the cloning machine to provide perfect copies of the unknown state but with a given failure probability. By checking (i.e. measuring) the state of the *probabilistic cloner* [49] after the process, one knows whether the cloning succeeded or not. As for the unambiguous state discrimination[20], the linearity of quantum operations restricts the use of probabilistic cloners to linearly independent sets of input states [48]. In particular a universal cloning machine, which should work over *all* pure states, can never be probabilistic in the sense defined above. However, if we are prepared to reduce the quality of our copies, it is possible to build a deterministic cloning machine that works on the whole set of input states. A *universal cloner* [25] produces, with unit probability, two distorted copies, the quality of which is independent of the input state. There are different criteria to judge how large is this difference or distance between the distorted copies and the perfect ones, but usually all of them lead to the same optimal cloning machine [137]. Imposing universality to the cloner means that the fidelity (quality measure) of the clones should be the same for any

[20]This is not a coincidence: unambiguous state discrimination and probabilistic exact cloning are equivalent in many ways and both can be understood as particular cases of *quantum state separation* [40].

input state $|\varphi\rangle$, which in turn means that each clone ought to be of the form (50): the Bloch vector of the clones has to be a shrunk version of the input Bloch vector. The optimal universal cloning machine [22] minimizes the decrease in the length of the Bloch vector and achieves a shrinking factor of $\eta_c^{opt} = \frac{2}{3}$ which corresponds to the optimum fidelity of $\bar{F}_c = \frac{5}{6}$. This type of quantum operation which uniformly "shrinks" the Bloch sphere is known as *depolarizing channel*[21] and has an operator sum representation defined by the Kraus operators,

$$A_1 = \sqrt{1-p}\mathbb{1},\ A_2 = \sqrt{\frac{p}{3}}\sigma_x,\ A_3 = \sqrt{\frac{p}{3}}\sigma_z,\ A_4 = \sqrt{\frac{p}{3}}\sigma_y. \tag{53}$$

This channel represents the situation in which the system is left untouched with probability $1-p$, while with probability p either a bit-flip error (σ_x) a phase-flip error (σ_z), or a simultaneous phase-flip and bit flip error (σ_y) occurs. The chosen representation is minimal; its Kraus operators are linearly independent and by Eq. (26) we know that any other representation will have at least the same number of Kraus operators. If we want a unitary implementation of this quantum operation we need a four dimensional auxiliary system, for this is the minimum number of Kraus operators. When applied to our cloner we find that universality requires an ancilla qubit: the "blank" qubit can account for two "auxiliary dimensions" and the ancilla qubit has to account for the other two. Moreover, the ancilla qubit will be entangled with the clones for most input states and its final state will depend on the input state—the ancilla contains information on the input state. Thus, in order to comply with the conditions of the universal cloning machine we are forced to let some information leak out of our system. In paper I [21] we show that is possible to do a sharp *effective POVM*[22] on the input system by doing a *joint* measurement on both clones and disregarding the ancilla. As we shall next see, such sharp measurements provide the optimal information gain on the unknown input: we would do equally well by measuring the input state directly, before the cloning transformation. This also means that although there is information in the ancilla, it is redundant with the information we can get from the clones.

[21] The term quantum channel refers to the quantum operations which appear in the context of quantum communication. It does not have further nuances other than the fact that in quantum communication the input and output Hilbert spaces are usually the same.

[22] An *effective* measurement [21] is the one which is realized indirectly on the system after it has undergone a known evolution which can involve an interaction with other systems.

Information gain in isotropic distributions: Davies' theorem already told us that an optimal POVM can always be chosen to be sharp. For isotropic distribution of input states the converse is also true: any sharp measurement is optimal. This can be easily seen by an explicit calculation. A POVM with elements $E_i = a_i(\mathbb{1} + \vec{t}_i \cdot \vec{\sigma})$ will generate the probability distribution $p(i|\vec{s}) = \mathrm{Tr}(E_i \rho_{\vec{s}}) = a_i(1 + \vec{s} \cdot \vec{t}_i)$. Integrating this distribution over all the possible input states we obtain the *a priori* probability for outcome i, $P_i = \int d^3s f(s) p(i|\vec{s}) = a_i$. Using the definition of the average information gain in Eq. (39) and Bayes' rule to calculate the *a posteriori* probability distribution we arrive at

$$\begin{aligned}
\Delta I &= -\int d^3s f(s) \log_2 f(s) \\
&\quad + \sum_{i=1}^{m} \int d^3s f(s) p(i|\vec{b}) \log_2 (f(s) \frac{p(i|\vec{s})}{a_i}) \\
&= \sum_{i=1}^{m} \int d^3s f(s) a_i (1 + \vec{s} \cdot \vec{t}_i) \log_2 (1 + \vec{s} \cdot \vec{t}_i) \\
&= 2\pi \sum_{i=1}^{m} a_i \int ds s^2 d\theta_i \sin\theta_i f(s) (1 + t_i s \cos\theta_i) \\
&\quad \times \log_2 (1 + t_i s \cos\theta_i) \\
&= \frac{\pi}{2} \sum_{i=1}^{m} a_i \int ds s^2 f(s) \Big[(1 + t_i s)^2 \log_2 (1 + t_i s) \\
&\quad - (1 - t_i s)^2 \log_2 (1 - t_i s) - 2 t_i s \log_2 e \Big] . \qquad (54)
\end{aligned}$$

Although we already see from here that the sharpness of the POVM determines the information gain, we make a couple of assumptions to simplify the result. First we assume that the set of possible input states has a constant degree of mixing, i.e. the *a priori* distribution function is $f(s) = \frac{1}{4\pi s^2} \delta(s - s_{in})$. Second, we assume that all POVM elements are equally sharp, i.e. their Bloch vectors are equal in length $t_i = t_o$. The average information gain is now given by

$$\begin{aligned}
\Delta I &= \frac{1}{4} t_o^{-1} \Big[(1 + t_o s_{in})^2 \log_2 (1 + t_o s_{in}) \\
&\quad - (1 - t_o s_{in})^2 \log_2 (1 - t_o s_{in}) - 2 t_o s_{in} \log_2 e \Big] , \qquad (55)
\end{aligned}$$

from which we see that it only depends on the sharpness of the POVM, not on the number of measurement outcomes and their *a priori* probabilities. In paper I [21] we give the maximum sharpness of the effective POVMs on the input, when measuring the different subsystems in the output of the cloner. Accordingly we find that the maximum average information gain when measuring the ancilla, one clone, or two clones are $\Delta I_a = 0.027$ bits, $\Delta I_c = 0.112$ bits, $\Delta I_{cc} = 1 - \frac{1}{2}\log_2 e = 0.279$ bits, respectively. The last value coincides with the optimum value achievable through a direct von Neumann measurement on the input state. Note that these values are way below the Holevo bound ($\Delta I_c = 1$ bit) which is reached when the input set consists of only two orthogonal states.

Based on the concatenation of several cloning machines Bruss *et al.* [23] studied the upper-bounds imposed by optimal state estimation on the optimal universal cloner and vice versa. They derived a formula that relates the shrinking factor of an $N \to M$ *universal cloner*[23] and the shrinking factors associated to the optimal state estimation (52) with N and M copies of the unknown state

$$\eta_{NM} = \frac{\eta_e^{opt}(N)}{\eta_e^{opt}(M)} = \frac{N}{M}\frac{M+2}{N+2}. \tag{56}$$

The actual transformation which gives this optimum shrinking factor for the M copies was found by Gisin and Massar [57].

The output of these cloning machines has very special properties that are studied in detail in paper I [21] and reflect many important aspects of quantum information. Of particular interest is the relation between the sharp measurements done in a part of the output, say, on the two clones, and the state of the remaining subsystem (the ancilla) conditional to a given measurement outcome. There is a very intuitive tradeoff between the information gained in the measurement and the ability to recover the original unknown input state in the subsystem which was not measured. A sharp measurement on a subsystem corresponds to a sharp effective POVM on the input (maximum information gain) *if and only if* the remaining subsystem is left in a state that is independent of the input. On the other hand, a sharp measurement on a subsystem corresponds to a completely

[23] Generalization of the $1 \to 2$ cloner that operates on N copies of an unknown state and creates M identical imperfect copies of it.

unsharp effective POVM, i.e. $E_i \propto \mathbb{1}$ (no information gain) *if and only if* the original input state can be recovered in the remaining subsystem by a fixed unitary operation[24]. These ideas will appear again in the forthcoming sections.

Let me now report[25] some interesting *conservation laws* that arise from the observation that all universal cloning machines in the literature can be brought by a fix rotation of the ancilla qubit to fulfill this symmetry

$$U_{UC}(V \otimes \mathbb{1} \otimes \mathbb{1})|\varphi\rangle_s|0\rangle_b|0\rangle_a = (V \otimes V \otimes V)U_{UC}\ |\varphi\rangle_s|0\rangle_b|0\rangle_a, \tag{57}$$

where s, b and a are the input, blank and ancilla qubits respectively, U_{UC} is the cloning transformation and the relation holds for any unitary operator $V = \exp(it\vec{p}\vec{\sigma})$. In particular it must hold for each term in the power expansion in t,

$$U_{UC}(V^{(n)} \otimes \mathbb{1} \otimes \mathbb{1})|\varphi\rangle_s|0\rangle_b|0\rangle_a = W^{(n)}U_{UC}\ |\varphi\rangle_s|0\rangle_b|0\rangle_a \tag{58}$$

where $V^{(n)}$ symbolizes the nth derivative of V in respect to t evaluated at $t = 0$, and $W = V \otimes V \otimes V$. By taking the norm of both terms in Eq. (58) we arrive to the following equality between input and output expectation values,

$$\langle V^{(n)}\rangle_{in} = \mathrm{Tr}_s(\rho_{in}V^{(n)}) = \mathrm{Tr}(\rho_{out}W^{(n)}) = \langle W^{(n)}\rangle_{out}. \tag{59}$$

The derivatives of V and W evaluated at $t = 0$ are

$$V^{(n)} = i^n(\vec{p}\vec{\sigma})^n = \begin{cases} i^n & \text{for } n \text{ even} \\ i^n\vec{p}\vec{\sigma} & \text{for } n \text{ odd} \end{cases}, \tag{60}$$

$$W^{(n)} = i^n M^n \tag{61}$$

$$\text{with } M = \vec{p}\vec{\sigma} \otimes \mathbb{1} \otimes \mathbb{1} + \mathbb{1} \otimes \vec{p}\vec{\sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \mathbb{1} \otimes \vec{p}\vec{\sigma}. \tag{62}$$

The powers of operator M are given by,

$$M^2 = 3\mathbb{1} + 2(\vec{p}\vec{\sigma} \otimes \vec{p}\vec{\sigma} \otimes \vec{p}\vec{\sigma})M \tag{63}$$

[24]These relations hold in general as far as the auxiliary system, in our case the blank and ancilla qubits, is in a known pure state before the global unitary evolution. The parenthesized comments concerning the information gain are of course also dependent on the particular set of possible inputs. The property that all sharp measurements lead to a maximum information gain is exclusive of isotropic distributions.

[25]These results came about from a collaboration with N. Lütkenhaus, D. Bruss and K.-A. Suominen, but are previously unpublished.

$$M^3 = 7M + 6(\vec{p\sigma} \otimes \vec{p\sigma} \otimes \vec{p\sigma}) \quad (64)$$

$$\dots$$

$$M^{2n} = a\mathbb{1} + (a-1)(\vec{p\sigma} \otimes \vec{p\sigma} \otimes \vec{p\sigma})M \quad (65)$$

$$M^{2n+1} = (3a-2)M + (3a-3)(\vec{p\sigma} \otimes \vec{p\sigma} \otimes \vec{p\sigma}) \quad (66)$$

$$M^{2n+2} = (9a-6)\mathbb{1} + (9a-7)(\vec{p\sigma} \otimes \vec{p\sigma} \otimes \vec{p\sigma})M. \quad (67)$$

For the first order term in t, Eq. (59) results in

$$\langle \vec{p\sigma} \rangle_{in} = \langle \vec{p\sigma} \otimes \mathbb{1} \otimes \mathbb{1} + \mathbb{1} \otimes \vec{p\sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \mathbb{1} \otimes \vec{p\sigma} \rangle_{out} = \langle \vec{p\sigma} \rangle_{c1} + \langle \vec{p\sigma} \rangle_{c2} + \langle \vec{p\sigma} \rangle_{a}. \quad (68)$$

I have relabeled the systems at the output to make the interpretation more direct ($\{s, b, a\} \to \{c1, c2, a\}$). Since this has to hold for all $\vec{s}$, we find that the input Bloch vector has to be equal to the sum of the Bloch vectors of the two clones and ancilla,

$$\vec{s}_{in} = \vec{s}_{c1} + \vec{s}_{c2} + \vec{s}_{a}. \quad (69)$$

The Bloch vector of the two clones is a shrunk version of the input Bloch vector, $\vec{s}_{c1} = \vec{s}_{c2} = \frac{2}{3}\vec{s}_{in}$. According to the previous conservation law the ancilla's Bloch vector has to be a shrunk inverted version of the input Bloch vector, $\vec{s}_{a} = -\frac{1}{3}\vec{s}_{in}$.

A universal NOT (U-NOT) [26], or spin flip, is an operation which takes an unknown state to its orthogonal state ($\vec{s} \to -\vec{s}$). It is straightforward to check that this is an anti-unitary operation which means that it is not completely positive[26] and it cannot be a quantum operation. It turns out [59] that the optimal U-NOT, which takes an unknown input state as close as possible (according to the fidelity) to its inverted version, produces a state with Bloch vector $\vec{s}_{inv} = -\frac{1}{3}s_{in}$. This is precisely the ancilla state at the output of a cloner. From (52) we see that this can be also achieved by doing state estimation and preparing an inverted guess. Moreover, we can prepare as many inverted copies as we please. This fits with our previous conclusion that the ancilla can not be used to increase the information gain: by doing state estimation of the input "through" the clones, we can in fact produce many "ancillae" for free.

For even order terms in Eq. (59) we obtain

$$\langle \vec{p\sigma} \otimes \vec{p\sigma} \otimes \mathbb{1} \rangle_{out} + \langle \mathbb{1} \otimes \vec{p\sigma} \otimes \vec{p\sigma} \rangle_{out} + \langle \vec{p\sigma} \otimes \mathbb{1} \otimes \vec{p\sigma} \rangle_{out} = -1. \quad (70)$$

[26] It is equivalent, up to a σ_y rotation, to the transposition operation that led to the Peres-Horodecki separability criteria in 2.2.

For the odd order (but $n > 1$) terms we obtain,

$$\langle \vec{p}\vec{\sigma} \rangle_{in} = -\langle \vec{p}\vec{\sigma} \otimes \vec{p}\vec{\sigma} \otimes \vec{p}\vec{\sigma} \rangle_{out}. \tag{71}$$

Since the proposed universal $N \to M$ cloners exhibit an analogous symmetry (58), similar conservation laws (a bigger number of them) can also be derived for those machines. These conservation laws can be very useful in studying the properties of the universal cloners, such as the entanglement, classical correlations, or the information content of the subsystems. However, there is a fact that makes them less powerful: they follow from an "empirical" observation. The postulated symmetry (58) does not follow directly form the defining properties of the universal cloner. The universality (F =constant) only implies,

$$\mathrm{Tr}_a \left(U_{UC}(V\rho_{in}V^\dagger \otimes |00\rangle\langle 00|)U_{UC}^\dagger \right) = V \otimes V\rho_{out}V^\dagger \otimes V^\dagger, \tag{72}$$

which is much softer than the postulated symmetry and from which the conservation laws do not follow. Showing in full generality the conditions for which the strong symmetry might follow from the soft one would restore the value of the derived conservation laws.

"No such thing as no-cloning: cloning can be found in nature in stimulated emission processes". With this statement Stig Stenholm shook the participants of the Workshop on the Physics of Quantum Information held in Helsinki (1998). But it turned out to be an insinuative rather than provocative statement, since it inspired Simon *et al.* [127] who showed that many stimulated emission processes can be understood as a combination of various $1 \to M$ universal cloning machines described above. So, nature has been producing the "best" clones allowed by quantum mechanics.

2.3.3 Teleportation

Suppose that Alice has an unknown quantum state on her hands that she wants to send to Bob. Imagine that they do not have a quantum channel available or that the unknown state is so precious that they do not want to run the risk of ruining it during the transmission. On the other hand, imagine that they have a classical channel, such as a telephone, available. A classically minded Alice will choose to measure the state, call Bob and tell him to prepare it. But, by now, we already know that this is not possible in quantum mechanics: a quantum measurement cannot extract all the information contained in the description of a quantum state. If these are really all the resources available to Alice and Bob, even a deep

understanding of quantum mechanics would not help them to do better than that. However, Bennett *et al.* [8] realized that if Alice and Bob happen to share a maximally entangled state, then they can manage to fulfill their task following this protocol:

1) Alice performs what is known as a joint *Bell-measurement* on the unknown state and her share of the EPR state. This measurement is a projection measurement on the four *Bell-states*

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{73}$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{74}$$

2) Alice communicates Bob which of the four possible measurement outcomes she got (2 bits of classical information).

3) Depending on the received message, Bob performs one of the operations $\{\mathbb{1}, \sigma_z, \sigma_x, -i\sigma_y\}$ on his qubit. The protocol ends here with Bob's qubit being in the unknown state that Alice *had* in her hands.

It is remarkable that only 2 bits of classical information suffice to reconstruct the state, specially considering that, even if the state was known by Alice, it would require an infinite amount of classical of information to send exactly the same state to Bob. The performance of teleportation only compares to sending the qubit directly to Bob through an ideal quantum channel. This mysterious transfer of quantum information can be easily understood by rewriting [8] the initial state as,

$$|\Psi\rangle_{123} = \frac{1}{\sqrt{2}}|\varphi\rangle_1(|00\rangle + |11\rangle)_{23} = \frac{1}{2}[|\phi^+\rangle_{12} \otimes |\varphi\rangle_3 + |\phi^-\rangle_{12} \otimes \sigma_z|\varphi\rangle_3$$
$$+|\psi^+\rangle_{12} \otimes \sigma_x|\varphi\rangle_3 + |\psi^-\rangle_{12} \otimes (-i\sigma_y)|\varphi\rangle_3]. \tag{75}$$

From here is easily verified that conditional on Alice's Bell-measurement outcome, Bob's respective states are, up to a trivial rotation, equal to the unknown state originally owned by Alice. The quantum information in the unknown state is 'disembodied' in two parts: a classical part (measurement outcome) and a quantum part (conditional state after measurement). Notice that none of these parts contains by itself any information whatsoever on the input state. It is straightforward to check that all Bell-measurement outcomes occur with probability $\frac{1}{4}$ independently of the input state, and that without the knowledge of this outcome Bob's state is a completely

mixed state —the quantum channel going from the input to Bob's state is a depolarizing channel (53) with $p = 3/4$. Only by rejoining the classical (in Alice hands) and the quantum (in Bob's hands) parts the quantum state $|\varphi\rangle$ can be recovered. Teleportation might seem to challenge the no-cloning theorem and the no faster-than-light signaling principle from special relativity, but the disembodiment and reconstruction of the quantum state is fully consistent with these immovable laws[27]: the unknown state is completely "erased" from Alice's systems by the Bell-measurement, and Bob has to wait for the classical message to be able to reconstruct the state.

It is crucial that Alice does not gain any information through the joint measurement. As discussed in the previous subsection, in order to be able to recover the input state after a measurement, the POVM element corresponding to the measurement outcome has to produce a flat probability distribution over all input states, i.e. $p(i|\varphi) = \mathrm{Tr}(E_i|\varphi\rangle\langle\varphi|) = c\ \forall|\varphi\rangle$. Accordingly, *any* POVM formed by POVM elements satisfying this condition will be equally good for teleportation. The isomorphism between the $d \times d$ complex matrices and pure states in $\mathcal{H}_A \otimes \mathcal{H}_B$ introduced before Eq. (11) provides us with a simple characterization of these POVMs.

A maximally entangled state is a bipartite pure state which subsystems are maximally mixed. According to Eq. (12) this implies that every pure state can be described by a unitary matrix U, $\frac{1}{\sqrt{d}}|U\rangle$. Making use of Eq. (11), this also means that starting from an arbitrary entangled state we can prepare any maximally entangled state by a local unitary operation $V \otimes \mathbb{1}|U\rangle = |VU\rangle$.

Bearing this in mind, let me describe a generalized teleportation protocol. Alice's unknown state is described by a density operator ρ acting on $\mathcal{H}_1$, and Alice and Bob share a maximally entangled $\frac{1}{\sqrt{d}}|\mathbb{1}\rangle_{23}$. Alice performs a joint measurement defined by the POVM elements

$$E_i = |v_i\rangle\langle v_i| \text{ with } |v_i\rangle = \alpha_i|U_i\rangle_{12} = \alpha_i U_i \otimes \mathbb{1}|\mathbb{1}\rangle_{12} \text{ and} \tag{76}$$

$$\sum_{i=1}^{n} E_i = \sum_{i=1}^{n} U_i \otimes \mathbb{1}|\mathbb{1}\rangle_{12}\langle\mathbb{1}|U_i^\dagger \otimes \mathbb{1} = \mathbb{1}. \tag{77}$$

Shur's lemma[28] provides a very convenient way to generate sets of POVM elements satisfying (77) [20] from the unitary irreducible representation

[27] These two laws are also consistent with each other. As pointed out by Gisin [56] the no-signaling condition fixes an upper-bound on the cloning fidelity.

[28] For a unitary irreducible representation $\{U_g\}$ of the group $G = \{g\}$, $\int U_g A U_g^\dagger = \mathrm{Tr}(A)\mathbb{1}$, holds for all operators A.

of groups. The unnormalized state of Bob's particle conditional to the measurement outcome E_i will be given by

$$\begin{aligned}\tilde{\rho}^i &= \mathrm{Tr}_{12}(\rho \otimes |\mathbb{1}\rangle_{23}\langle\mathbb{1}|E_i \otimes \mathbb{1}_3) \\ &= |\alpha_i|^2 \mathrm{Tr}_{12}(\rho \otimes |\mathbb{1}\rangle_{23}\langle\mathbb{1}|U_i \otimes \mathbb{1}_{23}(|\mathbb{1}\rangle_{12}\langle\mathbb{1}| \otimes \mathbb{1}_3)U_i^\dagger \otimes \mathbb{1}_{23} \\ &= |\alpha_i|^2 U_i \rho U_i^\dagger, \end{aligned} \tag{78}$$

and its probability of occurrence is indeed independent of the input $p(i|\rho) = \mathrm{Tr}(\tilde{\rho}_i) = |\alpha_i|^2$. The unitary operation U_i that Bob needs to implement to finish successfully the teleportation protocol is determined solely by the measurement outcome (the required bits of communication may be larger than d^2).

From the linearity of the whole protocol we notice that teleportation also works when the input state is part of a composite system. If this state turns out to be entangled, this entanglement is also teleported to Bob's site. This is known as *entanglement swapping* [144, 145, 17] and it allows to entangle particles that have never interacted. Once the entanglement between Alice and Bob is established they will effectively have an ideal quantum channel (of single use) and Alice can use a classical wide range broadcasting channel to send the quantum state to Bob without even knowing his precise whereabouts. Moreover, if Alice and Bob never had the chance to meet and prepare their entangled pair, they can use a noisy quantum channel and entanglement purification protocols [9] to obtain a maximally entangled state. Only when Alice and Bob have managed to prepare —at the cost of several "disposable" noisy entangled pairs—a maximally entangled state they will use it to teleport the precious unknown state.

A generalization of the teleportation protocol where Alice and Bob share a non-maximally entangled states (pure or mixed) has been used to characterize entangled states according to the optimum average teleportation fidelity [55, 69] or maximum probability of successful teleportation [100] that can be reached with the shared state.

Entanglement swapping demonstrates, by entangling two qubits that never interacted, the capability of quantum teleportation to "simulate", i.e. to reproduce the effects of, an entangling interaction on a bipartite separable state. In terms of quantum gates[29] the creation of a maximally

[29]The term quantum gate denotes any unitary operation used for quantum information processing. However, as logic-gates in classical computation, the term quantum gate usually refers to an elementary quantum operation on a few qubits which is standard in some broad sense, either because it is a useful building block in designing quantum algorithms or because it is part of a universal set of gates [1] from which any quantum

entangled state can be reduced to the action of a *controlled-NOT* gate, CNOT$= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x$ and a Hadamard gate, $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, as shown in Figure 3. Gottesman and Chuang [60] showed that teleportation

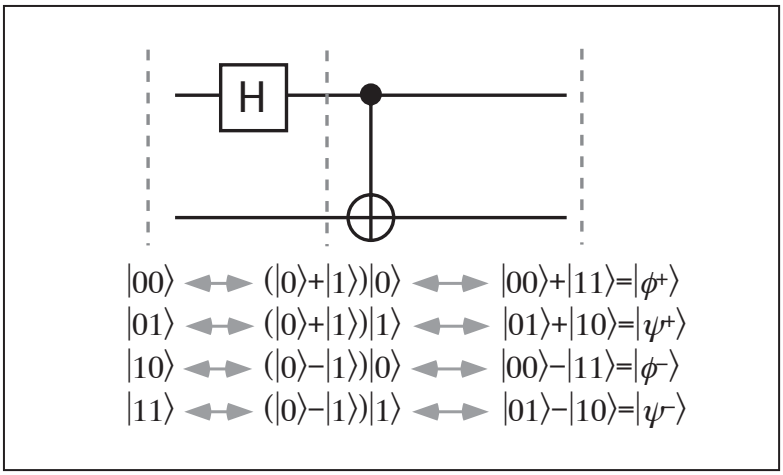

Figure 3: A Hadamard gate and a CNOT can be used to create the Bell-state basis from the separable canonical basis.

can in fact simulate the action of a CNOT over any two-qubit state. In this very enlightening work they show how to exploit the fact that the action of a CNOT gate *following* the action of any of the Pauli operators is equivalent to the action of CNOT *preceding* the action of some Pauli operators, or more succinctly CNOT$\in C_2$ where the *Clifford group* C_2 is defined by $C_2 = \{U | UC_1U^\dagger \subseteq C_1\}$ and $C_1 = \{\sigma_x, \sigma_y, \sigma_z\}$. The action of the Bell-measurement in teleportation is to operate on Bob's qubit with one of the Pauli operators chosen at random. Now imagine Alice and Bob share two maximally entangled states, Alice uses each of them to teleport two unknown states to Bob. After applying the "correcting" Pauli operators Bob applies a CNOT on them. Now, according to the above statement, the action of the CNOT after the Pauli operators is equivalent to the CNOT preceding another set of "correcting" Pauli operators. The teleportation of two states followed by the action of a $CNOT$ is completely equivalent to the teleportation of the two states using the shared state $|\xi\rangle_{11'22'} =$ CNOT$_{22'}|\phi^+\rangle_{12}|\phi^+\rangle_{1'2'}$ (instead of $|\phi^+\rangle_{12}|\phi^+\rangle_{1'2'}$) and a modified set of Pauli operators to recover the state. This is what Gottesman and Chuang

operation can be realized.

refer to as *teleporting a state 'through' a* CNOT. A trivial modification of the above protocol performs a CNOT on distant qubits, one qubit owned by Alice and the other by Bob. The same idea can be applied to other gates belonging to the Clifford group C_2 and elaborations of this idea allow to perform the gates contained in $C_k = \{U | UC_1U^\dagger \subseteq C_{k-1}\}$.

The most revolutionary point of this work is not so much the ability to perform non-local gates using entanglement[30] but the ability to perform non–trivial gates over unknown states by doing Bell–measurements and acting with Pauli operators on a prescribed state. As we will see, this will be of paramount importance in physical implementations of quantum information processing where controlled interactions are not readily available.

Note also that teleportation brings out the fungible character of information (quantum or classical)[31]. Once the entanglement is established between the distant Alice and Bob, using e.g. photons, teleportation allows to "send" the quantum state of systems, such as atoms in a cavity, which would be extremely difficult to send otherwise. This makes teleportation an important tool for distributed quantum processing in quantum networks.

2.3.4 Quantum Dense Coding

Quantum dense coding [13] can be presented as a variation of the teleportation protocol where the role of classical and quantum information are interchanged. Both are based on the idea of modifying the shared entangled state by local operations. In teleportation the quantum correlations are exploited to send quantum information, while in quantum dense coding they are used to double the classical capacity of a channel. The protocol goes as follows.

1) Alice performs one of the operations $\{\mathbb{1}, \sigma_z, \sigma_x, \sigma_y\}$ to her share of the maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}|\mathbb{1}\rangle$ thereby preparing one of the Bell-states

$$\{\frac{1}{\sqrt{2}}|\mathbb{1}\rangle = |\phi^+\rangle, \frac{1}{\sqrt{2}}|\sigma_z\rangle = |\phi^-\rangle, \frac{1}{\sqrt{2}}|\sigma_x\rangle = |\psi^+\rangle, \frac{1}{\sqrt{2}}|\sigma_y\rangle = -i|\psi^-\rangle\}.$$

2) Alice sends her qubit to Bob through a noiseless quantum channel.

[30] For instance, the CNOT between distant parties could be realized using the same resources by simply teleporting Bob's unknown qubit to Alice, and let Alice perform the CNOT and return the transformed qubit to Bob via teleportation.

[31] Without forgetting that information is still physical, of course.

3) Upon receiving Alice's qubit, Bob performs a joint Bell-measurement on this and his qubit. The outcome of the measurement will unambiguously tell Bob which of the four operations Alice applied. The protocol ends here and Alice has managed to transmit 2 bits of classical information by sending only one qubit.

The Holevo bound on the accessible information (1 bit per qubit) is of course on safe ground, for a qubit needs to be sent in order to establish the quantum correlations. The information is encoded in the four dimensional Hilbert space spanned by the two qubits ($\Delta I = S(\frac{1}{4}\mathbb{1}_4) = \log_2 4 = 2$ bits) but the four Bell-states can be prepared *locally*. Note that the transmitted qubit is in a maximally mixed state no matter which encoding operation Alice applied. This means that the 2 bits of classical information are all embedded in the quantum correlations and can be acquired only by having access to both involved qubits.

We have seen how teleportation allows to establish a quantum channel from an EPR pair and classical communication. Quantum dense-coding allows us to establish a high capacity secret classical channel from an EPR and a quantum channel. These two pillar protocols in quantum information processing are clear examples of why entanglement is considered a "resource" in quantum information processing. The ability to perform Bell-measurements is crucial in both. The relation between these protocols in quantum information has been made explicit in [138].

2.3.5 Quantum Key Distribution

Cryptography[32] is the science of hiding information in a string of bits that are meaningless to any untrustworthy party. To achieve this goal, Alice (the sender) uses an *encoding key* and an algorithm to encrypt her message producing the *cryptogram*. Bob (the receiver) must have a matching *decoding key* to *decrypt* the cryptogram. The cryptosystem is secure if it is "impossible" to a third party (the eavesdropper, Eve) to decrypt the cryptogram without the decoding key. There are basically two types of cryptosystems depending on whether the key is secret or public.

A very simple and effective private key cryptosystem is the *Vernam cipher* or also called *one-time pad*. Alice and Bob share a secret *random* binary string which is as long as the message. To encode her message, Alice simply adds each bit of her message to the corresponding bit of the

[32] For an entertaining exposition of the history of cryptography and cryptanalysis see [128].

key. The resulting cryptogram is sent to Bob, who decrypts the message by subtracting the key. Shannon [123] proved that this cryptosystem allows completely secure communication provided that the random key is as long as the message and is only used once. The zero-information content of the cryptogram is reflected by the following rather ludicrous observation. If Eve wants to crack the message by trying out all possible keys one by one, she will do nothing more than generate all possible messages of that length. The original message will of course be among them, but Eve has no means to recognize it[33]. The one-time pad is the only cryptosystem that provides provably secure communication, but it has an important drawback which renders it useless for most practical proposes: it requires the secure distribution of the key string, which has to be as long as the message and can not be re-used.

The first *public key* cryptosystems did not come until the late 70' but now they play a crucial role in most secure communications. In these systems users do not need to share any secret key beforehand. Public key cryptosystems are based on *one-way* functions for which it is easy to compute $f(x)$ for a given variable x, but difficult to obtain x from $f(x)$. Moreover, such one-way functions have a so-called *trapdoor* which allows one to ease the computation if some additional information is available. Factoring of large numbers is a typical example. It only takes few computational steps to calculate the product of two prime numbers $ab = c$, but the fastest known factoring algorithm requires a number of computational steps that grows exponentially with the number of bits in c, to find a and b. However, if one of the prime numbers a is known, the second prime number b can be easily computed.

If Alice wants to send a message to Bob, *he* first has to create a random private key. He uses it to compute a public key, which he announces publicly. Alice then uses the public key to encrypt her message. She sends the cryptogram to Bob, who decrypts it with his private key. The whole process of encryption and decryption can be described by a one-way function with a trapdoor "opened" by Bob's private key. Public-key cryptosystems are extremely effective and completely supersede private-key cryptosystems in situations where the exchange of a secret key is not viable. However, the security of these public-key systems is by no means proven and it strongly

[33]This brings to my mind the curious Borges tale [15] in which a library is reported to contain every possible book with 412 pages. In this library one could for example find the Spanish translation of the Kalevala in which the most thrilling episode is replaced by the first page of this thesis. However, it would be impossible to identify the faithful translation unless one knows it by heart.

relies on a shaky assumption. The definition of one-way functions is a bit vague, there is no guarantee that a fast algorithm to compute the x from $f(x)$ does not exist. The discovery of quantum computation, which promises an exponential speed up in respect to classical algorithms, has therefore been taken as a serious threat to public-key cryptosystems. But nearly at the same time quantum mechanics offered an alternative solution: *quantum key distribution.*

The idea of using non-orthogonal quantum states to protect information from being read by an unauthorized person was first introduced by Wiesner [140] in his "quantum money" that would frustrate any counterfeiter. In 1984 Bennett and Brassard [7] took Wiesner's innovative but extremely unpractical idea, and turned it into a feasible cryptosystem (BB84) that revolutionized cryptography and gave an important boost to the field of quantum information. The BB84 protocol basically borrows the one-time pad from classical cryptography and provides the means to securely distribute the key, thus granting absolute secure communication. This is how it works:

i) Alice sends randomly one of the fours states,

$$|0\rangle, |1\rangle, |\tilde{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |\tilde{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{79}$$

with equal probability. Here the states $|0\rangle$ ($|1\rangle$) and $|\tilde{0}\rangle$ ($|\tilde{1}\rangle$) represent the bit value '0' ('1'). These states can correspond for example to linearly polarized photons in the angles $0°, 90°, 45°$, and $135°$, respectively.

ii) Bob receives the state from Alice and he randomly chooses to measure it either in the $\{|0\rangle, |1\rangle\}$ basis (σ_z basis) or in the $\{|\tilde{0}\rangle, |\tilde{1}\rangle\}$ basis (σ_x basis). Only in the cases where Bob picked the "right" basis, i.e. the one used by Alice, Bob will learn the bit value sent by Alice. Whenever Bob measures in a "wrong" basis, that does not correspond to the state send by Alice, he can get both bit values with equal probability.

iii) After exchanging enough photons, Alice announces publicly the basis (σ_x or σ_z, but *not* the bit value) that she used to send the states, and Bob announces publicly his measurement basis.

iv) They throw away the cases in which they used different basis, and thus have established the secret key, known as the *sifted key.*

v) If, in an attempt to extract information, the eavesdropper perturbs the transmission, Alice's and Bob's key will be different. In order to assess the secrecy of their communication, Alice and Bob have to sacrifice some randomly chosen bits of the sifted key and check if they are identical. If they detect some irregularity, they throw away the whole key and start over again.

In practice, however, the protocol has to be refined a little to cope with the unavoidable errors during the preparation, transmission, and detection of photonic states. Since it is impossible to have a completely perfect implementation, and every error has to be attributed to an eavesdropping attack, some error correction and privacy amplification [10] protocols are needed to distill a completely secure key from a partially insecure one. The complete security in the presence of noise under all possible eavesdropping attacks has only been proven recently [98, 126]. A nice feature of quantum cryptography is that once the key is established, there is nothing that Eve can do to reveal the secret —even if she proceeds with the prospects of future technology or an ingenious mind that can help her unveil the secret in the future. The security of quantum cryptography resides solely in quantum mechanics (and on the right implementation of the protocol!). Several quantum key distribution protocols followed the BB84, and although they may be quite different from the practical point of view, they are all based on the same principle that non-orthogonal states cannot be measured without disturbing them.

In this sense, quantum key distribution falls closer to *steganography*[34] than to *cryptography*[35]. Methods in cryptography rely on the ingenious scrambling of the information before sending it and which only the receiver can unscramble upon receipt. On the other hand, methods in steganography provide secure communication by physically hiding it. For example, covering the written text with a thin layer of wax or letting the ink penetrate through the porous shell of a boiled egg, safely covers the information that the receiver can retrieve by removing the wax or pealing the egg. Of course any unauthorized attempts to peal the egg will become apparent when Bob receives it. In a "similar" fashion quantum key distribution hides classical information in quantum systems. The properties of quantum measurement, however, provide an absolutely secure "shell".

[34]From Greek *steganos*, meaning covered.
[35]From Greek *krypto*, meaning hidden.

3 Quantum Information: Implementations

3.1 Candidate Physical Implementations

Since the beginning of quantum information theory there has been a growing number of proposals for physical implementations of quantum information processing devices [52]: trapped ions, cavity QED, optical lattices, linear and non-linear optics, NMR, quantum dots, Josephson junctions, etc.. Although every implementation has its pros and cons that suit different scenarios, there are some general desirable properties. These are expressed as the abilities to [103]:

a) Identify qubits. A proper and robust representation of the qubits is necessary. Each qubit must be identified with a two-dimensional Hilbert space and the dynamics of the system should not take it out of this Hilbert space.

b) Perform a universal family of unitary operations (e.g. single qubit rotations $U_\alpha = \exp(i\alpha\sigma_x)$ and CNOT).

c) Prepare an initial state, ideally in a pure state.

d) Reliable method to perform measurements on the qubits.

In the context of quantum computation scalability is usually added to this list.

3.2 Linear Optical Implementations

There is no consensus as to the physical support that will be used to build quantum computers. However, there seems to be no dispute about using *optical photons* for quantum communication. The advantages are clear: maximum transmission speed in optical fibers or free space, weak coupling to the environment and negligible thermal noise. Quantum communication protocols use coherent state inputs (from a laser), linear elements, parametric down-converters and photodetectors. However, the down-converters are only used in the state preparation. In any case, the non-linearities involved here are of the modest kind. Let us now proceed to present the main properties of these basic ingredients.

A **coherent state** [90] of light is typically associated with the field that is produced by a laser[36]. Coherent states are defined through the relation $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, where $\hat{a}$ is the bosonic annihilation operator of the field

[36] See, however, text under continuos variable teleportation below.

mode, obeying the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$, and α is a complex number. Its phase and amplitude correspond to the phase and amplitude of the expected value of the electric field. Moreover, the quantum fluctuations around these values are as small as quantum mechanics allows, thus a coherent state is usually regarded as a classical state of light. States which cannot be interpreted as an ensemble of coherent states are called *non-classical*. A typical nonclassical state is the single photon state, which is the ideal qubit for quantum communication. In terms of the photon number states $\hat{n}|n\rangle = a^\dagger a|n\rangle = n|n\rangle$ (also called *Fock states*), the coherent states can be written as

$$|\alpha\rangle = \mathrm{e}^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{80}$$

It is clear that a coherent state has Poissonian photon statistics,

$$p_n = \mathrm{Tr}(\hat{n}|\alpha\rangle\langle\alpha|) = \frac{1}{n!}|\alpha|^{2n}\mathrm{e}^{-|\alpha|^2}, \tag{81}$$

with an average photon number equal to the intensity of the field $\langle\alpha|\mathbf{n}|\alpha\rangle = |\alpha|^2$. The coherent states of a given field mode always have a non-zero overlap,

$$|\langle\alpha|\alpha'\rangle|^2 = \mathrm{e}^{-|\alpha-\alpha'|^2}. \tag{82}$$

However, the coherent states span the whole Hilbert space and form an overcomplete basis,

$$\frac{1}{\pi}\int_{-\infty}^{\infty} \mathrm{d}^2\alpha |\alpha\rangle\langle\alpha| = \mathbb{1}. \tag{83}$$

Linear optical elements are the most common devices in an optical table: mirrors, half-wave plates, beam splitters and such. A great deal of the experimental advances in the study of the quantum properties of light owes its existence to these simple devices. A linear optical element is defined by the linear transformation between its input and output modes,

$$\hat{c}_j^\dagger = \sum_{k=1}^{n} U_{jk}\hat{a}_k^\dagger \tag{84}$$

where the U is unitary in order to fulfill the commutation relations of the output modes. The number of particles in the output is also automatically preserved.

A trivial linear element that only involves one mode is the *phase shifter* defined by,

$$\hat{c} = \mathrm{e}^{i\phi}\hat{a} = \mathrm{e}^{-iH_0}\hat{a}\mathrm{e}^{iH_0}, \tag{85}$$

where $H_0 = \phi\hat{n}$ is the generating Hamiltonian. A simple layer of a dielectric crystal can be used to provide interference between modes. In terms of its reflection r and transmission t coefficients the mixing of modes in this beam-splitter is given by

$$\hat{c}_1 = t\hat{a}_1 + r\hat{a}_2, \tag{86}$$

$$\hat{c}_2 = r\hat{a}_1 + t\hat{a}_2, \tag{87}$$

where unitarity implies $|t|^2 + |r|^2 = 1$ and $r^*t + rt^* = 0$. Without loss of generality one can assume that t is real while r is imaginary. By setting $t = \cos\theta$ and $r = i\sin\theta$ the Hamiltonian which generates this kind of evolution is given by

$$H_1 = -\theta(\hat{a}_1^\dagger\hat{a}_2 + \hat{a}_2^\dagger\hat{a}_1). \tag{88}$$

By allowing extra phase shifters in the output ports, one can generate the $SU(2)$ algebra (we dropped the global phase). The corresponding beam-splitter transformation can, thus, be written using the three angular momentum operators defined through the Schwinger relations [33],

$$J_1 = \frac{1}{2}(\hat{a}_1^\dagger\hat{a}_2 + \hat{a}_2^\dagger\hat{a}_1),\ J_2 = \frac{1}{2i}(\hat{a}_1^\dagger\hat{a}_2 - \hat{a}_2^\dagger\hat{a}_1),\ J_3 = \frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1 - \hat{a}_2^\dagger\hat{a}_2). \tag{89}$$

This provides an intuitive interpretation, in terms of three rotation angles, of the action of the four-port on the input fields, in particular when they are described as quasi-probability distributions [90].

This beam-splitter transformation models a large variety of *four-port* devices: *polarizing beam-splitters*, which use an anisotropic media to split the two polarization modes of the incident field into two momentum modes, *fiber-couplers* which mix light fields through optical tunneling, *polarization rotators* like some liquid crystals which rotate by a given angle the plane of polarization of linearly polarized light, or *wave retarders* where two linearly polarized components of the incident field have different refractive indices producing a phase retardation between both modes. Reck *et al.* [114] showed that any *multi-port* transformation of the form (84) can be reduced to the action of a series of elementary beam-splitters.

Photon detectors are the place where we locate the Heisenberg cut [104] of our quantum description, that is, the point where a measurement occurs and the transition from a quantum to a classical description occurs. Photodetectors used in quantum communication are photomultiplier tubes [117]. When a photon reaches the cathode of the tube it releases an electron (photoelectric effect) which accelerates towards the anode maintained at a

higher potential. On the way to the anode the photoemitted electrons might suffer collisions with metal or semiconductor surfaces producing an amplification of the electric current. A similar effect is used in the avalanche photodiodes [117] which are also widely used in quantum communication. The *quantum efficiency* η is the probability that a single photon contributes to the detected electric current. An inefficient detector ($\eta < 1$) can be modeled by placing a beam-splitter of transmittance $|t|^2 = \eta$ in front of a unit-efficiency detector ($\eta = 1$). In order to detect a single incident photon, high voltages have to be applied, which also increases the risk of producing *dark-counts*, i.e. detection events that are not triggered by an input photon. Dark-counts can be substantially reduced if detectors can operate at time-gated intervals, or if correlations between several detectors are measured. The *photon number resolution* determines whether the detector is able to distinguish signals with similar photon numbers. An *ideal photodetector* is the one which realizes the POVM $\{|n\rangle\langle n|\}_{n=0}^{\infty}$ on the measured field. Typically in quantum communication, photodetectors have single-photon sensitivity but no photon number resolution (see however [131]), thus it is described by the POVM element corresponding to a "click" $\sum_{n=1}^{\infty} |n\rangle\langle n|$ and that corresponding to a "no-click" $|0\rangle\langle 0|$. By using a *detector cascade* [129], i.e. by splitting the signal and sending it to several detectors, it is possible to get nearly ideal photodetection using detectors without photon-number resolution (see however [80]).

Parametric down converters provide the most basic, and therefore most accessible non-linear interaction between photons. This interaction arises due to the second order non-linear susceptibility of a crystal. In parametric down-conversion a *pump* photon has a small probability of spontaneously decaying into two photons of lower frequency, for historical reasons called *signal* and *idler* photons. Energy and momentum conservation impose the *phase matching conditions* $\omega_p = \omega_s + \omega_i$ and $\vec{k}_p = \vec{k}_s + \vec{k}_i$. Where the momentum inside the crystal is determined by the refractive index n, $k = \frac{\omega}{c} n(\omega)$. The phase matching conditions will be rarely satisfied. However, there are birefringent crystals where the refractive index of the photon depends on its polarization and propagation direction in respect to the crystal's optical axis. This introduces an extra degree of freedom which allows one to meet the phase-matching conditions. The maximum difference in refractive occurs between the *ordinary* and *extraordinary* normal modes which have mutually orthogonal linear polarizations. In *type-I* down-converters the signal and idler photons emerge with the same polarization, which is orthogonal to that of the pump. In *type-II* down-conversions, the

phase matching conditions occur when the signal and idler photons have mutually orthogonal polarizations, and the pump polarization is parallel to one of them. The phase matching conditions fix a characteristic emission spectra represented in Figure 4, where each emission cone corresponds to the signal and idler photons for a particular frequency. The real emission spectra is quite wide and gives rise to a whole family of paired signal-idler cones. In practice one only selects few modes from this complex spectra by using spatial and frequency filters. Of particular interest (see examples below) are the modes marked in Figure 4 for the type-II down-conversion at the intersection points of the degenerate idler (horizontally polarized) and signal (vertically polarized) cones. The photon pairs emitted in these directions are entangled in polarization, resulting in high-valued singlet states for two polarization qubits.

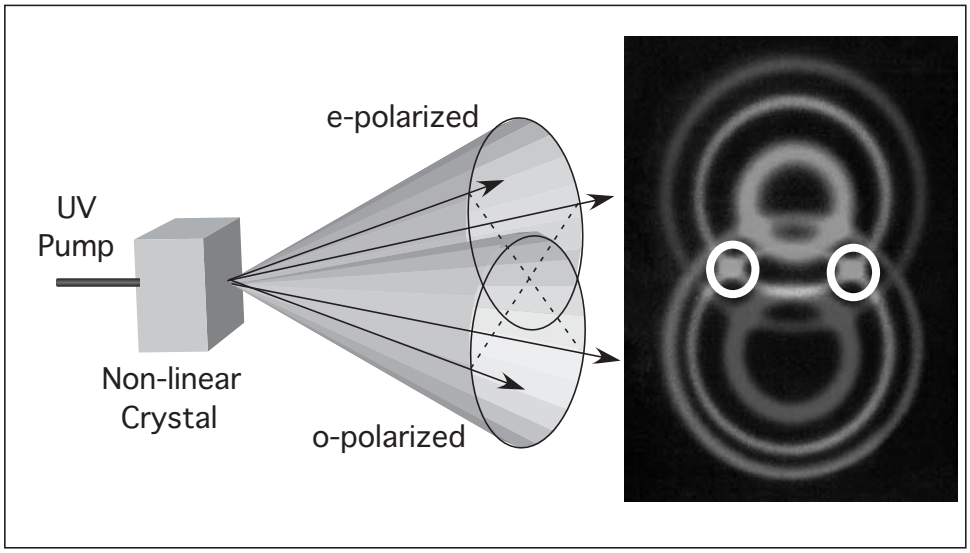

Figure 4: Left: Schematic representation of parametric down-conversion in type-II phase matching conditions. For simplicity we have plotted only the extraordinary and ordinary polarized cones for the degenerate case. The two emitted photons have opposite transversal momentum. Right: the projection of the cones for different frequencies (courtesy of Michael Reck [113]). I have marked with two white circles the directions from which the polarization entangled photons emerge. In type-I down-conversion the two cones are parallel and have the same polarization.

The full-quantum description of these phase-matched processes is provided by the following Hamiltonian in the interaction picture and rotating wave approximation,

$$H_{abc} = \kappa(\hat{a}^\dagger \hat{b}^\dagger \hat{c} + \hat{c}^\dagger ab), \tag{90}$$

where a, b and c are signal, idler, and pump modes respectively and the coupling constant κ depends on the second order susceptibility tensor. In parametric down-conversion the pump field is a coherent state $|\alpha\rangle$ from a laser. Since this is also a strong field it is possible to do the parametric approximation ($\kappa \to 0$ and $|\alpha| \to \infty$ with $\kappa\alpha$ =constant) which leaves an effective Hamiltonian

$$H_{ab} = \kappa\alpha(\hat{a}^\dagger \hat{b}^\dagger + ab) \tag{91}$$

after tracing out the pump field—see Eq. (7). This means that the interaction H_{abc} does not entangle the pump field with the other modes; otherwise the reduced evolution would not be unitary. This is a typical situation in quantum optics and many implementations of quantum information processing: an external field is used to drive a quantum system. To determine whether the field allows a classical description one has to make sure that the complete Hamiltonian, the initial fields and the interaction time are such that the driving field remains unaffected by the interaction. In other words, the driving field should not carry any information as to whether the transition (atomic, down-conversion, etc.) occurred. Coherent states are in this sense special since they remain untouched by the destruction operator. The precise mathematical justification requires a detailed analysis for each case, but in most cases the approximation holds for large amplitude coherent states.

The Hamiltonian H_{ab} generates the $SU(1,1)$ algebra and is the two-mode squeezing generator, or the single-mode squeezing in the degenerate case ($a = b$). The four modes emerging at the "cone intersection" in type-II down-conversion (see Figure 4) are similarly described by the Hamiltonian,

$$H_{ab} = \kappa\alpha(\hat{a}_x^\dagger \hat{b_y}^\dagger + \hat{a}_y^\dagger \hat{b}_x^\dagger + \hat{a}_x \hat{b}_y + \hat{a}_y \hat{b}_x), \tag{92}$$

where a,b denote the momentum and the subindices x and y denote horizontal and vertical polarizations, respectively. Even with strong pump fields, the non-linear effects are very small, and the interaction time is limited by the absorption and divergence of the light-beams in the crystal. Accordingly, the state of the outgoing modes, when the signal and idler are initially in the vacuum state $|\mathbf{0}\rangle$, is given by

$$\mathrm{e}^{-iH_{ab}\tau}|\mathbf{0}\rangle \;=\; |\mathbf{0}\rangle - i\xi(\hat{a}_x^\dagger \hat{b_y}^\dagger + \hat{a}_y^\dagger \hat{b}_x^\dagger)|\mathbf{0}\rangle + \mathcal{O}(\xi^2)$$

$$= \quad |\mathbf{0}\rangle - i\xi(|H\rangle_a|V\rangle_b + |V\rangle_a|H\rangle_b) + \mathcal{O}(\xi^2), \qquad (93)$$

where $\xi = \tau\kappa\alpha$ gives the probability amplitude of having the spontaneous emission of a polarization entangled pair. The birefringence that makes accessible the phase-matching conditions is also responsible for a time delay between the ordinary and extraordinary photons when travelling through the crystal. If this delay is longer than the coherence time the two terms in Eq. (93) become distinguishable and the entanglement vanishes. This can however be corrected by using compensators at the output beams.

The mode transformation induced by any combination of down-converters is linear, but mixes operator and destruction operators[37]

$$\hat{c}_j = \sum_{k=1}^{n} A_{jk}\hat{a}_k + B_{jk}\hat{a}_k^\dagger, \qquad (94)$$

where now the commutation relations for the output modes impose the conditions $AB^T = (AB^T)^T$ and $AA^\dagger = BB^\dagger + \mathbb{1}$. It is interesting to notice [19] that it is possible to reduce the general transformation of this form to the action of single-mode squeezers and linear elements. This can be seen in the recent proposal by Kwiat *et al.* [84] to create polarization entanglement from two adjacent crystals operated with type-I phase matching but with their optical axis aligned in perpendicular planes. If the crystals are thin enough so that the down-conversion processes in both crystals are coherent, *all* pairs of a given color will be polarization entangled.

Parametric down-converters can also provide single photon sources. The type-I Hamiltonian Eq. (91) on the vacuum state produces at small times the state $|\mathbf{0}\rangle - i\xi|1\rangle_a|1\rangle_b + \mathcal{O}(\xi^2)$. If we place a photodetector in mode a and this registers a "click", then the conditional state of mode b will be a single photon state[38] which is ready to be used as a qubit. Recently, Kim *et al.* [77] have reported experiments that hint at an alternative *deterministic* single-photon source. Of course this would be very desirable and would boost quantum communications, which is now restricted by the very rare —only one in ten billion photons are down-converted—and spontaneous emissions or by the very weak coherent states that decrease the efficiency of quantum key distribution protocols.

[37] It is not uncommon in the literature to refer to such devices as *active* linear devices as opposed to *passive* linear devices, which correspond to what I call linear elements.

[38] Strictly speaking, only a one-photon detection in mode a results in a single photon state. A "click" with no photon number resolution will lead to a state $\rho \propto |1\rangle\langle 1| + \mathcal{O}(\xi^2)$.

3.2.1 Experiments

In this section I will overview some representative experiments in quantum information that have already been realized in the labs.

Teleportation As we saw in 2.3.3, the creation and measurement of Bell-states is of paramount importance in teleportation. We have also seen that parametric down-conversion provides a reasonable source of entangled photons. The main problem that faces the implementation of teleportation in the labs is the Bell-measurement.

Innsbruck experiment: Figure 5 shows a schematic representation of the experiment [18]. A pulsed UV pump laser passes through a type-II non-

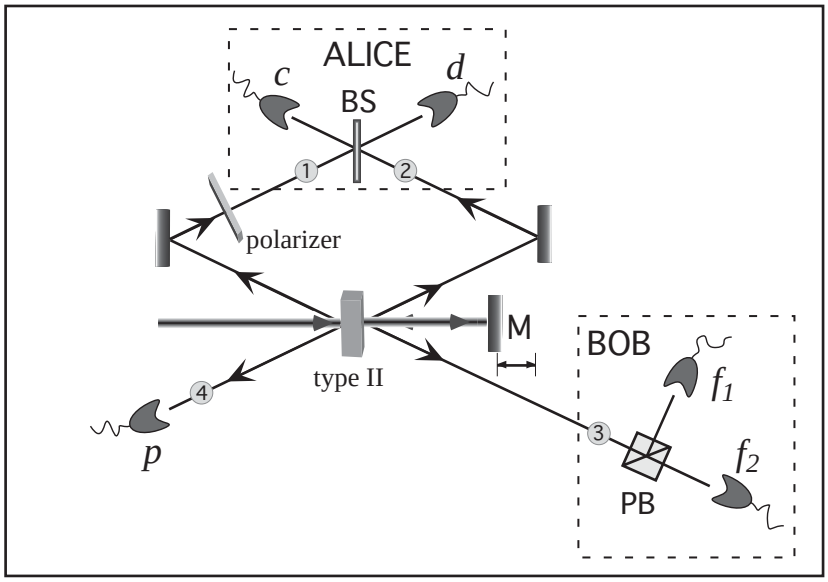

Figure 5: Experimental realization of teleportation in Zeilinger's group.

linear crystal and creates a pair of entangled photons (2,3) which form the EPR state shared by Alice and Bob. The same pump field is reflected back to the crystal producing a second pair of entangled photons (1,4). This second down-conversion provides Alice with a source of single photons to be teleported: a "click" in detector p assures the presence of photon 1. A polarizer is used to prepare the "unknown" state of photon 1. Alternatively, one could measure the polarization of photon 4 and thereby fix the

teleportee's polarization. Photons 1 and 2 are directed to a beam-splitter where the incomplete Bell-measurement occurs.

Bell measurement probes the collective or relative properties of the two qubits, it is essential that the carrier particles "forget" any information about their origin. The way to solve this is to give them a "common origin": photons are indistinguishable and after meeting and separating in a beam-splitter they lose their identity. Of course one has to make sure that the photons really meet in the beam-splitter. This entails a perfect mode-matching of the incoming photons. For all Bell-states but the singlet $|\psi^-\rangle$ the two photons emerge always through the same output port: the singlet is antisymmetric and therefore the two photons must emerge through different ports.

$$\begin{aligned}
|\phi^+\rangle &= \frac{1}{\sqrt{2}}\left(\hat{a}_x^\dagger \hat{b_x}^\dagger + \hat{a}_y^\dagger \hat{b}_y^\dagger\right)|\mathbf{0}\rangle \xrightarrow{\text{BS}} \frac{i}{2\sqrt{2}}\left(\hat{c}_x^{\dagger\,2} + \hat{c}_y^{\dagger\,2} + \hat{d}_x^{\dagger\,2} + \hat{d}_y^{\dagger\,2}\right)|\mathbf{0}\rangle \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}\left(\hat{a}_x^\dagger \hat{b_x}^\dagger - \hat{a}_y^\dagger \hat{b}_y^\dagger\right)|\mathbf{0}\rangle \xrightarrow{\text{BS}} \frac{i}{2\sqrt{2}}\left(\hat{c}_x^{\dagger\,2} - \hat{c}_y^{\dagger\,2} + \hat{d}_x^{\dagger\,2} - \hat{d}_y^{\dagger\,2}\right)|\mathbf{0}\rangle \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}\left(\hat{a}_x^\dagger \hat{b_y}^\dagger + \hat{a}_y^\dagger \hat{b}_x^\dagger\right)|\mathbf{0}\rangle \xrightarrow{\text{BS}} \frac{i}{\sqrt{2}}\left(\hat{c}_x^\dagger \hat{c}_y^\dagger + \hat{d}_x^\dagger \hat{d}_y^\dagger\right)|\mathbf{0}\rangle \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}\left(\hat{a}_x^\dagger \hat{b_y}^\dagger - \hat{a}_y^\dagger \hat{b}_x^\dagger\right)|\mathbf{0}\rangle \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}\left(\hat{c}_x^\dagger \hat{d}_y^\dagger - \hat{d}_x^\dagger \hat{c}_y^\dagger\right)|\mathbf{0}\rangle. \qquad (95)
\end{aligned}$$

In order to demonstrate that teleportation took place, the Innsbruck group measured the polarization of Bob's particle (3) using a polarizing beam-splitter and two photodetectors (f1,f2), and showed how the four-fold coincidences of detectors (c,d,p,f2) "vanished" when Bob measured his particle in the right basis. They also showed the increase in the four-fold coincidence when Bob measured in the wrong basis, i.e. with a different orientation of the polarizing beam-splitter. These changes in the counting rates where measured with respect to the rates obtained when teleportation was artificially disabled by decreasing the time overlap (and therefore the interference) between photons 1 and 2. This time-delay was enforced by displacing the mirror M.

This novel experiment cannot avoid getting some criticism:

1) Incomplete Bell-measurement. Only the singlet can be discriminated and the teleportation protocol only succeeds with probability $\frac{1}{4}$. If the unknown state is difficult to prepare or is very precious for whatever reason (see [79]), this may be a serious drawback.

2) *A posteriori* teleportation. The protocol *requires* Bob to detect his photon, and not only for "checking" purposes. From Eq. (93) we see

that the state produced by the pump pulse has, besides the entangled pair, a huge vacuum component and some higher order terms with two or more pairs of photons. The second order term has the same probability as the creation of the two pairs (1,4) and (2,3). Thus it is crucial to distinguish these two processes. If Bob is not allowed to detect his particle (directly or with a QND) then the photodetector p needs to have photon-number resolution to disregard the double-pairs. In any case, for most practical proposes the teleported state ends up being measured at some stage; thus this criticism is inconsequential.

Rome experiment: This scheme is quite peculiar in that the qubit representation is atypical. Popescu [112] found an interesting way to use "real" entanglement[39] and still be able to do a complete Bell-measurement, thus achieving the teleportation of a qubit between physically separated parties. Figure 6 depicts the experimental realization [16] of Popescu's scheme.

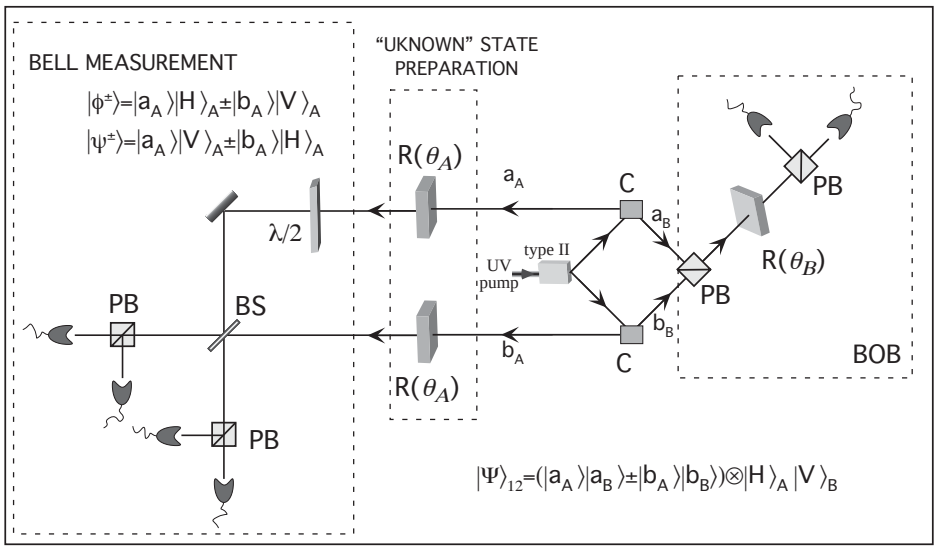

Figure 6: Experimental realization of teleportation in De Martini's group.

A non-linear crystal cut for type-II down-conversion is pumped with a UV cw laser producing a polarization entangled state. Each of the beams is

[39] As we will see below, a single photon can be used to represent n-qubits, and linear optics suffices for doing any unitary operation on them. In particular one can realize the quantum circuit for teleportation, but this would not be more than an emulation since in this representation there is no place for the key concept of entanglement.

sent through a calcite crystal (C in Figure 6) where the horizontal and vertical polarizations take different routes. The horizontally polarized beams are sent to Alice while the vertically polarized beams are sent to Bob. By doing so, Alice and Bob share a pair of photons which are entangled in momentum (or spatial paths a,b). There are no more particles involved. Instead of teleporting the state of a third particle, they teleport the polarization degree of freedom of Alice's photon. Two identical polarization rotators $R(\theta_A)$ are used to prepare the state to be teleported. The *complete* Bell-measurement corresponds to a direct realization of the gates in Figure 3[40]. The $\lambda/2$ plate flips the polarization ($x \leftrightarrow y$) whenever the photon takes the the upper path (a_1), and of course does not affect the photon in the lower path (b_1). This is precisely the CNOT with the momentum degree of freedom being the control qubit. To implement the Hadamard gate on this qubit we only need a 50/50 beam-splitter (which is polarization independent). Finally, polarizing beam-splitters and photodetectors perform a von Neumann measurement in the canonical basis. At Bob's site, the qubit in the momentum degrees of freedom is transferred to the polarization degrees of freedom and a polarization analyzer $P(\theta_B)$ checks that the teleportation succeeded. In the experiments the measured coincidences counts between Alice's and Bob's detectors where obtained for different preparation θ_A and detection angles θ_B and were shown to be fully consistent with the teleportation protocol. Notice that this verification procedure did not require to implement the "correcting" rotations at Bob's site for each of Alice's Bell-measurement outcomes.

The obvious drawback of this scheme is that the teleported state has to be prepared beforehand. This disallows[41] many interesting applications of quantum teleportation such entanglement swapping [144, 145, 17] or the implementation of non-local gates [60].

Caltech-Aarhus: For completeness I include here a third teleportation protocol. Figure 7 shows a schematic representation of the teleportation of continuous variables experiment [54]. Here, instead of teleporting a qubit encoded in a single photon, Alice and Bob teleport a quantum state of light with undetermined number of photons. In particular, in the experiment they teleported a coherent state of amplitude $\alpha_{\rm in} = x_{\rm in} + ip_{\rm in}$. The maximally entangled state needed to teleport these continuous variables

[40] Since both the CNOT and the Hadamard gates are their own inverses, the "disentangling" circuit corresponds to the "entangling" one read from left to right.

[41] At least, until technology provides the means to coherently transfer the state of a third particle to the polarization degree of freedom of Alice's photon.

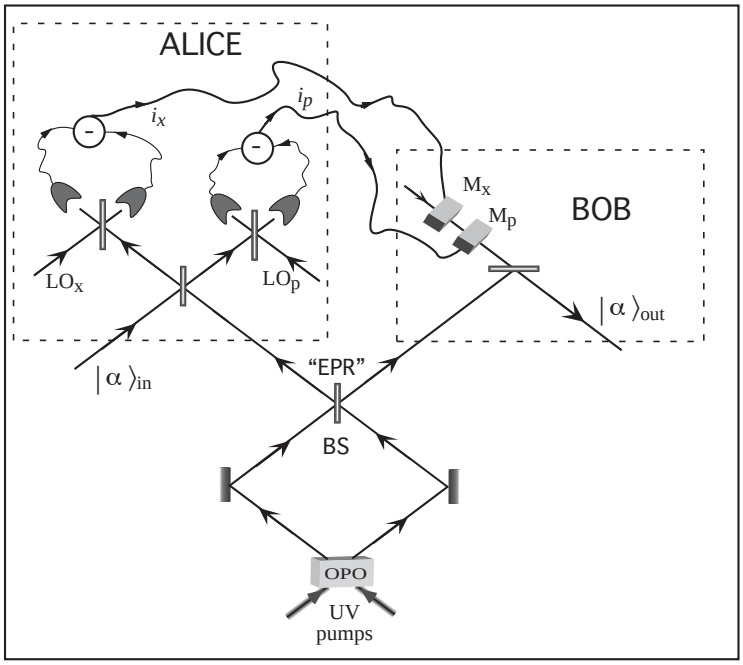

Figure 7: Experimental realization of teleportation in Kimble's group.

corresponds to a two-mode squeezed state (ideally with infinite squeezing). As discussed previously, two single mode squeezers combined in a beam-splitter can be used to create an effective two-mode squeezer (modes 1 and 2) needed for continuous variable teleportation. The single-mode squeezed states where created by a non-linear crystal in an optical parametric oscillator (OPO). The optical cavity in the OPO enhances some downconversion modes while inhibiting non-resonant modes, thus creating an intense narrow-band squeezed field. The Bell-measurement (with an infinite number of possible outcomes) consists in acquiring only the relative quadrature-phase variables, $x = \frac{1}{\sqrt{2}}(x_{\rm in} - x_1)$ and $p = \frac{1}{\sqrt{2}}(p_{\rm in} + p_1)$, between one mode of the EPR and the "unknown" coherent state. This can be easily done by two sets (one for each quadrature) of balanced homodyne detectors [90]. The two resulting photocurrents are then used by Bob to produce the necessary displacement operators on his share of the EPR to recover the initial coherent state.

The finite squeezing of the "EPR" will of course limit the fidelity of the teleported field, but current technology achieves very large squeezing

parameters. Hence, this is arguably the most complete teleportation experiment: it achieves the complete Bell-measurement, an unknown state (even entangled) can be teleported, and measuring the state at the output does not have to be necessarily a part of the procedure. Overall it is quite astonishing how simple the protocol turns out to be when going to infinite dimensional systems.

Notwithstanding, lately there has been a bit of controversy concerning the above experiment. The criticism comes about from the observation that the field emanating from a laser is strictly speaking not a coherent state of light: energy conservation requires it to be Fock diagonal, thus it can only be understood as a coherent state with a completely unknown phase. As Mølmer [99] puts it, assigning a particular phase to the output of a laser is a "convenient fiction" without any observable effects in experiments. Indeed, in most measurements (as homodyning or heterodyning) the absolute phase is irrelevant. However, it turns out to be a relevant matter in quantum information with continuous variables [116], for the entanglement shared by Alice and Bob "vanishes" if one does the phase averaging, and entanglement is not precisely something which easily falls under "convenient fiction". Van Enk and Fuchs [134] have cleared up this controversy by arguing that the outcome of a laser (with no phase drift) should actually be modeled as a bunch of systems (packets) each of them in the same coherent state $||\alpha|e^{i\phi}\rangle$ with an unknown phase ϕ,

$$\rho = \frac{1}{2\pi}\int_{\phi} d\phi |\alpha\rangle\langle\alpha| \otimes |\alpha\rangle\langle\alpha| \otimes \ldots \otimes |\alpha\rangle\langle\alpha| \tag{96}$$

With this, a measurement in the first subsystem fixes the phase of the rest, producing the very convenient coherent state of random, but determined, phase.

Quantum dense coding Figure 8 shows a schematic representation of the quantum dense coding experiment realized in Innsbruck[97].

Alice and Bob receive their share of a down-converted polarization entangled pair. Alice transforms locally the joint entangled state into one of the four Bell-states, by using a $\lambda/2$ oriented at 0° or 45°, followed by a $\lambda/4$ oriented at 0° or 90°. Having done that, she forwards the photon to Bob, who performs an incomplete Bell-measurement on both particles. As opposed to their teleportation experiment, the Innsbruck group could make a projection on *two* of the Bell-states in the quantum dense coding experiment. The main reason is that the quantum dense coding protocol

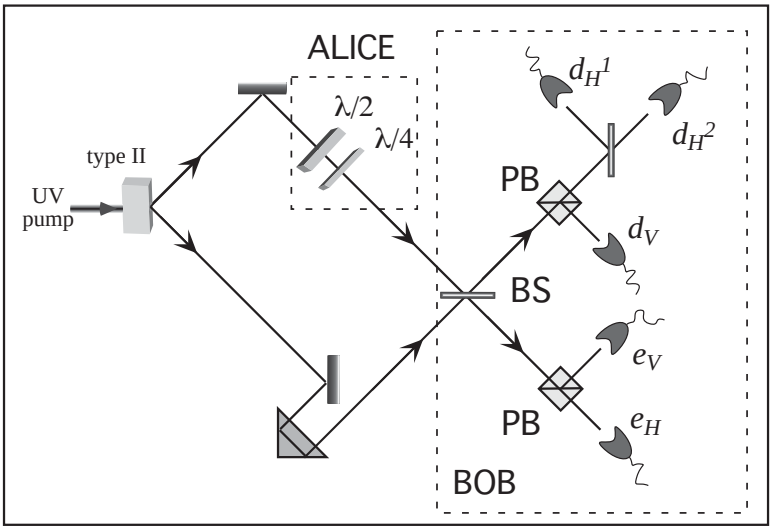

Figure 8: Experimental realization of quantum dense coding in Zeilinger's group.

only requires two-photon coincidences while the teleportation requires at least three-photon coincidences. This greatly reduces the complexity of the measurements and allows one to use more photo-detectors to measure the polarization at the output of the beam-splitter. Notice in (95) that by doing so, Bob can discriminate the two Bell-states $|\psi^{\pm}\rangle$. In the experiment a minimal cascading of photodetectors (d_H^1, d_H^2) was also used to identify two-photons since the detectors in "Geiger mode" cannot distinguish them from single-photons signals.

The experiment proceeds as in teleportation recording the coincidence-rates at Bob's detectors while sweeping the time-delay between both photons. As soon as the time-delay approaches zero the overlap of the photons wave-functions becomes large enough for interference effects to show up. Accordingly, the coincidence-rates at different detectors drastically increases or decreases depending on Alice's preparation. Since only three possible states could be discriminated by Bob, Alice could only communicate one *trit* ($\log_2 3$ bits) per qubit instead of the 2 bits.

Quantum key distribution Since the BB84 quantum key distribution protocol appeared, a plethora of variations and possible experimental schemes to implement them followed. Here, I will introduce an experiment that was

important at its time, since it achieved the transmission of a secret key over the record distance of 30 km. However, the main reason I chose this experiment is that it is representative of the state of the art quantum key distribution, while keeping close to the original BB84 protocol avoiding technical sophistications.

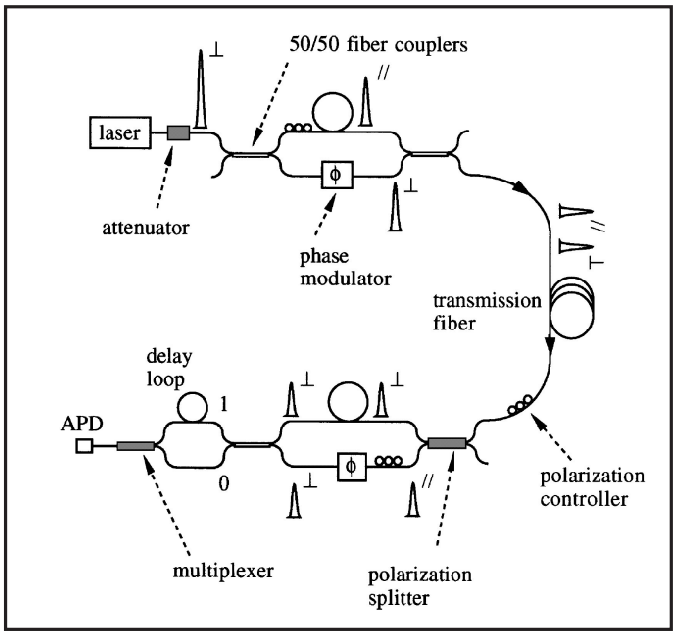

Figure 9: Experimental realization of Townsend quantum key distribution experiment (courtesy of Paul D. Townsend).

Unlike the teleportation or quantum dense coding experiments, no entanglement or Bell-measurements is needed here. The technological challenge consists in producing a setup which is suitable for efficient and secure quantum key distribution over long distances. Figure 9 shows a scheme of the quantum key distribution experiment in British Telecom [95]. A pulsed semiconductor laser is strongly attenuated to give an average photon number of $\mu \sim 0.1$. By doing so they generate a state for which the largest non-vacuum contribution comes from the single-photon state. The linearly polarized ($\perp$) pulse is split in a 50/50 fiber-coupler. A photon going through the upper fiber suffers a time delay and its polarization is flipped to $\parallel$, while a photon taking the lower fiber is sent through a phase modulator. The two pulses are then superposed in a second fiber coupler. The sent qubits are

represented by two orthogonal modes: the delayed $\|$-polarized mode and the not-delayed $\perp$-polarized mode. In principle it would be enough to use either time or polarization mode separation, however, the simultaneous use of both gives more stability to the system. Alice uses the phase modulator to randomly encode each pulse (or qubit) with four possible phase shifts ϕ_A, namely, $-45°, +135°$ (σ_x basis) and $+45°, -135°$ (σ_y basis) —these are analogous to the states $|0\rangle$, $|1\rangle$ and $|\tilde{0}\rangle$, $|\tilde{1}\rangle$ in Eq. (79). The encoded qubit is sent through the transmission fiber. At the other end of the fiber, Bob uses a similar setup to measure the qubit in a randomly chosen basis. The polarizing beam-splitter separates both modes and the time and polarization divisions are removed, allowing the two components to interfere at the 50/50 fiber coupler. The interference is controlled by the phase modulator in such a way that the photon takes the upper (*lower*) arm if the bit value is 1 (0). This amounts for a phase shift $\phi_B = -45°$ to measure in σ_x basis and $\phi_B = 45°$ to measure in σ_y basis. The bit values 0 and 1 are distinguished temporally at the photodetector by means of a delay loop in the upper fiber.

After sending a few thousand bits, Bob publicly communicates to Alice at which time slots he detected a photon and the basis he used for the measurement. Alice then tells Bob the time slots in which they used the same basis, hence establishing the sifted key. Alice and Bob compare some random bits of the sifted key to establish the error rate. In this experiment the BT group measured bit-error rates (without any eavesdropper) for different fiber lengths and average photon numbers, the extreme cases being a bit-error rate of 1.5% for a $l = 10$ km fiber and $\mu = 0.1$ and a bit-error rate of 4% for $l = 30$ km and $\mu = 0.2$. These error rates are below the required threshold to obtain a secure key after error-correction and privacy amplification [10]. The main source of bit-errors are the dark-counts at Bob detectors, and increases when the Bob's photoncount/dark-count ratio decreases. Thus the bit-error rate is increased by a reduction of the average photon number μ or by an increase in the transmission losses. The latter are due to losses in the components (mainly the phase modulators) and in the transmission fiber, and to the low quantum efficiency of the detector ($\eta \sim 0.1$).

3.2.2 Prospects: Possibilities and Limitations

The previous experiments illustrate how in spite of the lack of photon–photon interactions it is still possible to perform non-trivial operations on photonic qubits.

Linear optical elements suffice to perform any unitary operation on a single photonic mode (84). This already allows one to do a rather *sui generis* form of quantum information processing. Indeed, a photon entering an $n \times n$ multi-port is effectively an n-dimensional quantum system on which one can perform any unitary operation and measurement. This would allow one to do any quantum computation [37] using only beam-splitters and phase shifters. Of course, there is a catch: the number of modes needed to represent N qubits grows exponentially with the number of qubits, and so does the number of elements. So, the "physical space" grows linearly with the dimension of the Hilbert space, d. Moreover, any quantum information process based on entanglement or on the non-local nature of quantum mechanics is impracticable since this representation does not consist of distinct entangleable registers. These quantum networks are therefore relegated to be used as mere demonstration or pedagogical tools [83]. Note that in Rome's teleportation experiment this kind of representation is used for Alice's system, i.e. a single photon represents two qubits (half of the Bell-state + teleportee), making the complete Bell-measurement possible, but losing some important features of the original teleportation protocol.

In order to be loyal to the quantum information paradigm and contemplate all its implications, we stick to the *one photon per qubit* representation[42]. Typically the qubit is encoded in the polarization degrees of freedom of the photon. Since photons are indistinguishable particles, a second degree of freedom, like the momentum, has to "tag" them and make them distinct entangleable systems. For example, the two-qubit state $|\varphi\rangle \otimes |\phi\rangle$ will be represented by a two photon symmetrized wave function

$$|\varphi\rangle_1 \otimes |\phi\rangle_2 \equiv |\varphi\rangle|k_1\rangle \otimes |\phi\rangle|k_2\rangle + |\phi\rangle|k_2\rangle \otimes |\varphi\rangle|k_1\rangle, \tag{97}$$

where $\otimes$ separates the Hilbert spaces of both photons, which in turn are tensor products of the Hilbert spaces corresponding to the polarization and momentum degrees of freedom. Note that the wave function of two indistinguishable particles is entangled. Thus the ever-longed resource in quantum information is in fact everywhere in nature. However, "not all that glitters is useful entanglement", since any "local" operator acting on one photon cannot discriminate between the two photons, rendering futile

[42] I disregard quantum information in continuous variables which is not covered in this work. As demonstrated in the Caltech-Aarhus teleportation [54], linear elements have very high quantum information processing capabilities in these systems. See also [61].

any attempts to see the correlations[43] (see [111] for full discussion). This can be clearly seen if one tries to use the wave function (97) for teleportation or dense coding. In order to avoid confusion around "useful" entanglement and entanglement inherent to the particle statistics it is convenient to work in the second quantization. The two-photon wave function (97) in the second quantization reads,

$$|\varphi\rangle_1 \otimes |\phi\rangle_2 \equiv \hat{a}^\dagger_{\varphi k_1} \hat{a}^\dagger_{\phi k_2} |\mathbf{0}\rangle. \tag{98}$$

where $\hat{a}^\dagger_{\varphi k_1}$ can be written in terms of the horizontal and vertical polarization modes $\hat{a}^\dagger_{\varphi k_1} = \alpha \hat{a}^\dagger_{H k_1} + \beta \hat{a}^\dagger_{V k_1}$, and analogously for $\hat{a}^\dagger_{\phi k_2}$. The second quantization automatically takes care of the symmetrization, yielding the qubit representation straightforward. A single qubit is represented by a single excitation in the modes $\{\hat{a}_1, \hat{a}_2\}$. Any additional qubit will occupy in a similar fashion two *different* modes $\{\hat{a}_3, \hat{a}_4\}$. I refer to qudits encoded in indistinguishable particles using this representation as *i-qudits* (see paper IV [28]).

In papers II to IV [94, 31, 28] my collaborators and I study the possible measurements that one can realize on these photonic i-qubits using linear optical elements and photodetectors. For this purpose we introduce the most general linear-optics setup shown in Figure 10A. The input photons together with a predetermined auxiliary photonic state are sent through an array of linear elements or multiport, characterized by a unitary map U_1 (84). An ideal detector D_1 is placed in one of the output ports, $\hat{d}$. Corresponding to each measurement outcome k a second transformation U_2^k is realized on the remaining modes. This cascaded process is repeated until all the modes are measured.

In paper II [94] we present a *no-go theorem* that states that with such general setup it is impossible to perform a perfect Bell-measurement (see Figure 10). That is, we show that there will always be a detection event (a "click" combination in the output detectors) which could have been triggered by more than one Bell-state, thus impeding their unambiguous discrimination. For this purpose it is enough concentrate on the possible measurement outcomes of detector D_1. By enforcing the perfect state discrimination conditions for each outcome we arrive to a contradiction, thus proving the no-go theorem. The proof can be sketched as follows.

[43] Only by coupling the photonic modes, e.g., in a beam-splitter, inherent entanglement becomes apparent.

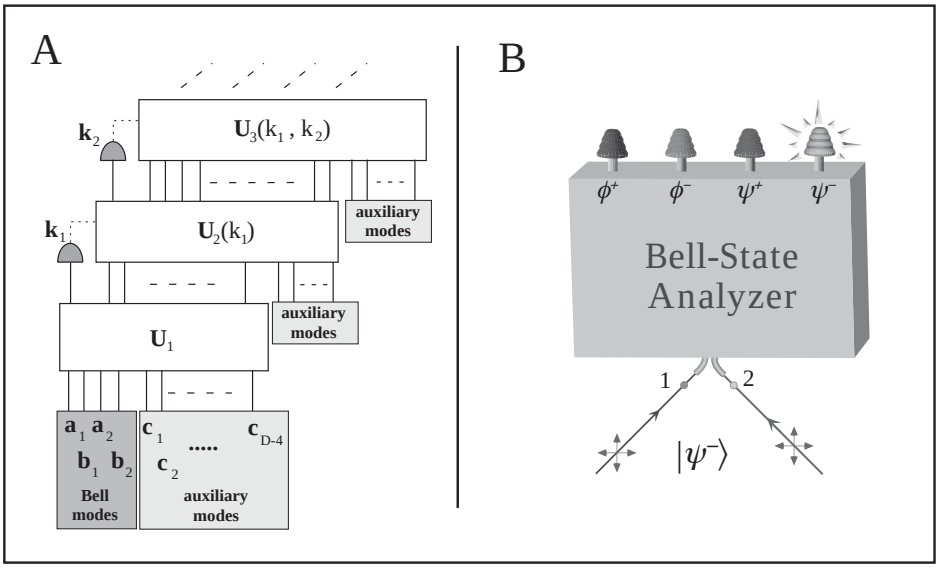

Figure 10: A) General measurement scheme with linear optical elements. B) Illustration of an ideal Bell-state analyzer. Two photons, each spanning two field modes, enter the analyzer through the input ports. A perfect projection onto the Bell-states means that each of the Bell-states should "light" one and only one of the four "bulbs" at the outputs.

1) We prove that there is always an event for which the fact whether it is conclusive or inconclusive does not depend on the auxiliary state. That is, we prove that if a Bell-analyzer without auxiliary photons has a non-zero probability of error, then a Bell-analyzer that uses auxiliary photons is doomed to fail also with a finite probability. This statement has been recently generalized by Carollo and Palma [35] for the perfect discrimination of any set of i-qudit states.

2) Once the problem is reduced to the case without auxiliary photons, we can study the possible detections at mode d, viz. 2 photon, 1 photon and 0 photon detection.

3) Two-photon detection—Imposing that the probability of this event is non-zero for at most one Bell-state we find that the first column vector of U_1 —which gives the linear relation between mode d and the input modes—has to be of a very precise form.

4) One-photon detection—Imposing the orthogonality of the conditional one-photon states of the single-photon detection event, we find that there is no unitary matrix compatible with the requirements.

5) Zero-photon detection—Obviously we can discard the remaining case: the zero photon detection represents a bad choice of mode d since it would be disconnected from the input Bell-modes.

In paper II we omitted the proof of one important result in step *1)*, and I shall therefore include it here:

Proof of Eq.(8) in paper II—We start by defining the polynomia $\tilde{Q}_{aux,l}$ following the definitions in Eqs. (5) and (6) in paper II.

$$|\Psi_i^{(total)}\rangle = \tilde{P}_{aux}\left(d^\dagger, e_k^\dagger\right)\tilde{P}_{\Psi_i}\left(d^\dagger, e_k^\dagger\right)|0\rangle \tag{99}$$

We expand the two polynomials in powers of $d^\dagger$ as

$$\tilde{P}_{aux}\left(d^\dagger, e_k^\dagger\right) = \sum_{l=0}^{N_{aux}} (d^\dagger)^l \tilde{Q}_{aux,l}\left(e_k^\dagger\right) \tag{100}$$

$$\tilde{P}_{\Psi_i}\left(d^\dagger, e_k^\dagger\right) = \sum_{l=0}^{N_{Bell}} (d^\dagger)^l \tilde{Q}_{\Psi_i,l}\left(e_k^\dagger\right). \tag{101}$$

$\tilde{Q}_{aux,N_{aux}}$ and $\tilde{Q}_{\Psi_i,N_{Bell}}$ correspond respectively to $\tilde{Q}_{aux}$ and $\tilde{Q}_{Psi_i}$ in Eqs. (5) and (6) in the paper.

We need to prove,

$$[\tilde{Q}_{aux,N_{aux}}, \tilde{Q}_{\Psi_i,N_{Bell}}] = 0. \tag{102}$$

Initially the Bell modes and auxiliary modes commute and therefore the polynomia $P_{aux}, P_{\Psi_i}^\dagger$ commute as well.

$$0 = [P_{aux}, P_{\Psi_i}^\dagger] = \sum_{l,k}\left[(d^\dagger)^l \tilde{Q}_{aux,l}, d^k \tilde{Q}_{\Psi_i,k}^\dagger\right] \tag{103}$$

$$= \sum_{l,k}(d^\dagger)^l d^k [\tilde{Q}_{aux,l}, \tilde{Q}_{\Psi_i,k}^\dagger] + [(d^\dagger)^l, d^k]\tilde{Q}_{\Psi_i,k}^\dagger \tilde{Q}_{aux,l} \tag{104}$$

$$= \sum_{l,k}(d^\dagger)^l d^k f_{l,k}(e_i, e_i^\dagger) \tag{105}$$

where we have made use of,

$$[(d^\dagger)^l, d^k] = -\sum_{s=1}^{min(l,k)} (-1)^s s! \begin{pmatrix} l \\ s \end{pmatrix} \begin{pmatrix} k \\ s \end{pmatrix} (d^\dagger)^{(k-s)} d^{(l-s)}. \tag{106}$$

From here we see that each term in the normally ordered expression needs to be equal to zero,

$$f_{l,k}(e_i, e_i^\dagger) = 0 \ , \ \forall \, l, k. \tag{107}$$

In particular, for the maximum values of l and k we get the commutation relation we were looking for,

$$0 = f_{N_{aux},N_{Bell}}(e_i, e_i^\dagger) = [\tilde{Q}_{aux,N_{aux}}, \tilde{Q}_{\Psi_i,N_{Bell}}]. \tag{108}$$

□

The general framework presented in this paper has set the ground for the research on the power of linear-elements for quantum information processing. Following the same line of action —steps *1-5* above—it is straightforward to prove similar no-go theorems for two-qubit basis sets that have more than two non-separable states (not necessarily maximally entangled). This puts experimental limitations on the realization of a quantum cryptography protocol proposed by Cabello [27].

Carollo *et al.* [36] also followed these guidelines to prove a no-go theorem for a very particular two-qutrit (-qudit[44] with $d = 3$) basis,

$$\begin{aligned} &|\psi_0\rangle = |2\rangle_A \otimes |2\rangle_B, \\ &|\psi_{\pm 1}\rangle = \frac{1}{\sqrt{2}}|1\rangle_A \otimes (|1\rangle \pm |2\rangle)_B, \ \ |\psi_{\pm 2}\rangle = \frac{1}{\sqrt{2}}|3\rangle_A \otimes (|2\rangle \pm |3\rangle)_B, \\ &|\psi_{\pm 3}\rangle = \frac{1}{\sqrt{2}}(|2\rangle \pm |3\rangle)_A \otimes |1\rangle_B, \ \ |\psi_{\pm 4}\rangle = \frac{1}{\sqrt{2}}(|1\rangle \pm |2\rangle)_A \otimes |3\rangle_B. \end{aligned} \tag{109}$$

Bennett *et al.* [11] provided this set as an example of what they called *non-locality without entanglement*: these nine basis states, despite being orthogonal and separable, cannot be discriminated locally and with classical communication (LOCC). With their no-go theorem, Carollo and coworkers proved that these peculiar basis states can not be discriminated under another class of operations, namely those provided by linear-optical elements.

The no-go theorem for the Bell-analyzer automatically puts forward a no-go theorem for a GHZ-analyzer[45], since one can always build a Bell-analyzer using a GHZ-analyzer. To see this it is enough to consider the

[44] A qu**d**it is the d-dimensional counterpart of the qubit.

[45] GHZ are three-qubit entangled basis states first given by Greenberger, Horne and Zeilinger to prove quantum non-locality without using inequalities [111].

two qubits and prepare a third qubit in state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Each of the eight possible outcomes of a GHZ-measurement performed on the three qubits will correspond to one and only one possible input Bell-state of the two qubits.

This "family" of no-go theorems leads to an important statement: although linear-optical elements can be used in a wide range of applications, they can never reach the full quantum information processing capabilities of the interaction-mediated gates.

Note that the no-go theorems give only qualitative results. They only set forth the impossibility to perform certain projection measurements, leaving room for analyzers which work to some extent, discriminating successfully in some occasions, and giving an inconclusive answer in others.

The purpose of paper III [31] is to find the quantitative upper-bound on the efficiency of a Bell-state analyzer. In order to tackle the problem we studied a simplified setup in which the auxiliary modes are initially in the vacuum state and no conditional dynamics are allowed. This is still a very relevant problem since *a)* it should help elucidate the role played by the "bare" linear-elements and *b)* it fixes the performance of the current applications where the use of extra photons and the implementation of conditional dynamics are still considered to be technological challenges[46]. This simplified setup is shown in Fig. 2 of paper III [31]. In that paper we show that such a Bell-state analyzer will inevitably give an inconclusive answer in *half* of the cases. That is precisely the limit achieved in some experiments described above [97].

In paper IV [28] I propose a new approach: instead of feeding the input basis states in the analyzer and studying under which circumstances they give distinguishable outcomes, that is, different "click" combinations, here I turn the problem around and ask what the different possible outcomes tell us about the input state. Of course, this approach leads to the definition of the set of POVMs that one can realize with linear optical elements.

The central result is derived in Eqs. (9-10) in the paper [28] and it gives the POVM induced on a pair of i-qudits (bosons and fermions) when those are sent through a fixed array of linear elements and are absorbed by particle detectors at the output ports. Specifically, the POVM elements $F^{ij} = |P^{ij}\rangle\langle P^{ij}|$, each of them associated to a detection event in detectors c_i and c_j, are given by the action of a linear map K on the set of normalized

[46]Mode-matching conditions—or photon wave-function overlap —hinder the interference of single photons coming from down-conversion sources. See [106] for recent progress in multi-photon interference.

states[47] $\{|\psi^{ij}\rangle \propto (|ij\rangle \pm |ji\rangle)\}$,

$$|P^{ij}\rangle = K|\psi^{ij}\rangle \;\text{ for }\; i \geq j = 1, \ldots, n \;\text{ with }\; K = \sqrt{2}A^* \otimes B^*, \qquad (110)$$

and the $d \times n$ matrices A and B satisfy the relations,

$$AA^\dagger = \mathbb{1}_d \;\;,\;\; BB^\dagger = \mathbb{1}_d \;\;,\;\; AB^\dagger = 0 \qquad (111)$$

$$\mathbb{1}_n - A^\dagger A - B^\dagger B \geq 0. \qquad (112)$$

These relations come about from the definition $U = (A, B, C)^T$ (see Eq. (8) in paper IV), U being the *unitary* transformation of the field modes associated to the linear-elements array.

The form of the map K automatically guarantees the completeness relation $\sum_{i \leq j} F^{ij} = \mathbb{1}$. Hence, to find out whether or not a given POVM $\{F^{ij} = |\tilde{P}^{ij}\rangle\langle\tilde{P}^{ij}|\}$ can be realized by linear–elements and particle detectors, one has to see if a map K exists which takes the states $\{|\psi^{ij}\rangle\}$ to the vectors of the desired form, i.e., $K|\psi^{ij}\rangle = \alpha_{ij}|\tilde{P}^{ij}\rangle$ for some complex number α_{ij}.

The problem of determining whether the transformation of a set of states to another is possible is of general interest in quantum information theory. Especially in the study of entanglement it would be extremely useful to find the conditions for which the state transformation can be achieved by the class of local operations and classical communication LOCC. There are already some results characterizing the deterministic transformation of a single bipartite pure state to another pure state, and the non-deterministic transformation from a pure state to a set of possible pure states [102]. However, little is known about deterministic transformation from a *set* of states to another set of states. It is my belief that the algebraic theory of linear preservers [91] can be of great use in this context. In the meantime we can already get some interesting results (see paper IV) from the particular form of our map K:

- K is separable and can therefore not increase the Schmidt rank of the original states $\{|\psi^{ij}\rangle\}$. In particular this means that *a)* two-photon detections ($i = j$) *always* lead to a separable POVM. Two photon detection always lead to an error when discriminating entangled states. *b)* it is not possible to have POVM elements that project on maximally entangled states of two qudits (with $d > 2$): $|\tilde{P}^{ij}\rangle \propto \sum_{l=1}^{d} |e_i\rangle|\tilde{e}_i\rangle$.

[47] Paper IV studies i-qudits —this includes both bosonic and fermionic qudits. Here the sign + (upper) corresponds to bosons while −(lower) corresponds to fermions.

- For qubits ($d = 2$) it is possible to have some maximally entangled POVM elements, but their total weight in the resolution of the identity can be at most one half—see Eq. (20) in paper IV for derivation. This fixes a tight upper-bound for a generalized Bell-measurement and for its possible applications.

Notice also that even with conditional dynamics (see Figure 10) the relation between input and output modes is always linear and the POVM element of a particular event can be easily found. A detection in modes $\hat{c} = \sum_j^{2d} \alpha_j \hat{a}_j$ and $\hat{d} = \sum_j^{2d} \beta_j \hat{a}_j$ can be easily seen to correspond to the POVM element $F^{cd} = |P^{cd}\rangle\langle P^{cd}|$. Following the formalism from paper IV, and using the isomorphism between complex matrices and bi-partite states (11,12), one arrives at the following result (analog to Eq. (13) in paper IV).

$$\begin{aligned}\langle 0|\hat{c}\hat{d}|C\rangle &= \sum_{i,j,k,l}^{n} \langle 0|\alpha_i \beta_j N_{kl} \hat{a}_i \hat{a}_j \hat{a}_k^\dagger \hat{a}_l^\dagger |0\rangle = 2\sum_{k,l}^{n} \alpha_k N_{kl} \beta_l \\ &= \mathbf{a_1}^T C \mathbf{b_2} \pm \mathbf{b_1}^T C^T \mathbf{a_2} = \mathrm{Tr}(C(\mathbf{b_2}^T \mathbf{a_1} \pm \mathbf{b_1}^T \mathbf{a_2})) = \langle P^{cd}|C\rangle \\ &\text{with } |P^{cd}\rangle = |\boldsymbol{a_1}\rangle|\boldsymbol{b_2}\rangle \pm |\boldsymbol{a_2}\rangle|\boldsymbol{b_1}\rangle, \end{aligned} \tag{113}$$

where the column vectors $\mathbf{a_1}$ and $\mathbf{b_1}$ are defined through

$$\alpha = (\alpha_1, \ldots, \alpha_{2d})^T = (\mathbf{a_1}, \mathbf{b_1})^T \text{ and } \beta = (\beta_1, \ldots, \beta_{2d})^T = (\mathbf{a_2}, \mathbf{b_2})^T,$$

and we have used the convention $|\mathbf{v}\rangle = \sum_{i=1}^{d} v_i |i\rangle$.

To conclude with the measurement on i-qudits, let me comment on a recent result which has been a real breakthrough in the study of quantum information processing with linear-optics. We have already stressed that the no-go theorems do not exclude the possibility of correctly discriminating a state of a given set with a finite probability ($0 < P_{\text{succ}} < 1$). Knill, Laflamme and Milburn [79] nearly exhausted this possibility by proving that with the general setup from Figure 10A one can do *any quantum operation* with a probability of success arbitrarily close to one. Moreover, they give a constructive proof of it.

In Section 2.3.3 we saw how one can implement an arbitrary operation using Bell-measurements by teleporting the state "through" the operation [60]. That is, the problem of performing certain gates is reduced to the problem of preparing a given entangled state. Knill *et al.* take this idea and give a procedure to prepare an auxiliary entangled state such that when teleporting the two unknown qubits through this state the output qubits

have effectively suffered a controlled–Z gate[48]. Since two Bell-measurement are required, the controlled-Z gate is correctly implemented with probability $p_s = \frac{1}{4}$. However, in the same work they present a way to enhance the probability of success of the "embedded" teleportation protocol to $p_s = 1 - \frac{1}{n+1}$ by using an n-photon highly entangled auxiliary state. To round things out they show that, with not too much of an overhead, the qubits can be encoded to make all the operations fault-tolerant[49]; thus proving that *linear-optics quantum computation* (LOQC) is *in principle* possible. Having said this, it is important to realize that the mere preparation of the auxiliary state required is far beyond the current technological possibilities—which is at the moment is struggling to achieve three or four-photon entangled states [106, 86].

Knill's *et al.* results have been very important for breaking with the skepticism promoted by the growing-number of no-go theorems. Indeed, *it is* (in principle) possible to use linear elements and particle detectors to realize *any* quantum operation with a probability asymptotically close to *unity*. One might think that these results set the end to the research of quantum information processing with linear elements. But, on the contrary it only stimulates it further: now that is clearer than ever that linear-elements are powerful devices, there is a bigger urge to understand how these simple devices handle quantum information. Bear in mind that Knill's *et al.* LOCQ is by no means optimized. There are many interesting applications (see paper IV for references), especially in quantum communication, where a simple beam-splitter can do most of the job and the use of LOQC would be an overkill.

In paper V [30] we examine the possibility of using linear optical elements and photodetectors to manipulate general quantum states of light, not necessarily photonic qubits. The characterization of the quantum states of light has been for decades an intense field of research both theoretically and experimentally [90]. Non-linearities are in general more accessible for this purpose, since one is not restricted to low photon numbers as in quantum information implementations. Nevertheless, linear elements are still the most preferred devices because they are extremely simple and their behavior is nearly ideal. Hence, it is also very relevant in this case to study the

[48] The *conditional sign-flip* gate is defined as C-Z$= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_z$, and together with single qubit rotations it forms a universal set of gates.

[49] Fault-tolerant operations tolerate, up to a given threshold, errors in their components. By tolerate I mean that the error does not propagate throughout the rest of the operation and can be detected and subsequently corrected. This is usually achieved by encoding the qubits in higher dimensional Hilbert-spaces.

power of linear-elements to manipulate quantum states of light. In paper V we take full advantage of the non-linearity provided by photodetectors and propose a very simple scheme to remove a single photon from a field mode in an arbitrary state. Linear elements are used to weakly couple the field mode to the detector mode and, as soon as one photon is detected, a feedback mechanism turns the coupling off, thus preventing any further losses. The so-called *adaptive absorption* also can be viewed as a very unsharp photon-number measurement, since larger photon numbers will loose one photon earlier. It is interesting to notice that if the feedback mechanism is deactivated so that an indefinite number of single-photon detections follows, the process describes a continuous photon-number measurement. In the limit of large times the continuous measurement and the direct projection measurement onto number-states will obviously result in the same total number of detected photons. However, the continuous measurement provides a much more accurate description of a real photodetector, which is crucial in understanding some experiment results. For example, the observation of interference effects from two independent sources with no defined phase, that justified the "convenient fiction" of assigning a phase to a laser field [99], can only be understood by the backaction of a succession of unsharp measurements that leads to a total von Neumann measurement.

The possibility of removing near-deterministically a single photon from an arbitrary state turns out to be a very relevant matter in evaluating the security of the current quantum key distribution implementations [29]. The proofs of security in [98, 126] assumed possible errors in the encoding, transmission and decoding of the sent qubits. However, they did not contemplate that the physical realization of the signals is not a real single-qubit. In current implementations, the lack of effective deterministic single photon sources is overcome by using very weak coherent pulses. Coherent pulses (81) contain multi-photon states with a probability $p_{n>1} = 1 - \exp(-\mu)(1-\mu)$. This opens a security loophole in the key distribution protocols. The possibility of extracting a photon from this multi-photon part of the signal provides Eve with a copy of the sent qubit which she can measure without disturbing Bob's measurement outcomes. If Eve assures that the intensity of the signals arriving to Bob does not decrease, then her attack will be imperceptible to Alice and Bob. To compensate for the losses she causes, Eve only has to provide a transmission fiber with lower losses than the one used by Alice and Bob.

The ideal way for Eve to take advantage of this loophole is to make a QND (quantum non-demolition) measurement on the number of photons in

the signal without disturbing its polarization, and split one photon from the signal whenever more than one photon are available. This is known as the *photon-number splitting attack* (*PNS*). QND measurements rely on the Kerr effect, governed by the third order non-linear susceptibility, rendering futile its use for low photon numbers. Moreover, even when the photon number is known, it is a non-trivial task to split exactly one photon without modifying the polarization[50]. Since the security of *present* quantum cryptography only depends on the *present* technology available to Eve, the PNS attack cannot be taken as a serious threat.

A technologically available alternative is the beam-splitting attack (BS), where Eve uses a beam-splitter to split *all* signals (single-photons included). This strategy is also ineffective since Eve actually splits many more signals than actually needed.

In paper VI [29] we propose adaptive absorption, or the *conditional beam-splitter attack*, as the means to split exactly one photon from the signal and thereby providing a simple, technologically available[51], and yet efficient attack on present quantum key distribution protocols.

In any case the single-photon part of the signal remains "untouchable" and can be used to guarantee the security of the protocol within some parameter regimes [93, 71]. Our result forces current experiments to take these operating regimes seriously if they want to guarantee security under any realistic attack.

3.3 Non-Linear Implementations

Although there has been some proposals [133] and even some preliminary experiments [78] to do quantum information processing using non-linear optics, those require either the Kerr effect, sum frequency generation (up-conversion) or the interaction with an atom, all of which are extremely ineffective and entail many technical problems at the single-photon level. However, when strong fields are available non-linear processes give rise to a wide range applications: four-wave mixing, phase conjugation, quantum non-demolition measurements, below shot-noise homodyne photocurrents, squeezing-mediated suppression of the spontaneous decay of a dipole

[50] This can be achieved for example through the Jaynes-Cummings Hamiltonian [93].

[51] Let me point out here that in paper IV we do not take into account the time delay produced on the signal by this eavesdropping attack. We disregard this problem by assuming that Eve can allways compensate the delay by finding a shorter route from Alice to Bob, or avoid the loop-delay by splitting the signal from several points *along* the transmission fiber.

quadrature, etc..

In paper VII [32] we propose an even more striking application of non-linearities. For this we contemplate a different system where non-linearities are much stronger than in optical fields, namely, degenerate atom-molecule systems, and show how two create a very special macroscopic superposition. The motivation behind this is obvious to any inquisitive mind.

Quantum mechanics is one of the most prominent theories in physics, a status achieved by its ability to predict the often "weird" behavior of the microscopic realm with astonishing accuracy. So far, the only "problem"[52] that faces quantum mechanics is that of determining its domain of validity, a problem that arises when applying quantum rules to macroscopic objects. Already Schrödinger highlighted the absurdity of applying quantum theory to macroscopic objects, by coupling the fate of a cat to the decay of a radioactive atom, thereby forcing the animal into a superposition of alive and dead. For some reason the classical world occupies a minute fraction of the Hilbert space assigned by quantum mechanics. A simple approach to the matter is *macrorealism* that asserts that macroscopic superpositions *do not* occur, full stop. Macrorealism is a conformist and not very constructive attitude since it does not specify what is *really* happening. Some more venturous theories have modeled the transition from quantum to classical by adding extra terms into the Schrödinger equation that become important only for macroscopic objects —the mass has been used to grade the "macroscopicness". It has been also speculated that there are non-quantum effects at sub-Planck scales that could have consequences in the macroscopic scale. Other theories, the most prominent of them is decoherence, try to explain *einselection* —or the natural selection of determined macroscopic states —within quantum mechanics. Creating macroscopic superpositions or "cat-states" can help us not only to persuade macrorealism that it is not a matter of principle that no quantum macroscopic objects exists, but also help to understand quantum mechanics decoherence mechanisms and the origin of einselection better.

In paper VII we pursue the creation of a superposition of two certainly distinct macroscopic objects: a "soup" of atoms and a "soup" of molecules. What I call soup here refers to a Bose-Einstein condensate of bosonic particles. The idea is to use photoassociation to coherently create molecules from an atomic condensate. Photoassociation occurs when an atom *pair*

[52]It would be too hard on quantum theory to call this a problem considering that it already describes phenomena from the Planck scale to the molecular scale (25 orders of magnitude!).

interacts with a photon driving a transition from the two-atom continuum to a bound state of the molecule. The first problem that appears is that photoassociated molecules are in short-lived excited electronic states that mainly decay to non-condensate modes, "killing" any cat or kitten that could exist. In this work we have therefore considered two-color free-bound-bound photoassociation, where the excited molecules are transferred by a second laser to a bound stable molecular state. Moreover, by using a large detuning we have adiabatically eliminated the excited molecular state, thereby hindering the deadly effects of the decay.

To study this system we have used a "toy model" which involves only three modes —one for each of the species: atoms, excited molecules and stable molecules—, and therefore disregards any dynamics in the spatial degrees of freedom. The validity of this model and the full-blown theory behind it was presented by Koštrun *et al.* in [81]. Besides the non-linearity introduced by the destruction/creation of atoms in pairs, we have also taken into account the non-linearities arising from atom-atom, molecule-molecule, and atom-molecule collisions. As opposed to the case of parametric down-conversion or squeezing, here the treatment needs to be fully quantum[53], because mean-field theories presuppose separable global states, while the longed-for cat-state is highly entangled. In the full-quantum treatment the evolution cannot be described by convenient algebra generators and we have to rely on numerical methods. The Hamiltonian in question (Eq. (6) in paper VII) conserves the "mass" $N = n_a + 2n_b$, here n_a and n_b are the number operators for atoms and stable molecules respectively. Since we start from an atomic condensate with a fixed number of atoms N, we can describe the whole dynamics using the basis states $|n\rangle \equiv |n\rangle_b|N-2n\rangle_a$. In this basis, the Hamiltonian is tri-diagonal and the dynamics can be easily simulated using the Crank-Nicholson numerical method.

We have shown that all these non-linear processes can be harnessed by the two laser fields (Figure 2 and caption in paper VII) to create a superposition of states with a very large number of molecules (molecular "soup") and states with a large number of atoms (atomic "soup"). Ideally, the state would be described by $|\Psi_{\mathrm{BIGCAT}}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_b|N\rangle_a + |\frac{N}{2}\rangle_b|0\rangle_a)$. Figure 2 in paper VII also shows that the dynamics of the system is such that the presence of the superposition in the intermidiate times can be detected by imprinting a phase in the molecular condensate.

[53] Only for the matter fields: the laser fields are treated semiclassically in the parametric approximation.

This is a very peculiar type of superposition since it seems to involve two objects in lieu of two states of the same object. Instead of a cat that was both alive and dead, this situation could metaphorically be termed an animal that is both cat and dog. Hence, with a system that is both a "soup" of molecules and a "soup" of atoms, quantum mechanics has not only crept closer to the macroscopic world but has apparently also gotten "weirder". Here, of course, we are exploiting the fact that naming two physical objects instead of attributing to each of them a different state of the same system is sometimes arbitrary or a matter of convenience. Strictly speaking, two states of a system can be considered different objects when there is no interaction that couples them. In this sense one could say that a photon is in fact the same object than a positron-electron pair. Moreover in quantum mechanics one can always stop the transition from one state to the other half-way, leaving the system in a superposition of both states. The fact that in the classical world we are not confronted with superpositions of different "objects" is arguably due to the superselection rules induced by decoherence which forbid their superposition. Thus in this sense, the more object-like our two states in the cat are, the more difficult it is to keep the cat alive.

4 Epilogue

Exactly a hundred and one years ago Max Plank discovered the quantum. Four decades of intense work of the most prominent physicists of the time led to the theory of quantum mechanics. Quantum mechanics enjoys an impeccable internal consistency and unprecedented agreement with experiments, and it only meets difficulties when interpreting its predictions. The basis of the theory of quantum mechanics has not changed since then. However, in the late 80's quantum information theory emerged, unraveling a source full of features that where hidden in this very basic formalism. The same old rules discovered decades ago are now embedded in a new information-theoretical framework in which they are being squeezed, turned and dissected. It is fascinating to see the amount of understanding and applications that are flourishing from this research field.

In this work I have presented my contribution in fundamental and applied aspects of quantum information theory. The main theme that outlines my work has been how to access the quantum information in a quantum system with some given resources; thus the POVM formalism has taken a central role.

Paper I studies to what extent one can process the quantum information of the input qubit of a quantum universal cloner if one has access only to some subsystem of output. This served to first, elucidate how quantum information is distributed in a cloning transformation and bring forward its potential uses in quantum information protocols, and second, to derive some general rules relating sharp measurements, information gain and state recovery on systems that have suffered an entangling evolution with some fixed auxiliary state.

Papers II-IV study how to process photonic qubits when one is restricted to use linear-optical elements and photodetectors. Papers II and III focus on the very relevant problem of performing Bell-measurements with these resources. In particular paper II gives a no-go theorem that asserts the impossibility of doing a *complete* Bell-measurement with a very general set-up which includes linear elements, photodetectors, auxiliary photons and feedback mechanisms. Paper III gives an upper-bound on maximum efficiency of an incomplete Bell-measurement in a restricted set-up consisting only of linear-elements and photodetectors. In paper IV I take a more general approach and find the first characterization of the set of POVMs that is possible to do on two qubits using linear-elements and photodetectors. This work also generalizes to $d \times d$ bipartite systems where qudits are represented in indistinguishable particles —both bosons and fermions. It is

very peculiar how quantum information is distributed when indistinguishable particles encoding two qubits are brought together in a linear device, and how photodetectors access to this information. This is not only of practical significance, making possible the use of optical photons in quantum information processing, but it also raises fundamental questions. In the same way that the natural locality constraints have boosted the study of the LOCC (Local Operations and Classical Communication), I feel that the class of realizable operations on i-qudits by linear elements can spark a similar interest.

Even if linear-elements most probably cannot account for all the storage, transmission, and processing requirements in every quantum information protocol, I believe that they can prove extremely useful in combination with more sophisticated tools, viz. cavities, non-linear crystals, ensemble of atoms or solid state devices, which would only be reserved for specialized tasks.

Paper V proposes adaptive absorption as a method to extract a single photon (or any given number of photons) from an arbitrary field mode by using only linear-elements and a very simple feed-back mechanism. Analogously adaptive amplification (mediated by an active liner element) could be used to add single excitations to a field mode. A combination of both methods can lead to interesting processes such as "non-absorbing" photon counting. Based on the idea of adaptive absorption, Paper VI puts forward a realistic eavesdropping attack on realistic quantum key distribution implementations.

In paper VII we leave the ideal world of linear optics and delve into the complex world of atoms and molecules to give a theoretical proposal for the creation a novel type of quantum superposition of two recognizably distinct objects. The mere idea of creating this type of "thing" can motivate more simple schemes and can push further the range of validity of quantum mechanics. These degenerate atom-molcule systems are also suited very well for studying entanglement in many-body systems.

References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.

[2] H. Barnum, C. M. Caves, D. A. Fuchs, R. Jozsa, and B. Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818–2821, 1996.

[3] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher. General fidelity limit for quantum channels. *Physical Review A*, 54(6):4707–4711, 1996.

[4] John S. Bell. *Speakable and unspeakable in quantum mechanics: collected papers on quantum philosophy.* Cambridge University Press, Cambridge, 1987.

[5] P. Benioff. Quantum-mechanical Hamiltonian models of Turing-machines. *Journal of Statistical Physics*, 29(3):515–546, 1982.

[6] C. H. Bennett. The thermodynamics of computation - a review. *International Journal of Theoretical Physics*, 21(12):905–940, 1982.

[7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems and Signal Processing.*, pages 175–179. IEEE, New York, 1984.

[8] 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.

[9] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722–725, 1996.

[10] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[11] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070–1091, 1999.

[12] C. H. Bennett and R. Landauer. The fundamental physical limits of computation. *Scientific American*, 253(1):48–56, 1985.

[13] C. H. Bennett and S. J. Wiesner. Communication via one-particle and 2-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[14] Rajendra Bhatia. *Matrix analysis*. Graduate texts in mathematics ; 169. Springer, New York, 1997.

[15] Jorge Luis Borges. *Ficciones (1935-1944)*. Sur, Buenos Aires, 1944.

[16] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 80(6):1121–1125, 1998.

[17] S. Bose, V. Vedral, and P. L. Knight. Multiparticle generalization of entanglement swapping. *Physical Review A*, 57(2):822–829, 1998.

[18] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[19] S. L. Braunstein. Squeezing as an irreducible resource. *quant-ph/9904002*, 1999.

[20] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi. Universal teleportation with a twist. *Physical Review Letters*, 84(15):3486–3489, 2000.

[21] D. Bruss, J. Calsamiglia, and N. Lütkenhaus. Quantum cloning and distributed measurements. *Physical Review A*, 63(4):042308, 2001.

[22] 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.

[23] D. Bruss, A. Ekert, and C. Macchiavello. Optimal universal quantum cloning and state estimation. *Physical Review Letters*, 81(12):2598–2601, 1998.

[24] Paul Busch, Pekka Lahti, and Peter Mittelstaedt. *The quantum theory of measurement*. Lecture notes in physics. Springer-Verlag, Berlin, 1991.

[25] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844–1852, 1996.

[26] V. Bužek, M. Hillery, and F. Werner. Universal-NOT gate. *Journal of Modern Optics*, 47(2-3):211–232, 2000.

[27] A. Cabello. Quantum key distribution in the Holevo limit. *Physical Review Letters*, 85(26):5635–5638, 2000.

[28] J. Calsamiglia. Generalized measurements by linear elements. *to appear Physical Review A (February 2002), quant-ph/0108108*, 2001.

[29] J. Calsamiglia, S. M. Barnett, and N. Lütkenhaus. Conditional beam splitting attack on quantum key distribution. *to appear Physical Review A (December 2001), quant-ph/0107148*, 2001.

[30] J. Calsamiglia, S. M. Barnett, N. Lütkenhaus, and K.-A. Suominen. Removal of a single photon by adaptive absorption. *Physical Review A*, 64(4):043814, 2001.

[31] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B - Lasers and Optics*, 72(1):67–71, 2001.

[32] J. Calsamiglia, M. Mackie, and K.-A. Suominen. Superposition of macroscopic numbers of atoms and molecules. *Physical Review Letters*, 87(16):160403, 2001.

[33] R. A. Campos, B. E. A. Saleh, and M. C. Teich. Quantum-mechanical lossless beam splitter - SU(2) symmetry and photon statistics. *Physical Review A*, 40(3):1371–1384, 1989.

[34] Howard Carmichael. *An open systems approach to quantum optics*. Lecture notes in physics. Springer-Verlag, Berlin, 1993.

[35] A. Carollo and G. M. Palma. The role of auxiliary states in state discrimination with linear optical devices. *quant-ph/0106041*, 2001.

[36] A. Carollo, G. M. Palma, C. Simon, and A. Zeilinger. Linear optical implementation of nonlocal product states and their indistinguishability. *Physical Review A*, 64(2):022318, 2001.

[37] N. J. Cerf, C. Adami, and P. G. Kwiat. Optical simulation of quantum logic. *Physical Review A*, 57(3):R1477–R1480, 1998.

[38] A. Chefles. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*, 239(6):339–347, 1998.

[39] A. Chefles and S. M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics Letters A*, 250(4-6):223–229, 1998.

[40] A. Chefles and S. M. Barnett. Quantum state separation, unambiguous discrimination and exact cloning. *Journal of Physics A - Mathematical and General*, 31(50):10097–10103, 1998.

[41] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum mechanics*. Wiley Interscience, New York, 1977.

[42] M. Czachor and M. Kuna. Complete positivity of nonlinear evolution: A case study. *Physical Review A*, 58(1):128–134, 1998.

[43] E. B. Davies. Information and quantum measurement. *IEEE Transactions on Information Theory*, 24(5):596–599, 1978.

[44] R. Derka, V. Bužek, and A. K. Ekert. Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement. *Physical Review Letters*, 80(8):1571–1575, 1998.

[45] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Series A - Mathematical, Physical and Engineering Sciences*, 400(1818):97–117, 1985.

[46] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 1982.

[47] D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126(5-6):303–306, 1988.

[48] L. M. Duan and G. C. Guo. Probabilistic cloning and identification of linearly independent quantum states. *Physical Review Letters*, 80(22):4999–5002, 1998.

[49] L. M. Duan and G. C. Guo. A probabilistic cloning machine for replicating two non-orthogonal states. *Physics Letters A*, 243(5-6):261–264, 1998.

[50] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[51] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, 1982.

[52] See the special issue on quantum information implementations in. *Fortschritte der Physik*, 48(9-11), 2000.

[53] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory*. PhD thesis, University of New Mexico, 1995. quant-ph/9601020.

[54] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998.

[55] N. Gisin. Nonlocality criteria for quantum teleportation. *Physics Letters A*, 210(3):157–159, 1996.

[56] N. Gisin. Quantum cloning without signaling. *Physics Letters A*, 242(1-2):1–3, 1998.

[57] N. Gisin and S. Massar. Optimal quantum cloning machines. *Physical Review Letters*, 79(11):2153–2156, 1997.

[58] N. Gisin and I. C. Percival. The quantum-state diffusion-model applied to open systems. *Journal of Physics A - Mathematical and General*, 25(21):5677–5691, 1992.

[59] N. Gisin and S. Popescu. Spin flips and quantum information for antiparallel spins. *Physical Review Letters*, 83(2):432–435, 1999.

[60] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[61] D. Gottesman, A. Kitaev, and J. Preskill. Encoding a qubit in an oscillator. *Physical Review A*, 64(1):012310, 2001.

[62] L. K. Grover. A fast quantum mechanical algorithm for database search. In *28th ACM Symposium on Theory of Computation*, page 212, New York, 1996. Association for Computing Machinery.

[63] J. B. Hartle. Quantum mechanics of individual systems. *American Journal of Physics*, 36(8):704–&, 1968.

[64] Carl W. Helstrom. *Quantum detection and estimation theory.* Mathematics in science and engineering ; 123. Academic Press, New York, 1976.

[65] A. S. Holevo. Information theoretical aspects of quantum measurements. *Probl. Inform. Transm.*, 9:177–183, 1973.

[66] Aleksandr Semenovic Holevo. *Probabilistic and statistical aspects of quantum theory.* North-Holland series in statistics and probability, 1. North-Holland Publishing Company, Amsterdam, 1982.

[67] Roger A. Horn and Charles R. Johnson. *Topics in matrix analysis.* Cambridge University Press, New York, 1991.

[68] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: Necessary and sufficient conditions. *Physics Letters A*, 223(1-2):1–8, 1996.

[69] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60(3):1888–1898, 1999.

[70] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density-matrix. *Physics Letters A*, 183(1):14–18, 1993.

[71] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *quant-ph/0107017*, 2001.

[72] I. D. Ivanovic. How to differentiate between nonorthogonal states. *Physics Letters A*, 123(6):257–259, 1987.

[73] G. Jaeger and A. Shimony. Optimal distinction between 2 nonorthogonal quantum states. *Physics Letters A*, 197(2):83–87, 1995.

[74] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[75] R. Jozsa and B. Schumacher. A new proof of the quantum noiseless coding theorem. *Journal of Modern Optics*, 41(12):2343–2349, 1994.

[76] R. S. Kennedy. On the optimum receiver for M-ary linearly independent pure state problem. *M.I.T. Res. Lab. Electron. Quart. Progr. Rep.*, 108:219–225, 1973.

[77] J. Kim, O. Benson, H. Kan, and Y. Yamamoto. A single-photon turnstile device. *Nature*, 397(6719):500–503, 1999.

[78] Y. H. Kim, S. P. Kulik, and Y. Shih. Quantum teleportation of a polarization state with a complete Bell state measurement. *Physical Review Letters*, 86(7):1370–1373, 2001.

[79] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[80] P. Kok and S. L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Physical Review A*, 61(4):042304, 2000.

[81] M. Koštrun, M. Mackie, R. Côté, and J. Javanainen. Theory of coherent photoassociation of a Bose-Einstein condensate. *Physical Review A*, 62(6):063616, 2000.

[82] Karl Kraus. *States, effects, and operations : fundamental notions of quantum theory.* Lecture notes in physics ; 190. Springer-Verlag, Berlin, 1983.

[83] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White. Grover's search algorithm: an optical approach. *Journal of Modern Optics*, 47(2-3):257–266, 2000.

[84] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard. Ultrabright source of polarization-entangled photons. *Physical Review A*, 60(2):R773–R776, 1999.

[85] F. Laloë. Do we really understand quantum mechanics? Strange correlations, paradoxes, and theorems. *American Journal of Physics*, 69(6):655–701, 2001.

[86] A. Lamas-Linares, J. C. Howell, and D. Bouwmeester. Stimulated emission of polarization-entangled photons. *Nature*, 412(6850):887–890, 2001.

[87] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, 1961.

[88] R. Landauer. Information is physical. *Physics Today*, 44(5):23–29, 1991.

[89] J. I. Latorre, P. Pascual, and R. Tarrach. Minimal optimal generalized quantum measurements. *Physical Review Letters*, 81(7):1351–1354, 1998.

[90] Ulf Leonhardt. *Measuring the quantum state of light*. Cambridge studies in modern optics. Cambridge Univ. Press, Cambridge, 1997.

[91] C. K. Li and S. Pierce. Linear preserver problems. *American Mathematical Monthly*, 108(7):591–605, 2001.

[92] G. Lindblad. Generators of quantum dynamical semigroups. *Communications in Mathematical Physics*, 48(2):119–130, 1976.

[93] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, 2000.

[94] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. Bell measurements for teleportation. *Physical Review A*, 59(5):3295–3300, 1999.

[95] C. Marand and P. D. Townsend. Quantum key distribution over distances as long as 30 km. *Optics Letters*, 20(16):1695–1697, 1995.

[96] S. Massar and S. Popescu. Optimal extraction of information from finite quantum ensembles. *Physical Review Letters*, 74(8):1259–1263, 1995.

[97] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in experimental quantum communication. *Physical Review Letters*, 76(25):4656–4659, 1996.

[98] D. Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, 2001.

[99] K. Mølmer. Optical coherence: A convenient fiction. *Physical Review A*, 55(4):3195–3203, 1997.

[100] T. Mor and P. Horodecki. Teleportation via generalized measurements, and conclusive teleportation. *quant-ph/9906039*, 1999.

[101] M. A. Neumark. Spectral functions of a symmetric operator. *Izv. Akad. Nauk SSSR, Ser. Mat.* , 4:277–318, 1940.

[102] M. A. Nielsen and G. Vidal. Majorization and the interconversion of bipartite states. *Quantum Information and Computation*, 1(1):76–93, 2001.

[103] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, 2000.

[104] Roland Omnès. *The interpretation of quantum mechanics*. Princeton series in physics. Princeton University Press, Princeton, N.J., 1994.

[105] M. Ozawa. Quantum measuring processes of continuous observables. *Journal of Mathematical Physics*, 25(1):79–87, 1984.

[106] J. W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403(6769):515–519, 2000.

[107] A. Peres. What is a state-vector. *American Journal of Physics*, 52(7):644–650, 1984.

[108] A. Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128(1-2):19–19, 1988.

[109] A. Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413–1415, 1996.

[110] A. Peres and D. R. Terno. Optimal distinction between non-orthogonal quantum states. *Journal of Physics A - Mathematical and General*, 31(34):7105–7111, 1998.

[111] Asher Peres. *Quantum Theory: Concepts and Methods*. Kluwer, Dordrecht, 1993.

[112] S. Popescu. An optical method for teleportation. *quant-ph/9501020*, 1995.

[113] M. Reck. *Quantum Interferometry with Multiports: Entangled Photons in Optical Fibers*. PhD thesis, Innsbruck University, 1996. http://www.uebersetzung-reck.de/physics/entangled.htm.

[114] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58–61, 1994.

[115] A. Royer. Reduced dynamics with initial correlations, and time-dependent environment and Hamiltonians. *Physical Review Letters*, 77(16):3272–3275, 1996.

[116] T. Rudolph and B. C. Sanders. Requirement of optical coherence for continuous-variable quantum teleportation. *Physical Review Letters*, 87(7):077903, 2001.

[117] Bahaa E. A. Saleh and Malvin Carl Teich. *Fundamentals of photonics*. Wiley series in pure and applied optics. Wiley, New York, 1991.

[118] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, and O. Hirota. Accessible information and optimal strategies for real symmetrical quantum sources. *Physical Review A*, 59(5):3325–3335, 1999.

[119] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23:807–812;823–828;844–849, 1935.

[120] B. Schumacher. Quantum coding. *Physical Review A*, 51(4):2738–2747, 1995.

[121] B. Schumacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54(4):2614–2628, 1996.

[122] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[123] C. E. Shannon. Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28:656–715, 1949.

[124] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Fundamentals of Computer Science*, Los Alamitos, CA, 1994. IEEE Press.

[125] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493–R2496, 1995.

[126] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

[127] C. Simon, G. Weihs, and A. Zeilinger. Optimal quantum cloning via stimulated emission. *Physical Review Letters*, 84(13):2993–2996, 2000.

[128] Simon Singh. *The science of secrecy : the secret history of codes and codebreaking*. Fourth Estate, London, 2000.

[129] S. Song, C. M. Caves, and B. Yurke. Generation of superpositions of classically distinguishable quantum states from optical back-action evasion. *Physical Review A*, 41(9):5261–5264, 1990.

[130] A. M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793–797, 1996.

[131] S. Takeuchi, J. Kim, Y. Yamamoto, and H. H. Hogue. Development of a high-quantum-efficiency single-photon counting system. *Applied Physics Letters*, 74(8):1063–1065, 1999.

[132] B. M. Terhal and P. Horodecki. Schmidt number for density matrices. *Physical Review A*, 61(4):040301, 2000.

[133] P. Törmä and S. Stenholm. Quantum logic using polarized photons. *Physical Review A*, 54(6):4701–4706, 1996.

[134] S. J. van Enk and C. A. Fuchs. The quantum state of a laser field. *quant-ph/0104036*, 2001.

[135] G. Vidal, J. I. Latorre, P. Pascual, and R. Tarrach. Optimal minimal measurements of mixed states. *Physical Review A*, 60(1):126–135, 1999.

[136] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, 1989.

[137] R. F. Werner. Optimal cloning of pure states. *Physical Review A*, 58(3):1827–1832, 1998.

[138] R. F. Werner. All teleportation and dense coding schemes. *Journal of Physics A - Mathematical and General*, 34(35):7081–7094, 2001.

[139] John A. Wheeler and Wojciech H. Zurek. *Quantum theory and measurement*. Princeton Series in Physics. Princeton University Press, Princeton, New Jersey, 1983.

[140] S. Wiesner. Conjugate coding. *SIGACT News*, 15:78, 1983.

[141] H. M. Wiseman and G. J. Milburn. Interpretation of quantum jump and diffusion-processes illustrated on the Bloch sphere. *Physical Review A*, 47(3):1652–1666, 1993.

[142] H. M. Wiseman and G. J. Milburn. Quantum-theory of optical feedback via homodyne detection. *Physical Review Letters*, 70(5):548–551, 1993.

[143] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[144] B. Yurke and D. Stoler. Einstein-Podolsky-Rosen effects from independent particle sources. *Physical Review Letters*, 68(9):1251–1254, 1992.

[145] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. Event-ready-detectors Bell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287–4290, 1993.