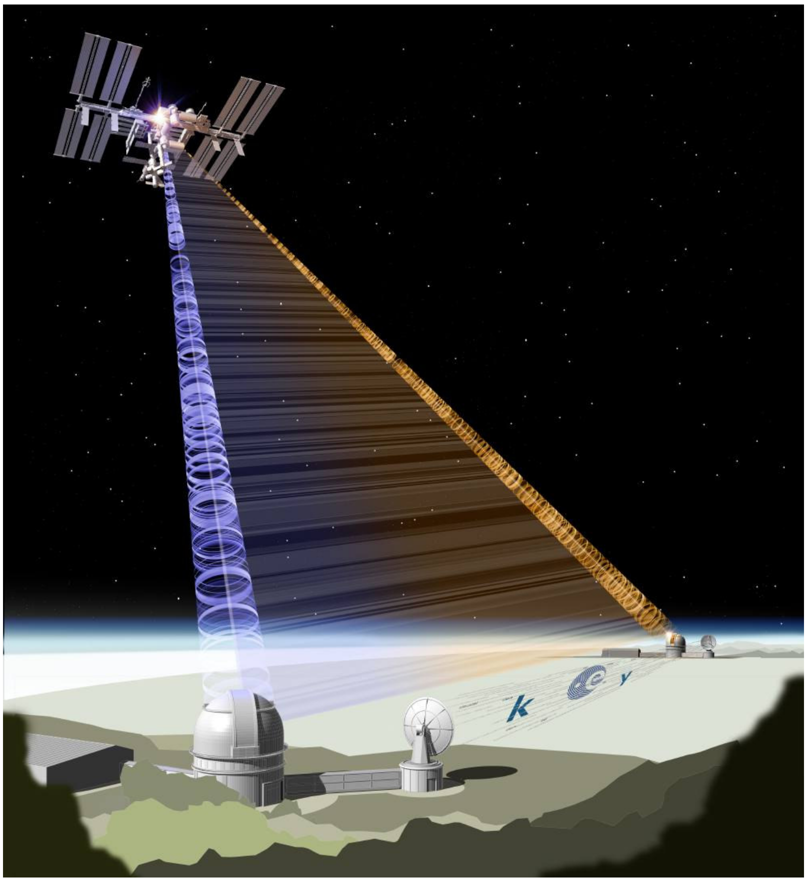
university of groningen

faculty of mathematics and natural sciences

school for natural sciences and technology

Spooky Action at Spacy Distances



Artist Impression of Space QUEST, ESA's QUantum Entanglement for Space experimenTs research project. The ISS will be outfitted with a quantum communication module, which transmits entangled photons to far-away receiving stations. If both stations obtain one of a pair of entangled photons, quantum communication between the stations is possible.

Bachelor research project

Keimpe Nevenzeel
School for Natural Sciences and Technology, University of Groningen
Group of Applied Physics, Université de Genève

Supervisors
Prof. dr. Nicolas Gisin & dr. Stefano Pironio
Group of Applied Physics, Université de Genève

Prof. dr. Marco Spaans & prof. dr. Holger Waalkens
Kapteyn Astronomical Institute & Johan Bernoulli Institute, University of Groningen

SPOOKY ACTION AT SPACY DISTANCES

KEIMPE NEVENZEEL

Group of Applied Physics, Université de Genève

Kapteyn Astronomical Institute & Johan Bernoulli Institute, University of Groningen

August 2009

Abstract

Three important quantum communication techniques have no classical counterpart: teleportation, single particle distillation and collective distillation. Of several protocols of these quantum communication techniques, the maximum obtainable efficiency is investigated. Two essential factors in the obtainable efficiency are the entanglement fraction x and the number of channels N that two distant communication partners Alice and Bob share, with x between zero and one and N smaller than infinity. If N is smaller than five, single particle distillation allows the highest efficiency while for N equal or larger than five it depends on x and N whether single particle distillation or collective distillation achieves the highest efficiency.

The ultimate application of quantum communication protocols is the establishment of a global quantum communication network. Both ESA and NASA finance extensive studies to establish such a network. ESA's program, the Space-QUEST program, currently brings the first experimental hardware up to TRL3, launch of this hardware is envisioned for 2015.

The fundamental property of quantum mechanics that allows quantum communication is non-locality. Non-local quantum states are entangled, meaning that they show stronger correlations than is possible with classical physics. A superposition of entangled states allows for quantum communication techniques. Paradoxally, superpositions of states are often observed at microscopic scales but never at macroscopic scales, although one can construct situations at which macroscopic superpositions occurs. This mismatch between theory and observations is called the macro-objectivation problem. Today, a discussion about this problem is mainly philosophical, but the loss of entanglement at the inflationary epoch may shed experimental light upon this fundamental problem.

PACS: 03.65.Ta, 03.65.Ud, 03.67.Bg, 03.67.Mn, 03.67.-a, 03.67.Hk, 04.62.+v, 42.50.Ex, 84.40.Ua and 98.80.Cq.

CONTENTS

ACKNOWLEDGEMENTS

The author gratefully acknowledges the hospitality prof. dr. N. Gisin offered at GAP, Université de Genève, Swiss, during the second semester of the academic year 2009. The author is indebted to dr. Stefano Pironio, MSc. Jean-Daniel Bancel and MSc. Cyril Branciard for fruitful discussions during the writing of this thesis and to prof. dr. M. Spaans and prof. dr. H. Waalkens for their supportive action at a distance. The Institute for Quantum Computing of the University of Waterloo, Canada, in particular director dr. R. Laflamme, prof. dr. D. Cory (MIT) and M.L. Payerl, is thanked for the excellent Undergraduate School on Experimental Quantum Information Processing, which sharpened the authors insights with regard to essential parts of this thesis.

Thanks to prof. dr. R. v.d. Weygaert, dr. ir. G. Tiesinga, prof. dr. P. Barthel, prof. dr. J. Top and prof. dr. S. Zaroubi for their trust and support in the conceptive phase of this thesis, to Markus Jakobi and Laurence Nurisso for initial support on practical matters and to Patrick Bos for providing the thesis layout.

Andrea Zelezná, Caroline Gay, Christoph Clausen, Cristine Martinez, Daniela Haviarova, Fabrizio de Robertis, Flávia Faria, Ionel Popa, Iulia Popa, Ligia Grafitescu, Marco Finessi, Markus Jakobi, Marta Serra, Rosanne van Diepen, Steve Darrow, Vasili Pankratov and Wybe Roodhuyzen are thanked for their moral support and making the authors stay in Genève more than worthwhile.

The author recognizes financial support from the Groninger Universiteits Fonds, GAP Optique, the Institute for Quantum Computing and a parental grant.

CHAPTER 1

INTRODUCTION

The advent of computer science was one of the most profound scientific revolutions in the twentieth century, both for science itself as for daily life. Cutting edge research programs like at CERN or LOFAR rely heavily on computers. In everyday life, computers evolved to an essential element in communication, finance, entertainment, ad infinitum.

The road to contemporary computer science was paved by the mathematician Alan Turing in 1936 with the development of an abstract model of a computer: the *Universal Turing Machine* [69]. A Universal Turing Machine is a computing model with a finite set of states; a finite set of symbols; an infinite 'tape' on which the head of the machine can read and write the symbols; and a transition function that determines the next state based on the current state and the current symbol the head points to. Later, the Turing Machine was also equipped with a random binary number generator. After decades of experience with computer science it is generally accepted [55] that a computational task could be performed by any computer we could theoretically build if and only if it can be performed by a probabilistic Universal Turing Machine. This result is generally stated as the following thesis.

Definition 1.1 (Classical Strong Church-Turing Thesis)**.** *A probabilistic Universal Turing Machine can efficiently simulate any realistic model of computation.*

An important word in this definition is 'efficiently', by which is meant in polynomial time[1]. Some problems cannot be solved in polynomial time but require exponential time[2]. The difference in polynomial and exponential time is an accepted way to draw the line between 'easy' and 'hard' problems. This distinction is computer independent due to a major result in computer science: any classical computer can emulate another classical computer with polynomial overhead [80]. Consequently: if a problem is polynomial on one classical computer, it will be polynomial on every classical computer.

Information theory of the twentieth century was based on classical physics. At the eve of the twenty-first century the field was revolutionized by the introduction of quantum mechanics. Within several years, the following advantages of quantum computers over classical computers were shown; many others may be lurking on the horizon.

[1]A problem can be solved in *polynomial time* if there is a $k \in \mathbb{N}$ such that the time needed to solve the problem is $cn^k + \mathcal{O}(n^{k-1})$, with n the number of bits and $c \in \mathbb{R}$.

[2]A problem can be solved in *exponential time* if the time needed to solve the problem is $cd^n + \mathcal{O}(d^{n-1})$ for some $c, d \in \mathbb{R}$

- The factorization problem[3] can be solved polynomially on a quantum computer, while it is (probably) exponential on a classical computer. [90]
- Quantum computers can simulate large quantum systems, which has many scientific and technological applications. [61, 35]
- Certain search algorithms can be substantially sped up with quantum computers. [43]
- Quantum cryptography can provide the first public key cryptographic system whose safety is not guaranteed by practical constraints like limited computer power (as todays systems), but by the very laws of nature. [14]

The facts above meant an axiomatic shift was necessary: the Turing thesis had to be adapted to quantum mechanics. The foundations of computer science had to be revised to include quantum mechanics, with classical computer science as a limit.

The elementary classical data-unit is a classical bit (*c*bit): generally a macroscopic system which can take the value 0 or 1. A n-*c*bit memory consists of 2^n states 00...00, 00...01, ..., 11...11, which can be manipulated by boolean operations.

The elementary quantum data-unit is the *qubit*: generally a microscopic system such as photons, atoms or nuclear spins. The states $|0\rangle$ and $|1\rangle$ are two good distinguishable states, for example horizontal and vertical polarization of a photon. Contrary to *c*bits , qubits can also be in the superposition of these two states, for example in the state $a|0\rangle + b|1\rangle$, with $a^2 + b^2 = 1$. A n-qubit state consists of any state of the form

$$|\psi\rangle = \sum_{i=00...0}^{11...1} c_i|x\rangle \tag{1.1}$$

with $\Sigma_i c_i^2 = 1$. Thus a qubit is a vector of unit length in a 2^n-dimensional Hilbert space. The exponential large dimensionality of qubit space compared to classical space is an important reason for the fact that quantum computers can provide an exponential speedup for certain tasks.

Quantum information can be communicated by sending quantum states (of qubits) around. The ways to do so will now be investigated in more detail; we will use several technical terms loosely, they will be defined more precisely in the chapters to come.

Consider two spatially separated observers Alice and Bob and suppose Alice wants to send qubit 1 in state $|\phi\rangle_1$ to Bob. Of course, the particle with the state can be send itself, but that is not always practical, for example because the fragile quantum state will probably decay in the process. Instead, suppose Alice and Bob share a quantum channel consisting of the pure noisy state

$$|\psi\rangle_{ab} = \xi(|00\rangle + x|11\rangle)_{ab} \tag{1.2}$$

with $x \in [0, 1]$ and the normalisation factor $\xi = 1/(1 + x^2)$. If she would send qubit 1 directly through the channel Bob will end up with a different state than Alice sent, because the channel is noisy. So, some other technique has to be employed:

Quantum error correction codes : the quantum version of classical error correction codes used every day in digital systems. A major drawback is that quantum error correction is fundamentally more difficult than its classical counterpart. Furthermore, this technique places significant restrictions on the channel between Alice and Bob.

[3] The problem of factoring an integer in its primes. This problem is of great practical value because modern public key cryptographic methods are based on the assumption that the factorization of a large integer is impossible from a practical perspective because it requires exponential time.

Probabilistic teleportation : a technique without classical counterpart. Alice creates locally a maximally entangled pair of particles and then teleports one of the particles pair using the quantum channel. With probability p Alice and Bob end up sharing a maximally entangled pair, while with probability $1 - p$ they loose the channel.

Single particle distillation : procedures which 'distill' maximally entangled states from noisy states, without having to resort to a local maximally entangled state.

Collective distillation : distillation over multiple quantum channels $(ab)_1, (ab)_2, ..., (ab)_n$ simultaneously. Because quantum channels are superadditive[4], the success probability of collective distillation can be higher than that of single particle distillation.

This thesis compares the efficiency of several protocols of all techniques without classical counterpart, the last three techniques, as function of the 'entanglement fraction' x. Both (future) applications of the theory developed in this thesis as well as better understanding the philosophical background behind the theory lead us ultimately to space. Therefore, *two key astrophysical applications of quantum entanglement will be investigated: the establishment of a global quantum communication network and inflationary entanglement.*

The structure of this thesis is as follows: first the physical and mathematical fundaments are constructed in chapter 3. With the fundaments in place one of the most counter intuitive properties of quantum mechanics is investigated in chapter 4: entanglement, sarcastically described by Einstein as *spooky action on a distance*. Familiarity with these concepts allows us to take a closer look at quantum teleportation in chapter 5 and quantum distillation in chapter 6. For both, various protocols to create optimal quantum channels will be examined. Generalizations of the scenario described above are studied in chapter 7, with most of the attention on the tripartite case. Chapter 8.1 discusses the 'ultimate application' of quantum channels: establishing a global quantum communication network.

But first, chapter 2 describes the philosophical origins of the concept of non-locality, the basis of what is to follow. Fascinatingly, future work on inflationary entanglement might place the philosophical discussions in this chapter on firm empirical grounds, as described in chapter 8.2. The conclusions and a summary are presented in chapter 9.

[4]More information can be send if n channels are used in parallel than with n separate channels.

CHAPTER 2

PHILOSOPHICAL PRELUDE - THE FALL OF LOCALITY

"God does not play dice."
Albert Einstein

"Einstein, stop telling God what to do."
Niels Bohr

It started as a physical debate over the completeness of quantum mechanics, but on a deeper level it was actually about one of the most fundamental questions in science: what does physical knowledge mean, and what can one objectively know about Nature? It was a debate between giants, men who had shaped the physics as we know it today. On one side there was Niels Bohr, one of founders of quantum theory. In his view, quantum physics and its philosophical interpretation were completed. The theory had heralded a new age in science, an age in which mankind had to accept that it would never know the objective reality out there, but just the shadows of it, seen through classical glasses. His opponent was no-one less then Albert Einstein, who refused till the end of his life to accept a theory as complete if it would not describe an objective world that would be there independent of observers. "Do you really believe the moon is not there if you are not looking at it?", Einstein asked Pais once.

> *"It was delightful for me to be present during the conversations between Bohr and Einstein. Like a game of chess. Einstein all the time with new examples. In a certain sense a perpetuum mobile of the second kind to break the uncertainty relation. Bohr from out of philosophical smoke clouds constantly searching for the tools to crush one example after the other. Einstein like a jack-in-the-box: jumping out fresh every morning."*
>
> Ehrenfest to Goudsmit et al, 1927

The Bohr-Einstein debate culminated with an ingenious paper written by Einstein, Podolsky and Rosen (from here on EPR). This paper was supposed to be a reductio ad absurdum argument against the completeness of quantum mechanics, but in a perhaps ironical twist of fate the main idea of the paper would establish quantum mechanics firmer than ever before. The true value of the paper was not recognized directly, however. It would take about thirty years until the "paradox" posed by EPR was solved. In this chapter, we will discuss the EPR paper, Bohr's response and the modern interpretation of the paper. Lastly, we will touch upon problems with the interpretation of quantum mechanics which remain until today. To be able to place the paper and the arguments therein better, first the scientific-philosophical world views of our two antagonists are investigated.

2.1 Bohr's position

Bohr was one of the founding fathers of quantum mechanics and played an influential role in the earlier philosophical interpretation of the theory [5]. But although he was seen as a hero in the eyes of his contemporaries, most modern philosophers consider his writings and arguments therein hard to follow or even internally inconsistent. To quote Scheibe, an important commentator on Bohr:

> *"Bohr's mode of expression and manner of argument are individualistic sometimes to the point of being repellent ... Anyone who makes a serious study of Bohr's interpretation of quantum mechanics can easily be brought to the brink of despair."*

Bohr thought that classical physics is based on the belief that the world can be described at least partly without reference to the observer. In other words: in classical physics objects exist independent of observation. For quantum physics this belief doesn't hold: in the quantum regime facts about objects only come into being after measurement [36]. According to Bohr's philosophy, *the principle of complementarity*, the act of measuring a quantum object with a classical device introduces an uncontrollable disturbance in both systems. In the measuring device, the disturbance produces the result. Because the disturbance is uncontrollable, results can be predicted only statistically. In the quantum object, this disturbance alters the value of all observables which don't commute with the observable being measured. This leads to the Uncertainty Principle. The best we can do is to give an objective *description* of physics, by stating the results of our measurements in classical terms.

So if all what we know of the world is due to classically stated measurement results, what is the state of a quantum system before measurement? (Through which slit goes an electron in a two-slit experiment?) Bohr's answer is simple: we don't know and we can never know. One can only ask meaningfull questions about a system which we measure, any questions about reality without measurement is not within the realm of physics.

2.2 Einstein's position

According to Einstein quantum mechanics was as a nice theory, but he considered Bohr's ontological way out of fundamental questions about the interpretation of quantum mechanics unsatisfactory. For centuries physicists had developed theories which tried to explain the objective world 'out there', independent of the existence of an observer, and Einstein was not prepared to abandon this ideal of physics. He thought quantum mechanics only gave a probabilistic answers to some questions because it was not a complete theory: there are 'hidden' variables that co-determine the outcome of quantum experiments. If these variables would be known the probabilistic nature of quantum mechanical predictions would disappear and physical objects would also be real without measurement. His *Trennungsprinzip* (separability principle) provided the criterion to define distinct objects as real: real objects could be distinguished from each other if they were spatially separated. Let Einstein speak for himself:

> *" It is characteristic of these physical things [i.e. bodies, fields, etc.] that they are conceived of as being arranged in a space-time continuum. Further, it appears to be essential for this arrangement of the things introduced in physics that, at a specific time, these things claim an existence independent of one another, insofar as these things "lie in different parts of space". Without such an assumption of the mutually independent existence (the "being-thus") of spatially distant things, an assumption which originates in everyday thought, physical thought in the sense familiar to us would not be possible. Nor does one see how physical laws could be formulated and tested without such a clean separation.*
> ...
> *For the relative independence of spatially distant things A and B, this idea is characteristic: an external influence on A has no immediate effect on B; this is known as the principle of 'local action', which is applied consistently only in field theory. The complete suspension of this basis principle would make impossible the idea of the existence of (quasi-) closed systems and, thereby, the establishment of empirically testable laws in the sense familiar to us."*

Although at the time the physics community had embraced Bohr's views, Einstein would oppose the belief in completeness of quantum physics till the end of his life.

> *"He had a certain belief that - not that he said it in those words but that is the way I read him personally - that he had a sort of special pipeline to God, you know. ... He had these images of ... that his notion of simplicity that that was the one that was going to prevail."*
>
> Pais about Einstein [57]

2.3 The EPR paper

The epistemological battle between Bohr and Einstein raged for decades. In one of the later stages of the 'war', EPR wrote a paper entitled "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" [32]. This paper employed a reduction ad absurdum argument to show the incompleteness of quantum mechanics, where the following condition of completeness was used:

Definition 2.1 ((necessary) condition for completeness of a physical theory)**.** *Every element of the physical reality must have a counterpart in the physical theory.*

Here, EPR give the following sufficiency conditions for elements of physical reality:

Definition 2.2 (elements of reality (sufficiency condition))**.** *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*

From these definitions, they arrive at the following argument:

> *"... it is shown in quantum mechanics that, if the operators corresponding to two physical quantities, say A and B, do not commute, that is, if $AB \neq BA$, then the precise knowledge of one of them precludes such a knowledge of the other. Furthermore, any attempt to determine the latter experimentally will alter the state of*

> *the system in such a way as to destroy the knowledge of the first. From this follows that either:* (1) the quantum-mechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality." *[32]*

Now suppose we have a system with two subsystems, I and II, which interacted at a certain moment in the past. Their combined wave function is given by $\psi(x_1, x_2)$, where x_1 and x_2 are the variables used to describe the first and second system respectively. Let $a_1, a_2, a_3, ...$ be the eigenvalues of physical quantity A of system I with corresponding orthogonal eigenvectors $\alpha_1(x_1), \alpha_2(x_1), \alpha_3(x_1), ...$ Then we can write:

$$\psi(x_1, x_2) = \sum_{i=1}^{\infty} \alpha_i(x_1)\beta_i(x_2) \tag{2.1}$$

with $\beta_i(x_2)$ the corresponding coefficients for system II. The set of vectors α_i was determined by the physical quantity A. If instead of A we had chosen another quantity, say B with eigenvalues $c_1, c_2, c_3, ...$ and corresponding system I eigenvectors $\chi_1(x_1), \chi_2(x_1), \chi_3(x_1), ...$ then we can write

$$\psi(x_1, x_2) = \sum_{i=1}^{\infty} \chi_i(x_1)\gamma_i(x_2) \tag{2.2}$$

with $\gamma_i(x_2)$ coefficients for system II. If we measure A and found a certain a_k, system 2.1 will collapse in state $\alpha_k(x_1)\beta_k(x_2)$, while if we measure B and found a certain c_l, system 2.2 will collapse into state $\chi_l(x_1)\gamma_l(x_2)$.

> *"We see therefore that, as a consequence of two different measurements performed upon the first system, the second system may be left in states with two different wave functions. On the other hand, since at the time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system. ... Thus,* it is possible to assign two different wave functions (in our example β_k and γ_l) to the same reality (the second system after interaction with the first).
> ...
> *Previously we proved that either (1) the quantum-mechanical description of reality given by the wave function is not complete or (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality. Starting then with the assumption that the wave function does give a complete description of the physical reality we arrived at the conclusion that two physical quantities, with non-commuting operators, can have simultaneous reality. Thus the negation of (1) leads to the negation of the only other alternative (2). We are thus forced to conclude that the quantum-mechanical description of physical reality given by wave functions is not complete."* *[32]*

The first lines of this quote contain Einstein's Trennungsprinzip: when two systems are spatially separated they are two distinguishable systems and thus two different systems; hence, measurement on one of them cannot instantaneously influence the other.

Contrary to modern view, the Bohr-camp considered the problem EPR raised to be only another variation of earlier problems raised by Einstein which they had solved long ago. Their reaction varied between surprise that Einstein considered the problem worthwhile for publication to outright irritation. To quote Pauli:

> *"Einstein has once again made a public statement about quantum mechanics ... As is well known, that is a disaster whenever it happens. "Because, so he concludes razor-sharply, - nothing can exist if it ought not exist" (Morgenstern). Still, I must grant him that if a student in one of their earlier semesters had raised such objections, I would have considered him quite intelligent and promising. ... Thus it might anyhow be worthwhile if I waste paper and ink in order to formulate those inescapable facts of quantum mechanics that cause Einstein special mental troubles."*
> Pauli to Heisenberg, June 15, 1935

Within two months of the publication of the EPR paper, Bohr had written a response [15], which would be published in the same journal and under the same title as the original EPR paper. In this paper, Bohr states that:

> *"[The EPR] argumentation, however, would hardly seem suited to affect the soundness of quantum-mechanical description which is based on a coherent mathematical formalism covering automatically any procedure of measurement like that indicated. The apparent contradiction in fact discloses only an essential inadequacy of the customary viewpoint of natural philosophy for a rational account of physical phenomena of the type with which we are concerned in quantum mechanics ... the necessity of a final renunciation of the classical ideal of causality and a radical revision of our attitude towards the problem of physical reality." [15]*

In the paper, Bohr discussed in length the difference between the objective reality and observers, the influence of measurements on the object and what we can know of the physical reality by means of quantum mechanics:

> *"Indeed we have in each experimental arrangement suited for the study of proper quantum phenomena not merely to do with an ignorance of the value of certain physical quantities, but with the impossibility of defining these quantities in an unambiguous way. The last remarks apply equally well to the special problem treated by Einstein, Podolsky and Rosen..." [15]*

Thus the concrete scientific question EPR posed was answered with a doubtful metaphysical discourse, the question itself was not addressed. Nevertheless, for decades Bohr's answer would dominate main-stream physics. EPR's attempt to retain realism in physics was seen as outdated, in modern physics questions about objects "beyond measurement" ought not to be asked.

2.4 Completeness versus locality

Although Bohr responded fast, today it is generally agreed that Bohr's response to EPR is fuzzy at least, some commentators even deny its coherence and see it as oracular [5]. So in absence of a intelligible response, let's analyze the arguments of EPR a bit closer ourselves. After their definitions of completeness and elements of reality, EPR tries to show the following claims:

1. A quantum mechanical system is *either* incomplete (in the sense that it does not adhere to definition 2.1) *or* non-commuting observables don't have simultaneous reality.

2. If quantum mechanics is complete ⇒ two non-commuting observables have simultaneous reality.

To prove the first claim, note that if both non-commuting observables would have simultaneous reality, they would be a part of the complete description of reality. If then quantum mechanics would provide a complete description, they would both be predictable. However, contemporary quantum mechanics states that the values of two non-commuting observables cannot be predicted both, thus either contemporary quantum mechanics is incomplete or the observables really can't have reality at the same time.

To prove the second claim, EPR consider the system with particles I and II described earlier and make implicitly the assumption of locality, where locality is defined as:

Definition 2.3 (Locality)**.** *The assumption that Alice's measurement cannot instantaneously influence the result of Bob's measurement.*

Assume reality and locality hold, an assumption named *local realism*. If Alice would measure the position of her particle, she knows the position of Bob's particle as well and the position of Bob's particle would be real. Due to locality, a measurement at Alice's side can't instantaneously influence Bob's side, so the position of Bob's particle has to be real even if Alice doesn't measure position. Analogously, if Alice would perform a measure the momentum of her particle, she knows the momentum of Bob's particle and the momentum of Bob's particle is real, even if she doesn't actually perform the measurement. Consequently, position and momentum of Bob's particle are simultaneously real, which finishes the prove of claim 2. Thus if local realism holds and we assume quantum mechanics is complete, it follows from claim 2 that two non-commuting observables have simultaneous reality, which is in contradiction with claim 1. Consequently, under this assumption quantum mechanics is incomplete [36].

For decades the choice between completeness or local realism remained philosophical, a matter of taste more than of decisive argument. The world had to wait for almost thirty years before the choice could be resolved in a scientific way.

2.5 Bell's inequalities

In 1964 John Bell wrote an ingenious article in which he proposed a mathematical criterion to determine whether a physical theory supports local realism or not [11]. Because an experimental test of Bell's criterion was difficult, Clauser *et al* generalized Bell's work to the CHSH inequality [26]. The CHSH inequality measures the degree of correlation between observables. First, the CHSH inequality is developed. Then, this inequality is applied to quantum mechanics.

2.5.1 The CHSH inequality

Suppose Alice and Bob both have a particle and carry out two measurements. Let a, a' and b, b' be the possible measurement settings of the devices of Alice respectively Bob. Define λ as (a vector of) hidden variables: properties of the system that we can't necessarily measure. The hidden variables have a probability distribution $f(\lambda)$, with $\int f(\lambda)\, d\lambda = 1$. Let $A(a, \lambda)$ and $B(b, \lambda)$ be Alice's and Bob's measurement outcomes. Assume that measurement will simply reveal a preexisting value (reality), for simplicity $+1$ or -1. Then the degree of correlation E between A and B is given as:

$$E(a,b) = \langle AB \rangle \tag{2.3}$$

Locality can be imposed by demanding that A does not depend on b and vice versa, which gives the following correlation function:

$$E(a,b) = \langle \int f(\lambda) A(a,\lambda) B(b,\lambda)\, d\lambda \rangle \tag{2.4}$$

Under the assumptions above:

$$\begin{cases} B(b,\lambda) + B(b',\lambda) = \pm 2 \\ B(b,\lambda) - B(b',\lambda) = 0 \end{cases} \tag{2.5}$$

or the other way around. Consider the following combination of correlations:

$$\begin{aligned} &|E(a,b) + E(a,b') + E(a',b) - E(a',b')| && (2.6)\\ =&|\langle \int f(\lambda) \left[A(a,\lambda)B(b,\lambda) + A(a,\lambda)B(b',\lambda) + A(a',\lambda)B(b,\lambda) - A(a',\lambda)B(b',\lambda)\right]\, d\lambda\rangle| \\ =&|\langle \int f(\lambda)A(a,\lambda)\left[B(b,\lambda) + B(b',\lambda)\right] + f(\lambda)A(a',\lambda)\left[B(b,\lambda) - B(b',\lambda)\right]\rangle| && (2.7)\\ \leq& 2 \end{aligned}$$

where for the last step the average of the probability distribution $f(\lambda)$ was taken. This is the CHSH inequality:

$$|E(a,b) + E(a,b') + E(a',b) - E(a',b')| \leq 2 \tag{2.8}$$

Thus, if the outcome of B is independent of A, the maximum absolute value of the combination of the correlations of equation 2.8 is 2. Note that this is a mathematical result, it does not depend on any specific physical theory. The CHSH inequality can be used to check whether quantum mechanics is a local theory. If the inequality holds, locality might hold. Otherwise, it has to be discarded, in quantum mechanics and in any other conceivable physical theory.

2.5.2 CHSH in quantum mechanics

Consider the following spin EPR pair:

$$|\psi\rangle^- = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \tag{2.9}$$

Alice and Bob choose the measurements:

$$\begin{aligned} a &= Z_1 & b &= -\tfrac{1}{\sqrt{2}}(Z_2 + X_2) \\ a' &= X_1 & b' &= \tfrac{1}{\sqrt{2}}(-Z_2 + X_2) \end{aligned} \tag{2.10}$$

This gives (assuming a uniform distribution for λ):

$$\begin{aligned} E(a,b) &= -\tfrac{1}{\sqrt{2}}\left(\langle Z_1 Z_2\rangle + \langle Z_1 X_2\rangle\right) = \tfrac{1}{\sqrt{2}} \\ E(a,b') &= \tfrac{1}{\sqrt{2}}\left(-\langle Z_1 Z_2\rangle + \langle Z_1 X_2\rangle\right) = \tfrac{1}{\sqrt{2}} \\ E(a',b) &= -\tfrac{1}{\sqrt{2}}\left(\langle X_1 Z_2\rangle + \langle X_1 X_2\rangle\right) = \tfrac{1}{\sqrt{2}} \\ E(a',b') &= \tfrac{1}{\sqrt{2}}\left(-\langle X_1 Z_2\rangle + \langle X_1 X_2\rangle\right) = -\tfrac{1}{\sqrt{2}} \end{aligned} \tag{2.11}$$

Consequently,

$$|E(a,b) + E(a,b') + E(a',b) - E(a',b')| = 2\sqrt{2} > 2 \tag{2.12}$$

Interestingly, it seems that quantum mechanics can break the CHSH inequality and thus it cannot be a local theory! This stunning prediction was experimentally confirmed by Aspect *et al* in 1982 [7] and many times thereafter. The experimental setup is shown in figure 2.1. Source S emits an entangled pair of photons which go to polarizers I and II. Depending on the polarization of the photons, they go either to the $//$ or to the $\perp$ direction. With help of three detectors, all single counts are filtered out and with a fourfold coincidence technique $E(a,b)$ can be measured in a single run. By rotation of the polarimeter the other correlation coefficients can be measured.

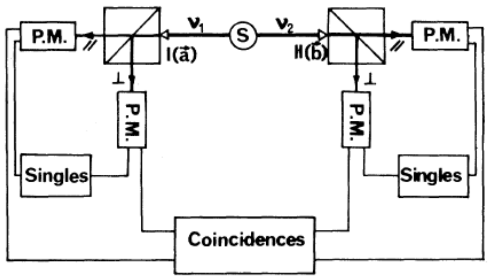


Figure 2.1: *[7] Experimental setup of Aspect's experiment. The source S emits entangled photons ν_1 and ν_2 which the polarizing cubes I and II let through in either the $//$ or the $\perp$ direction. Subsequently the polarized photons are measured.*

The experimental result was $E(a,b) + E(a,b') + E(a',b) - E(a',b') = 2.70 \pm 0.05$, a 14σ violation of the CHSH inequality [1]. The conclusion seems unavoidable: quantum mechanics is not local realistic.

It now seems we can give up either locality as defined by definition 2.3 or realism as defined by definition 2.2. Before we can decide what to throw away, we need to know a bit better what we are dealing with, in particular the term *realism* can mean several things. Four possible meanings can be distinguished [70]:

1. **Naive Realism**: a point of view within the philosophy of perception which advocates that all aspects of a perceptual experience have their origin in some corresponding identical feature of the perceived object. For example, if Bob sees Alice's blond hair, a naive realist will state that the perceived blondness resides in the hair and that it is passively revealed by Bob's perceptual experience. I.e. naive realism means that whenever an experiment on an object is performed, the outcome of that measurement is simply a passive revealing of some pre-existing intrinsic property of the object. A more physical example: measurement of the spin of an electron reveals the spin an electron already had prior to measurement.

   Naive realism is not an independent assumption of locality, however. In fact, the pre-existence of measurables is derived from locality plus a subset of QM predictions.[2] Therefore, if realism means naive realism, it can simply be discarded in the phrase *local realism*.

[1] At USEQIP, see appendix A, the author measured the non-locality of nature himself, be it with a 'mere' $5sigma$ violation.

[2] Furthermore, the CHSH inequality, an inequality giving numerical predictions on an EPR like experiment, can be derived without reference to 'instruction sets' and thus naive realism.

2. **Scientific Realism**: a point of view within the philosophy of science that well-established scientific theories provide a literally true description of the world. The statistical interpretation of QM (which will be described in next section) is an example of an opposite point of view: instrumentalism. This view point holds that scientific theories only provide nice calculating aids in predicting experiments, but can't say anything about the *real* world.

   In the derivation of the CHSH inequality, however, no reference is made to any scientific theory. It is equivally valid for scientific realism as for instrumentalism and so if realism means scientific realism, the term can also be discarded within the context of *local realism*.

3. **Perceptual Realism**: the idea that sense perceptions give direct access to and provide valid information over the real physical world. It justifies the reality of this paper in front of you because you can see it, of the chair below you because you feel it and of the coffee on your desk because you can taste it. Perceptual realism is one of the fundaments of empiricism, because for experiments to say anything useful about the world, you need to be able to trust your senses in reading of your measurement devices, et cetera. If realism means perceptual realism, it is out of place in the phrase *local realism* as well, because if we reject perceptual realism doing any experiments by itself is useless, as is any interpretation of measurement results.

4. **Metaphysical Realism**: the metaphysical position that there is an objective world 'out there', however it may look like. Here we can be short: if one doesn't endorse metaphysical realism there can be no CHSH inequality, no Clauser *et al* and hence, even this paper and text is all in your head!

Summarizing the four possible meanings of realism, we see that the term *realism* within the phrase *local realism* actually is superfluous and there is no choice between either dropping locality or realism. We are left with one and only one alternative:

Result 2.1. *Quantum mechanics is fundamentally non-local!*

2.5.3 Closing the loopholes

Two implausible though logically correct objections can be raised against Aspect's experiment in support of local models:

The locality loophole : the measurement is skewed because elements in the experimental setup can communicate. Before measurement, the polarimeters can in some way 'agree on the measurement outcome'. To close the locality loophole, the measurement process of A, denoted as s_a, has to be spacelike separated from the measurement process of B and vice versa. The measurement process includes the choice of measurement setting, actual detection and writing the result to memory. Figure 2.2 shows an illustration.

The detection loophole : the measurement is skewed because the detectors have a 'preference' for certain particles. Photon detectors are not very efficient (normal detection efficiency is around 70 %). Usually a fair sampling hypothesis is assumed, i.e. each photon has the same probability to be detected. But perhaps detectors prefer a certain property such that it seems the sample violates the CHSH inequality, yet if all the photons would have been detected no violation would occur. To close the detection loophole, a very high detection efficiency is required.

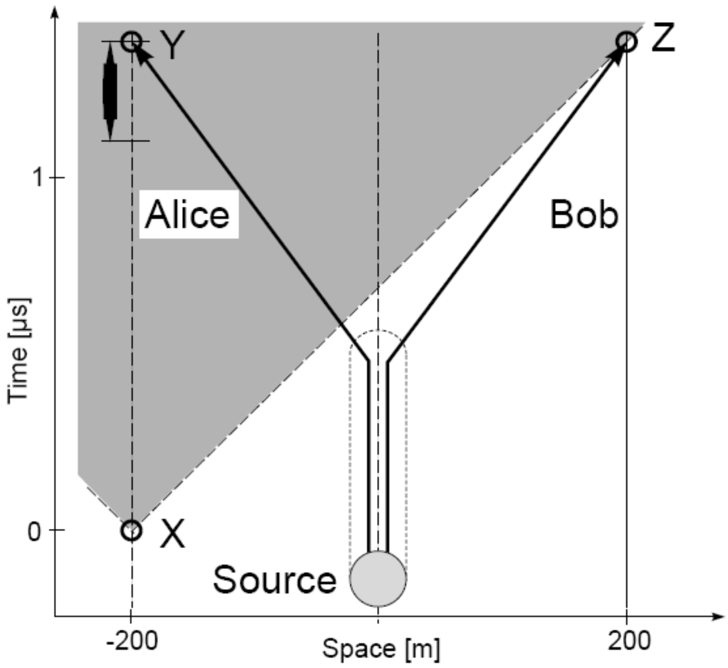


Figure 2.2: *[104] Spacetime diagram of a measurement required to close the locality loophole. Selecting the measurement settings, detecting the photon and writing it to disc is all part of the measurement process, depicted in the diagram as black bar. This process on Alice's side must lie inside the shaded region invisible to Bob during his own measurement. If we want to measure at spacetime points Y and Z, we must select the measurement settings after point X.*

The first locality loophole free experiment was performed in 1998 [104] and used entangled photons and fast random switches to have to spacelike separated measurements, see figure 2.3. In 2001, the first detection loophole free experiment test was published [82]. Heavy $^9Be^+$ ions were used to assure a very high detection efficiency. However, local models have been developed that require locality *and* detection loophole free experiments [63]. To date, despite several proposals, such experiments have not been done. The most probable configuration of such an experiment will use two EPR pairs, both pairs consist of a photon (which can travel very fast) and an ion (which can be perfectly detected). The photons travel a relatively large distance to a detector, where entanglement swapping (to be defined in section 5.2.5) is used to entangle the ions. The ions are subsequently measured.

2.6 Complete victory?

Bell's inequality provided a way to experimentally decide in the battle between completeness and locality, disfavouring the latter. But the victory of completeness in this battle doesn't imply completeness won the entire war: whether or not quantum mechanics is complete is subject of intensive debate till today. In the last part of this philosophical prelude, guided by Ref. [58], we will shortly touch upon one of the most prominent problems in the contemporary interpretation of quantum mechanics: the macro-objectivation problem.

Among others double split experiments clearly show interference of particles at micro level. If one wants to ascribe any form of reality to QM, undeniably the microscopic particle is in a

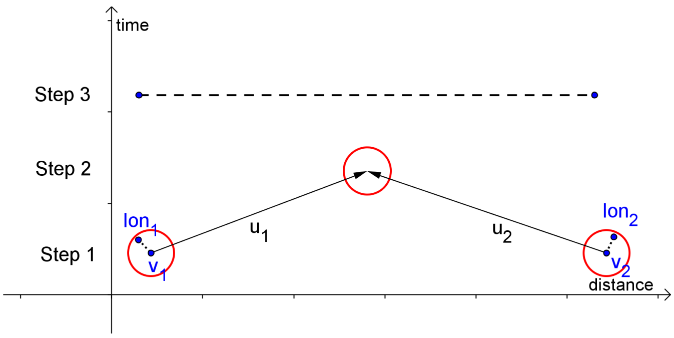


Figure 2.3: *[104] Spacetime diagram of a measurement required to close the locality loophole. Selecting the measurement settings, detecting the photon and writing it to disc is all part of the measurement process, depicted in the diagram as black bar. This process on Alice's side must lie inside the shaded region invisible to Bob during his own measurement. If we want to measure at spacetime points Y and Z, we must select the measurement settings after point X.*

superposition of going through both slits and thus is in a superposition of states. Contrary to micro level, at macro level superposition of states is never observed. But one can construct a situation in which the superposition at microlevel implies superposition at macrolevel. This contradiction between theoretically expected but never observed macro-entanglement is the macro-objectivation problem, the most famous example is without doubt Schrödinger's cat:

> *"A cat is penned up in a steel chamber along with the following diabolical device (which must be secured against direct interference by the cat): in a Geiger counter there is a tiny bit of radioactive substance so small that perhaps in the course of one hour one of the atoms decays but also, with equal probability, perhaps none; if it happens, the counter tube discharges and through a relay releases a hammer which shatters a small flask of hydrocyanic acid. If one has left this entire system to itself for an hour, one would say that the cat still lives if meanwhile no atom has decayed. The first atomic decay would have poisoned it."*
>
> [96]

Thus after one hour the combined state $|\psi\rangle$ of the cat and the radioactive substance can be written as the entangled superposition state:

$$|\psi\rangle = |\text{cat}\rangle|\text{substance}\rangle = \frac{1}{\sqrt{2}}\left(|\text{dead}\rangle|\text{decayed}\rangle + |\text{alive}\rangle|\text{full}\rangle\right) \tag{2.13}$$

Here, the microscopic superposition of states leads directly to superposition of macroscopic states. The superposition collapses if the cat is observed, but as long as the box remains closed QM gives the unsatisfying result that the cat has to be in a superposition of dead and alive. Many other paradoxal results like this can easily be constructed, but superposition of macroscopic systems is evidently untrue.

There are two principle options to choose: (i) QM is the complete truth about the universe, at microscopic and macroscopic level and (ii) QM is *not* the complete truth about the universe. If one chooses the first option, there are several ways out of the paradox sketched above which loosely can be put in three categories, differing in whether they ascribe 'reality' to the amplitudes of QM at micro- or at macro-level.

Statistical interpretation : QM is only a recipe that gives the outcome of experiments, any question as to the physical meaning of the amplitudes, both microscopic and macroscopic, is strictly meaningless. The only type of questions that can be meaningfully asked is about the probability of a certain outcome. This argument is logically consistent, but also a bit depressive: physics can't aim to give a description of the universe, it should just give some calculus rules that describe the results of measurements.

Orthodox ('decoherence') interpretation states that the QM amplitudes are real on microscopic scale (an electron in a slit experiment does not go through one particular slit), but not on macroscopic scale (the amplitudes give only the probability that the cat is either dead or alive). That at small and large scales the amplitudes can be interpreted differently is due to decoherence: for any realistic macroscopic systems the interaction with the environment cannot be neglected and this continued 'observation' collapses any interference patterns. But this interpretation contains a logical flaw: from a strictly formal point of view the QM formalism makes no distinction between macro- and micro systems, and thus QM cannot be interpreted fundamentally different at different scales.

Relative state ('many worlds') interpretation states that the amplitudes of QM at both micro- and macro level are real. Each measurement outcome is realized, but only in a different 'branch' of realities. Thus in Schrödingers cat experiment the cat is both dead and alive and remains so even when we open the box, 'in the particular branch of your reality' you observe the cat as either dead or alive, in the 'the other realities' the cat can be something else than what you observed. A major problem with this interpretation (besides its vagueness) is how to interpret probability amplitudes. Suppose the probability that the cat is alive is $\frac{1}{10}\pi$, what does this mean within the framework of reality branches?

The different interpretations of QM which assume QM is complete all have fallacies, so what if we assume QM is not complete? Many approaches have been suggested, it is beyond the scope of this thesis to give a complete overview. So instead, one prominent approach is considered: macrorealism. Although there are many variations on this approach which differ in the details, the basic idea is similar: a 'collapse-axiom' is added to QM. This axiom states that every once and a while (say, every 10^6 years) wave functions spontaneously collapse. In normal one-particle experiments, this kind of collapse will not occur because the time span during which the particle is in the experimental setup is extremely small compared to the collapse time, but in macroscopic systems (with more than 10^{20} particles), the probability of collapse of one of the particles is extremely high. And because almost all the particles within a macroscopic system are entangled, the collapse of one particle will result in the collapse of the entire system. A nice property of macrorealism is that it is experimentally falsifiable by experiment: if we observe quantum interference of macroscopically distinct states macrorealism has to be rejected. Several experiments have been proposed or performed such as molecular diffraction or the usage of flux in superconducting devices, but to date no definite answer has been found.

Result 2.2. *A contemporary problem with the interpretation of quantum mechanics is the theoretically predicted but never observed superposition of macroscopic states. The philosophical problem is named the macro-objectivation problem.*

CHAPTER 3

MATHEMATICAL AND PHYSICAL PRELIMINARIES

Quantum theory is a mathematical model of the physical world. Based on four axioms connecting mathematics and the physical world, quantum theory tries to give a framework in which to develop physical theories, but it doesn't give laws of physics themselves. Before we embark on our search for ways to create perfect quantum channels some basic results from quantum (information) theory are shortly reviewed. The purpose of this treatise is just to highlight those aspects which are of direct use within this thesis; as a review of quantum theory as a whole it is far from complete. Under the assumption the reader has some background in quantum mechanics, in each of the first four sections one of the axioms is reviewed and exemplified: (i) quantum spaces and states; (ii) quantum composite systems; (iii) quantum evolution; and (iv) quantum measurements. In these sections, quantum theory is developed in terms of state vectors, but an equivalent and sometimes more convenient way of dealing with it is in terms of density matrices. This is discussed in section (v). Finally section (vi) describes fidelity, a measure to quantify how different two states are. This review is largely based on [69], [55], [74] and [34]. The reader who is familiar with quantum theory and quantum information theory can skip both this and the following chapter and go directly to chapter 5.

3.1 Quantum spaces and states

Before we can state the first axiom, we have to define the mathematical space in which quantum mechanical systems live:

Definition 3.1 (Hilbert space $\mathcal{H}$.)**.** *A Hilbert space is a complex vector space with inner product $\langle u, v\rangle$ which is complete in the norm, i.e.*

$$\|u\| = \sqrt{\langle u, u\rangle}$$

(The completeness in the norm is especially important for infinite-dimensional systems, as it will ensure the convergence of certain eigenfunction expansions like Fourier analysis.)

Example 3.1 (Discrete Hilbert space)**.** *The complex vector space $\mathbb{C}^n$ with the inner product $\langle u, v\rangle$ of $u, v \in \mathbb{C}^n$ defined on it, endowed with the Euclidean norm, is a Hilbert space. If any other norm is used, it is not a Hilbert space because requirement that the norm is complete is not satisfied.*

Example 3.2 (Continuous Hilbert space). *Let* $1 p < \infty$ *and let* f, g *be measurable functions on measure space* X [1]*, then the* L^p *norm is defined as:*

$$\|L^p\| = \left(\int_X |f|^p\right)^{1/p}$$

For $p = 2$ *the inner product of* f *and* g *is defined as:*

$$\langle f, g\rangle = \int_X f(x)g(x)dx$$

and therefore L^2 *is a Hilbert space. Any* L^p *with* $p \neq 2$ *doesn't give a Hilbert space*

Now we have defined Hilbert spaces, the stage on which the play of quantum mechanics unfolds, we can give the first axiom of quantum theory:

Axiom 3.1. *Any isolated physical system lives in a Hilbert space* $\mathcal{H}$*, which is the state space of the system. The system can be completely described by its state vector, a unit vector in the system's space. Notational remark: a state vector is usually denoted with* $|\psi\rangle$*.*

One of the simplest physical systems, and for this thesis also the most important one, is a *qubit*: a system which can be in (the superposition of) two states: $|0\rangle$ and $|1\rangle$. In general, a qubit can be written as:

$$|\psi\rangle = a_1|0\rangle + a_2|1\rangle \tag{3.1}$$

with $\sum_i a_i^2 = 1$. Here, the states $\{|0\rangle, |1\rangle\}$ can be seen as basis vectors and $\{a_1, a_2\}$ as their corresponding amplitudes. The normalization condition $\sum_i a_i^2 = 1$ is important for quantum measurement, as we will see later. A complex amplitude can be written as $e^{i\alpha}|\alpha|$ and thus we can write the qubit state also as:

$$\begin{aligned} |\psi\rangle &= e^{i\phi}\cos(\tfrac{1}{2}\theta)|0\rangle + e^{i\varphi}\sin(\tfrac{1}{2}\theta)|1\rangle \\ &= e^{i(\phi-\varphi)}\left(\cos(\tfrac{1}{2}\theta)|0\rangle + e^{i\varphi}\sin(\tfrac{1}{2}\theta)|1\rangle\right) \end{aligned}$$

Because of the way quantum measurements work, global phase factors don't have a physical meaning, only the relative phase factor between the states is important. Technically, this means we could describe quantum states by equivalence classes, but in practical notation the equivalence classes are just implicitely understood. Thus for our qubit we can simply write:

$$|\psi\rangle = \cos(\tfrac{1}{2}\theta)|0\rangle + e^{i\varphi}\sin(\tfrac{1}{2}\theta)|1\rangle \tag{3.2}$$

The qubit state vector is often depicted as a point on a two-dimensional surface in three-dimensional space named the Bloch sphere, see figure 3.1 below.

A physical example of a qubit is the spin-orientation of an electron, which in general is in a superposition of spin-up and spin-down. Let $|0\rangle$ and $|1\rangle$ represent the orthogonal basis vectors for spin-up and spin-down respectively, than we can write for a general spin-state of an electron: $|\phi\rangle = a_1|0\rangle + a_2|1\rangle$.

The notion of a qubit can be slightly generalized to a qudit: a system which can be in (the superposition of) m states:

$$|\psi\rangle = a_1|0\rangle + a_2|1\rangle + ... + a_m|m-1\rangle \tag{3.3}$$

with $\sum_i a_i^2 = 1$.

[1] Loosely, a measure space is a space on which a measure can be defined and a measurable function is a structure-preserving function between two measurable spaces.

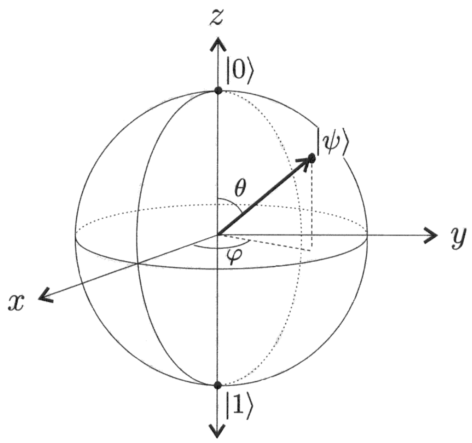


Figure 3.1: *[55] Schematic representation of quantum bit on two-dimensional surface, the Bloch sphere.*

3.2 Quantum composite systems

Suppose now we have not one, but several quantum systems. Axiom 2 describes how we build up the state space of a composite system from its components:

Axiom 3.2 (Axiom 2: composite systems.)**.** *The state space of a composite system is the tensor product of the state spaces of the individual physical systems.*

Suppose that we have two qudits of dimensions m and n respectively, with Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. The combined Hilbert space $\mathcal{H}$ of both qudits has dimensions $m \times n$ and is given by the tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Every element $|u\rangle \in \mathcal{H}$ can be written as a linear combination of tensor products $|v\rangle \otimes |w\rangle$, with $|v\rangle \in \mathcal{H}_1$ and $|w\rangle \in \mathcal{H}_2$. Often, $|v\rangle \otimes |w\rangle$ is shortly written as $|v\rangle|w\rangle$ or as $|vw\rangle$. In concrete situations, the tensor state of two systems in their combined space can be computed with the Kronecker product.

Definition 3.2 (Kronecker product)**.** *Let A be a $m \times n$ matrix and B a $p \times q$ matrix, then the Kronecker product of these matrices is given by*

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n} \\ A_{21}B & A_{22}B & \cdots & A_{2n} \\ \vdots & & & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{pmatrix} \tag{3.4}$$

Example 3.3. *Suppose we have the two matrices A and B given by:*

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 5 \\ 10 \end{pmatrix}$$

The Kronecker product of both is:

$$A \otimes B = \begin{pmatrix} 1 \cdot 5 & 2 \cdot 5 \\ 1 \cdot 10 & 2 \cdot 10 \\ 3 \cdot 5 & 4 \cdot 5 \\ 3 \cdot 10 & 4 \cdot 10 \end{pmatrix} = \begin{pmatrix} 5 & 10 \\ 10 & 20 \\ 15 & 20 \\ 30 & 40 \end{pmatrix}$$

Example 3.4. *Let $|v\rangle = a_1|0\rangle + a_2|1\rangle$ and $|w\rangle = b_1|0\rangle + b_2|1\rangle$ be two qubit states. In the basis $\{|0\rangle, |1\rangle\}$ we can write these states as $|v\rangle = \left(\begin{pmatrix} a_1 & a_2 \end{pmatrix}\right)^T$ and $|w\rangle = \left(\begin{pmatrix} b_1 & b_2 \end{pmatrix}\right)^T$. Using the basis $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ we can write their product state as $|v\rangle \otimes |w\rangle = \left(\begin{pmatrix} a_1b_1 & a_2b_1 & a_1b_2 & a_2b_2 \end{pmatrix}\right)^T$*
.

3.3 Quantum evolution

Now we know how to define quantum states, it is natural to consider how they evolve in time. But before we can state the axiom involving time evolution, we again need a definition:

Definition 3.3 (Adjoint, Hermitian and normal operators.)**.** *Let V be a Hilbert space with vectors $|v\rangle$ and $|w\rangle$, than for every linear operator U there is an operator $U^\dagger$ called the adjoint or Hermitian conjugate such that*

$$\langle\langle v|, U|w\rangle\rangle = \left\langle U^\dagger \langle v|, |w\rangle \right\rangle$$

For finite dimensional operators in matrix representation, the Hermitian conjugate is given by the complex conjugate transpose of the operator, i.e. $U^\dagger = U^{T*}$. If $U^\dagger = U$, the operator is called self adjoint or Hermitian and if $UU^\dagger = U^\dagger U$ the operator is called a normal operator. Note that an Hermitian operator is always a normal operator, but the converse is not true.

Example 3.5. *Let the operator U_{ex} be defined by the matrix*

$$U_{ex} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$

Since $U_{ex}^\dagger = U_{ex}$ the operator is Hermitian and normal.

Now we can state the time evolution axiom of quantum mechanics

Axiom 3.3 (Axiom 3: quantum evolution)**.** *The time evolution of a state of a closed quantum system is given by the Schrödinger equation:*

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

with $\hbar$ Planck's constant, a physical constant determined by experiment, and H an Hermitian matrix named the Hamiltonian.

How exactly the Hamiltonian looks like is an important part of physics research and much of 20^{th} century physics was about finding good Hamiltonians, because when the Hamiltonian is known the dynamics of the system can be understood completely. From a strict quantum mechanics point of view, however, finding a good Hamiltonian is just a detail of a specific system with specific physical laws. For the purpose of this thesis we also don't really need to find Hamiltonians, and we can rephrase axiom 3 in a slightly more relevant formulation, which can be seen as the axiom's discrete variant. To do so, we need the following definition and theorem:

Definition 3.4 (Unitary operator)**.** *An operator U is called unitary if $U^\dagger U = 1$ and $UU^\dagger = 1$, with $U^\dagger$ the adjoint.*

Example 3.6. *Consider again the operator U_{ex} from example 3.5. Direct computation shows that:*

$$U_{ex}U_{ex}^\dagger = U_{ex}^\dagger U_{ex} = \tfrac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$$

so we have that U_{ex} is a unitary operator.

All important operators are Hermitian or unitary and thus normal operators. For normal operators we can define the following important theorem:

Theorem 3.1 (Spectral Decomposition)**.** *Any normal operator M on a vector space V (for example an Hilbert space) is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal.*

A proof of this theorem can be found in [69], pg. 72. Now we can write the discrete version of axiom 3:

Theorem 3.2 (Discrete version of axiom 3.)**.** *The time evolution of a closed quantum system is described by a unitary transformation U. I.e., the state $|\psi(t_0)\rangle$ of the system at time t_0 and the state $|\psi(t_1)\rangle$ at time t_1 is related by the unitary operator $U(t_0, t_1)$ as $|\psi(t_1)\rangle = U(t_0, t_1)|\psi(t_0)\rangle$.*

Proof. For an arbitrary unitary operator U there is an Hermitian operator H and vice versa such that (this claim will be shown below):

$$U(t_0, t_1) = \exp\left[\frac{-iH(t_1 - t_0)}{\hbar}\right]$$

Let according to the theorem

$$|\psi(t_1)\rangle = U(t_0, t_1)|\psi(t_0)\rangle$$

Than for $t_1 = t_0 + dt$ and $dt \to 0$, the Schrödinger equation is satisfied. To show that H is indeed Hermitian, first use that U relates to H as $H = -i\log(U)$. Since U is unitary it is a normal operator and therefore by the spectral theorem U is diagonalize. The logarithm of a diagonalizable matrix can be written as $\log(U) = X\log(D)X^{-1}$, with D the diagonal matrix consisting of the eigenvalues of U, $\log(D)$ the matrix where all eigenvalues λ_i have been replaced by $\log(\lambda_i)$ and X the matrix with on the j^{th} column the eigenvector corresponding to the eigenvalue of the j^{th} column of D. Thus we have $H = -iX\log(D)X^{-1}$. Using that $\left(X^{-1}\right)^\dagger = \left(X^\dagger\right)^{-1}$ and that $U^\dagger = U^{-1}$ we obtain:

$$\begin{aligned} H^\dagger &= \left(-i\hbar X\log(D)X^{-1}\right)^\dagger = i\hbar\left(X^{-1}\right)^\dagger \left(X^\dagger\right)^{-1}\log(D^\dagger)X^\dagger \\ &= i\hbar\left(X^\dagger\right)^{-1}\left[X^\dagger X\log(D^{-1})X^{-1}\left(X^\dagger\right)^{-1}\right]X^\dagger \\ &= -iX\log(D)X^{-1} = H \end{aligned}$$

I.e., H is Hermitian. Conversely, if some Hermitian H satisfies the Schrödinger equation, than by writing out the matrix exponentials in $UU^\dagger$ and $U^\dagger U$ explicitely it follows directly that U is unitary. □

With the theorems above in mind, we can state a theorem that will be used throughout this thesis:

Theorem 3.3 (Schmidt decomposition). *For every bipartite pure state $|\psi\rangle_{ab}$ of the composite system $ab \in \mathcal{H}_a \otimes \mathcal{H}_b$ there is an orthonormal basis $|i\rangle_a$ for system A and an orthonormal basis $|i\rangle_b$ for system B such that*

$$|\psi\rangle = \sum_i \lambda_{ii} |i\rangle_a |i\rangle_b \tag{3.5}$$

with λ_{ii} the Schmidt coefficients, non-negative real numbers satisfying $\sum_i \lambda_{ii}^2 = 1$. The number of non-zero Schmidt coefficients is called the Schmidt number.

Proof. Let $|j\rangle$ be an orthonormal basis for system A of dimension m and $|k\rangle$ an orthonormal basis for system B of dimension $n < m$. Then the arbitrary vector $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{jk} z_{jk} |j\rangle |k\rangle \tag{3.6}$$

with z_{jk} a $m \times n$ matrix of complex numbers. Singular value decomposition allows us to write $z = v\lambda w$, with v an $m \times n$ unitary matrix, w a $n \times n$ unitary matrix and λ a $n \times n$ diagonal matrix. Plugging this in equation 3.6 gives:

$$|\psi\rangle = \sum_{ijk} v_{ji} \lambda_{ii} w_{ik} |j\rangle |k\rangle \tag{3.7}$$

Define $|i_a\rangle = \sum_j v_{ji} |j\rangle$ and $|i_b\rangle = \sum_k w_{ik} |k\rangle$. These states are well defined because v_{ji} and w_{ik} are unitary matrices and thus are an allowed transition from the old to the new state. Substituting these states in the previous equation we obtain:

$$|\psi\rangle = \sum_i \lambda_{ii} |i_a\rangle |i_b\rangle \tag{3.8}$$

□

What does this theorem tell us? Normally an arbitrary state $|\psi\rangle$ in $\mathcal{H}_a \otimes \mathcal{H}_b$ is written as in equation 3.6, where we need two indices for both the subspaces. The Schmidt decomposition states that for a pure bipartite state we actually only need one index and $\min(m, n)$ terms because 'the cross-terms have vanished'. Here, the entries on the diagonal matrix λ_{ii} are the square roots of the probability of outcome ii: $\sqrt{p_{ii}}$.

Example 3.7. *Consider the state*

$$|\psi_{ex}\rangle = \tfrac{1}{2} \left(|00\rangle + |11\rangle - |01\rangle - |10\rangle \right)$$

The density matrix z of this state is

$$z = \tfrac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

which has singular value decomposition $z = v\lambda w$, with v, w and λ defined as:

$$v = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \qquad \lambda = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad w = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

Thus we can write

$$|0_a\rangle = \sum_j v_{j1}|j\rangle = \frac{1}{\sqrt{2}}\left(-|0\rangle + |1\rangle\right)$$
$$|1_a\rangle = \sum_j v_{j2}|j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$|0_b\rangle = \sum_k w_{1k}|k\rangle = \frac{1}{\sqrt{2}}\left(-|0\rangle + |1\rangle\right)$$
$$|1_b\rangle = \sum_k w_{2k}|k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

and the Schmidt decomposition is:

$$|\psi_{ex}\rangle = \sum_i \lambda_{ii}|i_a\rangle|i_b\rangle = 1 \cdot |0_a\rangle|0_b\rangle + 0 \cdot |1_a\rangle|1_b\rangle$$

One eigenvalue is non-zero, thus the Schmidt number is 1.

The Schmidt decomposition has a number of useful consequences, one of which is the following lemma.

Lemma 3.4. *The Schmidt number cannot increase under LOCC operations.*

Proof. Consider an arbitrary pure bipartite state $|\psi\rangle = \sum_{jk} z_{jk}|j\rangle|k\rangle$, with z_{jk} an $m \times n$ matrix. By singular value decomposition we can write $z_{ij} = v\lambda w$ with v, w and λ also unitary matrices. From this follows the Schmidt decomposition $|\psi\rangle = \sum_i \lambda_{ii}|i_a\rangle|i_b\rangle$ with $|i_a\rangle = \sum_j v_{ji}|j\rangle$ and $|i_b\rangle = \sum_k w_{ik}|k\rangle$. If we apply the unitary transformation U_a, which only influences Alice's qubit, we get

$$U_a|\psi\rangle = U_a \sum_i \lambda_{ii}|i_a\rangle|i_b\rangle = \sum_i \lambda_{ii}(U|i_a\rangle)|i_b\rangle = \sum_i \lambda_{ii}|i'_a\rangle|i_b\rangle \tag{3.9}$$

with $|i'_a\rangle = \sum_l u_{lj}v_{ji}|l\rangle$. Analogous reasoning can be applied to unitary transformations on Bob's part. If Alice's and Bob's particle are spatially separated, every LOCC operation can be seen as a combination of separate operations on Alice's and Bob's part. Thus, from the equation above we see that for LOCC operations the matrix λ and thus the Schmidt number remain the same. □

3.4 Quantum measurement

As scientists we usually measure systems with a measurement device. Interaction of the system with the measurement device makes that the system is not longer closed and therefore unitary evolution is insufficient to describe the system completely. The fourth axiom states how quantum systems behave under measurements:

Axiom 3.4 (Axiom 4: quantum measurement)**.** *Quantum measurements are described by a collection of measurement operators M_q, where q indexes the possible outcomes. Let $|\psi\rangle$ be the quantum state before measurement, than the measurement operators have the following properties:*

- *The probability of outcome q is given by $p(q) = \langle\psi|M_q^\dagger M_q|\psi\rangle$.*
- *The state of the system after measurement is given by $\frac{M_q|\psi\rangle}{\sqrt{p(q)}}$.*
- *The measurement operators M_q satisfy the completeness equation $\sum_q M_q^\dagger M_q = I$.*

There are several types of measurement operators. The classical work on quantum measurement was written by Von Neumann in 1932. He considered quantum observables with classical counterparts like positions, energies and momenta. Their various possible measurement outcomes are mutually exclusive and sum up to one, which motivated the following definition:

Definition 3.5 (Projective measurements)**.** *Let $\mathcal{O}$ be an observable with eigenvalues q and spectral decomposition*

$$\mathcal{O} = \sum_q qP_q \tag{3.10}$$

with P_q the projector onto the eigenspace of $\mathcal{O}$ with eigenvalue q. The set of projection operators P_q satisfy all the properties of measurement operators and are orthogonal to each other.

Example 3.8 (Computational basis)**.** *A nice example of a measurement is a measurement of one qubit in the computational basis defined as $\{|0\rangle, |1\rangle\}$. The corresponding measurement operators are $M_0 = |0\rangle\langle 0| = \left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$ and $M_1 = |1\rangle\langle 1| = \left(\begin{smallmatrix}0 & 0\\ 0 & 1\end{smallmatrix}\right)$.*

Example 3.9 (Bell basis measurement)**.** *A slightly more elaborate example is a measurement of an entangled[2] pair in the Bell basis, which has the elements:*

$$\begin{aligned} |\phi^+\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) & |\phi^-\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\ |\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) & |\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \end{aligned} \tag{3.11}$$

The corresponding measurement operators are

$$\begin{aligned} M_{\phi^+} &= |\phi^+\rangle\langle^+\phi| & M_{\phi^-} &= |\phi^-\rangle\langle^-\phi| \\ M_{\Psi^+} &= |\Psi^+\rangle\langle^+\Psi| & M_{\Psi^-} &= |\Psi^-\rangle\langle^-\Psi| \end{aligned}$$

Von Neumann's approach to quantum measurement, however, turned out to be too narrow. Although quantum observables with a classical counterpart can be measured adequately with orthogonal operators, this is not true for all quantum observables: macroscopically different situations can be produced by states which are not orthogonal. For example, suppose we prepare the spin state of a spin-$\frac{1}{2}$ particle by selecting the upper beam in a Stern-Gerlach device. We can choose the orientation of the magnet in the directions $\mathbf{n}_1$ and $\mathbf{n}_2$. The resulting beams have quantum states $|\psi\rangle_1$ and $|\psi\rangle_2$ given by $\mathbf{n}_j \cdot \sigma|\psi\rangle_j = |\psi\rangle_j$ and their overlap is:

$$\| \langle\psi_1, \psi_2\rangle \| = \tfrac{1}{2}(1 + \mathbf{n}_1 \cdot \mathbf{n}_2)$$

[2]This term will be defined in chapter 4.

which in general is not equal to zero. Consequently, the question "Was state $|\psi\rangle_1$ prepared?" cannot be answered with certainty, as there is a possibility that this question is answered with "yes" even when the particle was prepared in state $|\psi\rangle_2$. As Peres [73] puts it: "Once the spin-$\frac{1}{2}$ particle has been severed from the macroscopic apparatus which prepared it, it does not carry the full information relative to the preparation procedure. Some questions become ambiguous, and only probabilities can be assigned to their answers. This situation is radically different from the one prevailing in classical physics. Therefore quantum tests cannot be restricted to mere imitations of classical measurements ... and more general procedures must be considered." This leads to the following definition:

Definition 3.6 (Generalized measurements)**.** *A generalized quantum measurement is a projective quantum measurement where the orthogonality condition of the operators is skipped.*

Sometimes we are mainly concerned with the probabilities of the possible measurement outcomes and not so much with the actual post-measurement state, for example in a measurement setup in which the measurement is performed only once (an often encountered situation in quantum information). In these situations, *Positive Operator Valued Measurements* (POVM) are very useful[3] because they allow easy mathematical treatment.

Definition 3.7 (POVM)**.** *Suppose we have a quantum system $|\psi\rangle$ on which we perform a measurement with operators M_q. Define $E_q \equiv M_q^\dagger M_q$, then $\sum_q E_q = I$ and $p(q) = \langle\psi|E_q|\psi\rangle$. The set E_q is a POVM.*

Example 3.10. *Suppose Alice gives Bob with equal probability one of the states below and he has to guess which state he received.*

$$|\psi_1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad\qquad |\psi_2\rangle = |1\rangle$$

Bob can perform a POVM that sometimes is inconclusive, but when it gives a result it will always be the correct result. The POVM is given by:

$$\begin{aligned} E_1 &\equiv \frac{\sqrt{2}}{1+\sqrt{2}}\tfrac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) \\ E_2 &\equiv \frac{\sqrt{2}}{1+\sqrt{2}}|0\rangle\langle 0| \\ E_3 &\equiv I - E_1 - E_2 \end{aligned}$$

Because $\langle\psi_1|E_1|\psi_1\rangle = 0$, if Bob gets a non-zero result for E_1 he knows he received $|\psi_2\rangle$. Analogously, because $\langle\psi_2|E_2|\psi_2\rangle = 0$, a non-zero result for E_2 implies $|\psi_1\rangle$. Only when Bob gets E_3, the measurement is inconclusive because he could have had both states. The probability p_{E_3} of an inconclusive result is:

$$p_{E_3} = p_{\psi_1} \cdot \langle\psi_1|E_3|\psi_1\rangle + p_{\psi_2} \cdot \langle\psi_2|E_3|\psi_2\rangle = \tfrac{1}{1+\sqrt{2}}$$

Note that the measurement operators are not orthonogal, so this example also shows concretely that the restriction to orthogonal measurements considered by Von Neumann is too narrow.

[3] A positive operator A is an operator for which $\langle w, Aw\rangle \geq 0 \forall w$.

Note that a generalized measurement and a POVM are equivalent in the sense that for every set of measurement operators M_q one can define a POVM as $\forall q : E_q = M_q^\dagger M_q$ and for each POVM one can define a set of measurement operators as $\forall q : M_q = \sqrt{E_q}$. Neumark [73] showed that for every desired POVM there is an experimentally realizable procedure that generates it.

A fundamental difference between quantum mechanics and classical mechanics is the accuracy to which an operator can be measured. In classical mechanics, the accuracy depends only on the measurement: more precise measurements give a lower uncertainty and in theory the uncertainty can be arbitrarily small. In quantum mechanics this situation is radically different because of the Uncertainty Relations, first discovered by Heisenberg and mathematically shown by Kennard [56]. Below we will derive the Uncertainty Relations. Before we can do so we will formally define the *commutator* of two operators, a mathematical operation which we already encountered in the philosophical prelude.

Definition 3.8 (Commutator and anti-commutator)**.** *Let $\hat{A}$ and $\hat{B}$ be two operators, then their commutator $[\hat{A}, \hat{B}]$ and anti-commutator are defined as:*

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$$
$$\{\hat{A}, \hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$$

The operators $\hat{A}$ and $\hat{B}$ are called commuting operators if $[\hat{A}, \hat{B}] = 0$. Otherwise, they are non-commuting operators.

Example 3.11. *The standard example of two non-commuting operators are the position and momentum operators. Let $\hat{x} = x$ and $\hat{p} = -i\hbar\partial/\partial x$ be the position and momentum operator respectively and $f(x)$ an arbitrary function of x, than*

$$[\hat{x}, \hat{p}]f(x) = -i\hbar\left(x\tfrac{\partial}{\partial x} - \tfrac{\partial}{\partial x}x\right)f(x) = i\hbar\left(-x\tfrac{\partial f(x)}{\partial x} + x\tfrac{\partial f(x)}{\partial x} + f(x)\right) = i\hbar f(x)$$

Now we can define the Uncertainty Relations, from which follows that two non-commuting operators cannot be known simultaneously with arbitrary low uncertainty.

Theorem 3.5 (Generalized Heisenberg Uncertainty Relations)**.** *Let C and D be two observables with standard deviation $\Delta(C)$ and $\Delta(D)$, then the generalized Heisenberg Uncertainty Relations are given by:*

$$\Delta(C)\Delta(D) \geq \tfrac{1}{2}|\langle\psi|[C, D]|\psi\rangle|$$

This relation should be interpreted as follows: if a large number of identical states $\langle\psi|$ are prepared and undergo identical measurement procedures for observable C in some and observable D in others, then, $\Delta(C)\Delta(D)$ will satisfy the inequality above. It is important to note that the uncertainty is an intrinsic property of nature and not in any way related to measurement uncertainty or perturbations of the system due to measurements.

Proof. Let $\hat{A}$ and $\hat{B}$ be two Hermitian operators and suppose that $\langle\psi|\hat{A}\hat{B}|\psi\rangle = x + iy$, than $\langle\psi|[\hat{A}\hat{B}]|\psi\rangle = 2iy$ and $\langle\psi|\{\hat{A}\hat{B}\}|\psi\rangle = 2x$. This allows us to write

$$\langle\psi|\{\hat{A}\hat{B}\}|\psi\rangle + \langle\psi|[\hat{A}\hat{B}]|\psi\rangle = 4(x^2 + y^2) = 4\langle\psi|\hat{A}\hat{B}|\psi\rangle^2 \leq 4\langle\psi|\hat{A}^2|\psi\rangle\langle\psi|\hat{B}^2|\psi\rangle \quad (3.12)$$

where in the inequality we used Cauchy-Schwarz. If we substitute $\hat{A} = C - \langle C\rangle$ and $\hat{B} = D - \langle D\rangle$ we obtain:

$$\tfrac{1}{2}|\langle\psi|[C, D]|\psi\rangle| = \tfrac{1}{2}|\langle\psi|[\hat{A}\hat{B}]|\psi\rangle| \leq \sqrt{\langle\psi|\hat{A}^2|\psi\rangle\langle\psi|\hat{B}^2|\psi\rangle} = \Delta(C)\Delta(D) \quad (3.13)$$

□

Example 3.12. *The best known Heisenberg Uncertainty Relation is probably the uncertainty relation between the position operator $\hat{x}$ and momentum operator $\hat{p}$. Direct computation gives:*

$$\Delta\hat{x}\Delta\hat{p} \geq \tfrac{1}{2}\hbar$$

3.5 Density operators

Quantum mechanics can be formulated in terms of state vectors $|\psi\rangle$ as above, but a mathematical equivalent and sometimes more practical formulation is possible in terms of density operators or density matrices ρ.

Definition 3.9 (Density operator)**.** *Let a quantum state be in one of the ensemble of states $|\psi_i\rangle$ with probability p_i, with $i \in \{1, ..., n\}$ for some n. Then the density operator for the system is given by:*

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{3.14}$$

The density operator completely specifies all the properties of the quantum ensemble. In case the quantum state is exactly known, the density operator is said to be in a *pure state*, in this case we simply have $\rho = |\psi\rangle\langle\psi|$. If the system can be in several quantum states with a certain probability, the density operator is in a *mixed state*.

Example 3.13. *Consider a qubit which is in the mixed state*

$$|\psi_1\rangle = \sqrt{\tfrac{1}{2}}\,(|0\rangle + i|1\rangle) \qquad \textit{with probability} \qquad p_1 = \tfrac{3}{4}$$
$$|\psi_2\rangle = \sqrt{\tfrac{1}{2}}\,(|0\rangle - i|1\rangle) \qquad \textit{with probability} \qquad p_2 = \tfrac{1}{4}$$

In the basis $\{|0\rangle, |1\rangle\}$, the density operator of the qubit is given by:

$$\rho = \tfrac{3}{8}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} + \tfrac{1}{8}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} = \tfrac{1}{4}\begin{pmatrix} 2 & i \\ -i & 2 \end{pmatrix}$$

Not all operators are density operators. The following theorem states which properties an operator ρ has to satisfy to be a density operator [69]:

Theorem 3.6 (Characterisation of density operators)**.** *A matrix ρ is the density operator of some ensemble $\{p_i, |\psi_i\rangle\}$ if and only if ρ satisfies the conditions:*

Trace condition *: ρ has trace equal to one.*

Positivity condition *: ρ is a positive operator.*

Proof. First, we prove that a density operator $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ satisfies the conditions mentioned above. Note that for a state $|\psi\rangle = \sum_j a_j|j\rangle$ we have that $\sum_j a_j^2 = 1$. Consequently, $\mathrm{tr}(|\psi\rangle\langle\psi|) = \sum_j a_j^2 = 1$. Then

$$\mathrm{tr}(\rho) = \sum_i p_i \,\mathrm{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1 \tag{3.15}$$

Suppose $|\phi\rangle$ is an arbitrary vector in state space, then:

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i \,\mathrm{tr}(\langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle) = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0 \tag{3.16}$$

Conversely, assume ρ is any operator satisfying the trace and positivity conditions above. Because ρ is positive, it is Hermitian and thus normal. Consequently, we can make a spectral decomposition of ρ, given by

$$\rho = \sum_k \lambda_k |k\rangle\langle k| \tag{3.17}$$

with $|k\rangle$ orthogonal vectors and λ_k real non-negative eigenvalues of ρ. The trace condition gives that $\sum_k \lambda_k = 1$, thus a system in state $|k\rangle$ with probability $p_k = \lambda_k$ gives rise to the density operator ρ. □

It should be noted that there are a lot of ensembles of quantum states that have the same density operator.

Example 3.14. *Consider a quantum system with the following density operator:*

$$\rho = \tfrac{3}{4}|0\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1|$$

This density operator might be prepared by the following ensemble:

$$|\psi_1\rangle = |0\rangle \qquad \textit{with probability} \qquad p_1 = \tfrac{3}{4}$$
$$|\psi_2\rangle = |1\rangle \qquad \textit{with probability} \qquad p_2 = \tfrac{1}{4}$$

But also by the ensemble:

$$|\psi_1\rangle = \sqrt{\tfrac{3}{4}}|0\rangle + \sqrt{\tfrac{1}{4}}|1\rangle \qquad \textit{with probability} \qquad p_1 = \tfrac{1}{2}$$
$$|\psi_2\rangle = \sqrt{\tfrac{3}{4}}|0\rangle - \sqrt{\tfrac{1}{4}}|1\rangle \qquad \textit{with probability} \qquad p_1 = \tfrac{1}{2}$$

To see that quantum mechanics can be stated in density operators just as well as in state vectors, we briefly reformulate the axioms of quantum mechanics above in terms of density operators:

Axiom 1: the state space . Any isolated physical system lives in a Hilbert space $\mathcal{H}$, which is the state space of the system. The system can be completely described by its density operator, operators characterized by theorem 3.6, acting on the state space of the system. If a quantum system is in a state described by ρ_i with probability p_i, the density operator for the system is given by $\sum_i p_i \rho_i$.

Axiom 2: composite systems . The state space of a composite system is the tensor product of the state spaces of the individual physical systems.

Axiom 3: quantum evolution (discrete version) . The time evolution of a closed quantum system is described by a unitary transformation U. I.e., the state $\rho(t_0)$ of the system at time t_0 and the state $\rho(t_1)$ at time t_1 is related by the unitary operator $U(t_0, t_1)$ as $\rho(t_1) = U(t_0, t_1)\rho(t_0)U(t_0, t_1)^\dagger$.

Axiom 4: quantum measurement . Quantum measurements are described by a collection of measurement operators M_q, where q indexes the possible outcomes. Let ρ be the density matrix before measurement, than the measurement operators have the following properties:

- The probability on outcome q is given by $p(q) = \mathrm{tr}(M_q^\dagger M_q \rho)$.

- The state of the system after measurement is given by $\frac{M_q \rho M_q^\dagger}{\sqrt{p(q)}}$.
- The measurement operators M_q satisfy the completeness equation $\sum_q M_q^\dagger M_q = I$.

In case of a system of multiple particles, density matrices give a description of the state of the entire system. But often we are only interested in the state of a subsystem of one or a few particles. To investigate a subsystem if the density operator of the entire system is known, we can use the reduced density operator.

Definition 3.10 (Reduced density operator)**.** *Consider a system with two subsystems a and b. The state of the entire system is given by $\rho^{ab} \in \mathcal{H}^{a\otimes b}$. The reduced density operator $\rho^a \in \mathcal{H}_a$ for system a is given by:*

$$\rho^a = \mathrm{tr}_b(\rho^{ab}) \tag{3.18}$$

with tr_b the partial trace, defined as:

Definition 3.11 (Partial trace)**.** *Consider a system with two subsystems a and b. The partial trace $\mathrm{tr}_b : \rho^{ab} \to \rho^a$ is given by:*

$$\mathrm{tr}_b(\rho^{ab}) \equiv \mathrm{tr}(\rho^b)\rho^a \tag{3.19}$$

By extension, for a system with n subsystems the partial trace is given by:

$$\mathrm{tr}_{a_i}(\rho^{a_1 \ldots a_n}) \equiv \mathrm{tr}(\rho_i^a)\rho^{a_1} \otimes \ldots \rho^{a_{i-1}} \otimes \rho^{a_{i+1}} \otimes \ldots \otimes \rho^{a_n} \tag{3.20}$$

In case of a qubit, let $|a_1\rangle$ and $|a_2\rangle$ be two vectors in the state space of a and $|b_1\rangle$ and $|b_2\rangle$ be two vectors in the state space of b. Then the equation above simplifies to:

$$\begin{aligned} \mathrm{tr}_b(\rho^{ab}) &= \mathrm{tr}_b(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \\ &\equiv |a_1\rangle\langle a_2|\,\mathrm{tr}_b(|b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2|\langle b_1|b_2\rangle \end{aligned} \tag{3.21}$$

Example 3.15. *Consider the system $|\psi\rangle_{ab} = (\frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2}|11\rangle)_{ab}$. What is the density operator of Bob's system?*

To find the density operator of Bob's system, Alice's qubit needs to be traced out. The density operator corresponding to the system above is:

$$\rho_{ab} = |\psi\rangle\langle\psi|_{ab} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & \sqrt{3} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \sqrt{3} & 0 & 0 & 3 \end{pmatrix}$$

Tracing out Alice's qubit gives:

$$\begin{aligned} \rho_b &= \tfrac{1}{4}|0\rangle\langle 0|_b(1\cdot\langle 0|0\rangle + 0\cdot\langle 1|1\rangle)_a + \tfrac{1}{4}|0\rangle\langle 1|_b(0\cdot\langle 0|0\rangle + 0\cdot\langle 1|1\rangle)_a \\ &+ \tfrac{1}{4}|1\rangle\langle 0|_b(0\cdot\langle 0|0\rangle + 0\cdot\langle 1|1\rangle)_a + \tfrac{1}{4}|1\rangle\langle 1|_b(0\cdot\langle 0|0\rangle + 3\cdot\langle 1|1\rangle)_a \\ &= \tfrac{1}{4}|0\rangle\langle 0|_b + \tfrac{3}{4}|1\rangle\langle 1|_b \end{aligned}$$

The following lemma states a useful property of the trace:

Lemma 3.7 (Cyclic property of trace)**.** *For two linear operators A and B we have:*

$$\mathrm{tr}(AB) = \mathrm{tr}(BA) \tag{3.22}$$

Proof. Let $|b_1\rangle, ..., |b_n\rangle$ be the orthonormal basis of the operators, then we can write:

$$\begin{aligned} \mathrm{tr}(AB) &= \sum_i \langle b_i|AB|b_i\rangle = \sum_{i,j} \langle b_i|A|b_j\rangle\langle b_j|B|b_i\rangle \\ &= \sum_{i,j} \langle b_i|B|b_j\rangle\langle b_j|A|b_i\rangle = \sum_{i,j} \langle b_i|BA|b_i\rangle = \mathrm{tr}(BA) \end{aligned}$$

□

3.6 Fidelity

In section 3.4 we expounded on quantum measurements, such measurements will in general alter the measured measured state. In several occasions it is necessary to quantify how different two states are, for example before and after measurement. An often used measure for the difference between two states is the *fidelity*, defined as:

Definition 3.12 (Fidelity $F(\rho, |\psi\rangle)$). *For a given pure state $|\psi\rangle$ the fidelity of an arbitrary density matrix ρ is defined as:*

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

Example 3.16 (Identical states). *From the definition we see that $F = 1$ if and only if $\rho = |\psi\rangle\langle\psi|$, i.e.: if both states are identical.*

Example 3.17 (Fidelity random guess [80]). *A single qubit is in an unknown pure state $|\phi\rangle$, selected at random over an ensemble uniformly distributed over the Bloch sphere. At random we guess the state of the qubit is $|\psi\rangle$. What, on average, will be the fidelity of our guess?*

If we guess an arbitrary state $|\psi\rangle$, we can rotate the Bloch sphere such that $|\psi\rangle$ is spin up in the z-axis, i.e. $|\psi\rangle = |0\rangle$ in the z-basis. Let the unknown state ϕ be given by $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $\alpha^2 + \beta^2 = 1$ and $0 \leq \alpha, \beta \leq 1$. Then the fidelity of our random guess is:

$$\begin{aligned} F(\rho_\phi, |\psi\rangle) &= \langle\psi||\phi\rangle\langle\phi||\psi\rangle = |\langle\psi||\phi\rangle|^2 \\ &= |\alpha\langle 0, 0|+\rangle\beta\langle 0, 1||\rangle^2 = \alpha^2 \end{aligned} \tag{3.24}$$

Assuming a uniform distribution for α^2 [4], the average fidelity $\bar{F}$ becomes:

$$\bar{F} = \int Ff(f)dF = \int \alpha^2 d(\alpha^2) = \tfrac{1}{2}$$

Example 3.18 (Fidelity classical communication). *Now, suppose we randomly select a qubit ϕ as in the previous example, and we are allowed to make a classical (= projective) measurement, say a projection on its z-axis. What is the fidelity we obtain?*

Assume the arbitrary state $|\phi\rangle$ is the same as in the previous example. Again, without loss of generality we can rotate the Bloch sphere such that we work in the basis of the z-axis. Then the projective measurement operators are $P_0 = |0\rangle$ and $P_1 = \langle 1|$, or equivalently the POVM:

$$E_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \qquad E_1 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

Measuring $|\phi\rangle$ with this POVM projects $|\phi\rangle$ in the following density matrix:

$$\begin{aligned} \rho = p_0 E_0 + p_1 E_1 &= \langle\phi|\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)|\phi\rangle\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \langle\phi|\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)|\phi\rangle\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \\ &= \begin{pmatrix} \alpha^2 & 0 \\ 0 & \beta^2 \end{pmatrix} \end{aligned}$$

The resulting fidelity is:

$$F(x) = \langle\phi|\rho|\phi\rangle = \alpha^4 + \beta^4 = 2\alpha^4 - 2\alpha^2 + 1$$

[4] We guess at random and the probabilities are given by the squares of the factor in front of a vector.

The resulting average fidelity $\bar{F}$ is

$$\bar{F} = \int Ff(f)dF = \int 2\alpha^4 - 2\alpha^2 + 1d(\alpha^2) = \tfrac{2}{3}$$

Thus, the average classical fidelity, i.e. the average fidelity obtainable by classical communication, is $\frac{2}{3}$. For quantum states this is problematic, as it means that we will always loose information if we try to communicate a quantum state in a classical way. As we will see below, with quantum information techniques like teleportation fidelity 1 can be obtained.

Fidelity is a very general definition. In this text we are mainly interested in the relation between the state before and after measurement. Within this context the *entanglement fidelity* is an useful measure as well:

Definition 3.13 (Entanglement fidelity $F_e(\rho)$ [85])**.** *Consider an entangled state $|\psi_{a\otimes b}\rangle$ shared between Alice and Bob with Hilbert space $\mathcal{H}_a$ and $\mathcal{H}_b$ respectively. Suppose that Bob performs operation $\mathcal{E}_b$ on his part of the shared system while Alice doesn't do anything, then the overall operation on the system is given by $\mathcal{I} \otimes \mathcal{E}$ and the state after the operation is:*

$$\rho'_{ab} = \mathcal{I} \otimes \mathcal{E}(|\psi_{ab}\rangle\langle_{ab}\psi|)$$

The fidelity of this process is named the entanglement fidelity

$$F_e = \text{tr}\left(|\psi_{ab}\rangle\langle\psi_{ab}|\rho'_{ab}\right) = \langle\psi_{ab}|\rho'_{ab}|\psi_{ab}\rangle \tag{3.25}$$

In essence, the entanglement fidelity measures how faithfully the entangled state $|\psi_{ab}\rangle$ is preserved under operation $\mathcal{I} \otimes \mathcal{E}$. Although both fidelities look quite similar they are not the same. As illustration, consider the ensemble of states $|\psi_i\rangle$ with probability p_i, given by the density matrix

$$\rho_a = \sum_i p_i |\psi_i^a\rangle\langle\psi_i^a|$$

Let $\mathcal{E}_a$ be a measurement operator and let ρ'^a_i be the state if we apply $\mathcal{E}_a$ to the i^{th} state $\rho'^a_i = \mathcal{E}_a(|\psi_i^a\rangle\langle\psi_i^a|)$. The fidelity of this process is $F_i = \langle\psi_i^a|\rho'^a_i|\psi_i^a\rangle$. Then, the average fidelity of the ensemble is given by

$$\bar{F} = \sum_i p_i F_i$$

For the operator $\mathcal{E}_a$ and initial state ρ_a we can also calculate the entanglement fidelity F_e and it turns out [85] that

$$F_e \leq \bar{F}$$

In this thesis we consider ways to create a perfect quantum channel, as considered above such a channel has fidelity 1. For this situation it can be shown that [86]:

$$F = 1 \text{ for all pure states in the support of } \rho_a \Leftrightarrow F_e = 1 \tag{3.26}$$

In chapter 2 we witnessed the fall of locality within quantum mechanics, something which sets quantum mechanics clearly apart from classical physics. But exactly what caused this dramatic demise wasn't discussed. Using the concepts developed in this chapter, the next chapter will investigate the 'holder' of non-local interactions: entanglement.

CHAPTER 4

ENTANGLEMENT - SPOOKY ACTION AT A DISTANCE

From chapter 2 we know that quantum mechanics is (very likely) non-local. Particles can exhibit non-local behaviour if they are *entangled* [96] [1]. Schrödinger considered entanglement to be the characteristic property of quantum mechanics and it is important because it overcomes the LOCC constraint (*Local quantum Operations and Classical Communication*). In the context of quantum information theory, we can say that all *classical correlations* are due to LOCC operations and correlations that cannot be explained by LOCC operations are quantum correlations. Entanglement is a kind of quantum correlation that plays a quintessential role in quantum communication, because perfect quantum communication is essentially equivalent with perfect entanglement distribution. Loosely, n particles are entangled if the state of one of the particles cannot be described completely without describing the states of the other particles as well. More mathematical, n particles are entangled if they are non-separable, where separable states are defined as:

Definition 4.1 (Separability)**.** *A density operator ρ_{abc} of many parties $a, b, c, ...$ is said to be separable if it can be written as:*

$$\rho_{abc} = \sum_i p_i \rho_a^i \otimes \rho_b^i \otimes \rho_c^i \otimes ...$$

with $\sum_i p_i = 1$

Separable states can be created easily from nothing with LOCC operations: Alice samples from distribution p_i, informs all parties X of her outcome and all parties create ρ_X^i. Separable states satisfy local hidden variable models and don't violate Bell's inequalities. An example of a bipartite (two-party) separable state is:

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)_{ab} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)_a \otimes |0\rangle_b$$

Conversely, non-separable or entangled states cannot be written as the tensor product of the states of different parties, cannot necessarily be described by local hidden variable models and can violate Bell's inequalities. An example of a bipartite entangled state is:

[1] Thus, non-locality implies entanglement, but interestingly the converse is not necessarily true. There are non-local states which do not violate any Bell inequality and are not useful for teleportation. [29]

Example 4.1.

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)_{ab}$$

From this state one can see that a measurement of Alice on her particle will influence Bob's state as well: if Alice measures 0, Bob's state is projected in 0 too, while if Alice measures 1 Bob's state is also 1.

Not all entangled states have the same "amount of entanglement". As illustration, intuitively the state of example 4.1 is more entangled than the state of equation 4.1 below, because the state below "has an entangled and a separable part" whereas the state above is "fully entangled".

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{6}} \left(|00\rangle + |11\rangle\right)_{ab} + \frac{1}{\sqrt{6}} \left(|0\rangle + |1\rangle\right)_{a} |0\rangle_b \tag{4.1}$$

Because entanglement is a quantum correlation the amount of entanglement between two states cannot be increased due to LOCC operations.

There are different types of entanglement, as two states with the same amount of entanglement cannot be necessarily transformed in each other with LOCC operations. This motivates the following definition:

Definition 4.2 (Equivalent entanglement)**.** *Let $|\psi\rangle_1$ and $|\psi\rangle_2$ be two entangled states. $|\psi\rangle_1$ is entangled in an equivalent way as $|\psi\rangle_2$ if both of them can be LOCC-obtained from the other with nonzero probability.*

Pure bipartite entangled states have the convenient property that they are all equivalent. Due to this, the amount of entanglement in bipartite states can be uniquely ordered[2]. The existence of a unique order makes bipartite entanglement the simplest type of entanglement and it will be discussed in section 4.1. Extension to multiparticle entanglement will be discussed in section 4.2.

Up till then, all definitions and examples of entanglement refer to entanglement between objects with discrete states like qudits. However, for example in EPR's paper the position and momentum of the particles were entangled, two continuous variables. The mathematical description of continuous variable entanglement is quite different from the discrete case, but it will be the key to understand the role of entanglement within cosmology and is studied in section 4.3. Section 4.4 gives some basic mathematics to calculate with quantum channels, entangled states used for information transfer. Despite all mathematics above, entanglement remains a mind boggling concept and perhaps the only reason it is accepted by the scientific community is its experimental observation. Section 4.5 will highlight the most important experimental results. Finally, in section 4.6 the theoretical limitations of entanglement are discussed: no cloning and no superluminal communication.

4.1 Bipartite entanglement

One of the most important properties of bipartite entanglement is that all bipartite entangled states are equivalent, due to the existence of an unique maximally entangled state[3]. Below it will be shown that every bipartite pure state can be LOCC-obtained from the maximally entangled state with certainty. In other parts of this thesis, mainly in the chapters 5 and 6, we will prove

[2] I.e. for a given state the amount of entanglement may differ for different entanglement measures, but the order in increasing amount of entanglement is the same for all possible entanglement measures.

[3] Here unique has to be read as unique up to a local unilateral operation.

that the converse is true as well, be it probabilistically instead of with certainty. Two major references for this section are [79] and [77].

Theorem 4.1. *For an m-dimensional qudit the maximally entangled states are given by:*

$$|\mu\rangle_m = \frac{1}{\sqrt{m}}\left(|00\rangle + |11\rangle + \ldots + |m-1, m-1\rangle\right) \tag{4.2}$$

We'll prove this theorem for the bipartite pure qubit case, as these states are the major players in this thesis. (For the qudit case, the interested reader is referred to [100].)

Lemma 4.2. *The Bell states as defined in example 3.9 are the maximally entangled bipartite pure qubit states.*

Proof. To show this, we have to show that a Bell state, we take

$$|\phi\rangle^+ = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

can be transformed into an arbitrary bipartite pure qubit

$$|\psi\rangle = \xi\left(|00\rangle + x|11\rangle\right) \tag{4.3}$$

with $\xi = \frac{1}{\sqrt{1+x^2}}$ and $x \in [0, 1]$.

Suppose Alice and Bob share the Bell state above and Alice adds an ancilla particle in the state $|\psi\rangle_1 = |0\rangle$, then the combined state is given by:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |011\rangle\right)_{1ab} \tag{4.4}$$

where the a and b stand for Alice's respectively Bob's part of the shared pair. If Alice performs the following measurement on her particles:

$$M_1 = \xi\left(|0\rangle\langle 0| + x|1\rangle\langle 1|\right) \otimes \mathbb{I}$$
$$M_2 = \xi\left(x|1\rangle|0\rangle + |0\rangle|1\rangle\right) \otimes \left(|1\rangle\langle 0| + |0\rangle\langle 1|\right)$$

the resulting density matrix is given by:

$$\rho_{\text{output}} = M_1|\psi\rangle\langle\psi|M_1^\dagger + M_2|\psi\rangle\langle\psi|M_2^\dagger$$

which has corresponding output state

$$|\psi\rangle_{\text{output}} = \frac{1}{\sqrt{2}}\xi\left[|0\rangle_1\left(|00\rangle + x|11\rangle\right)_{ab} + |1\rangle_1\left(x|10\rangle + |01\rangle\right)_{ab}\right]$$

Subsequently, Alice measures her ancilla particle 1 and informs Bob of her measurement result. If she measures $|0\rangle$, then the two parties obtain the desired state. If she measures $|1\rangle$, Alice has to perform a unitary rotation and they obtain the desired state $|1\rangle$ as well. So given a Bell state any arbitrary bipartite pure qubit state can be obtained with certainty. Since mixed states are sums of pure states, any bipartite mixed qubit state can be obtained as well. □

Before we proceed we need to deal with a technicality. As just shown, a maximally entangled qubit can be transformed to any other qubit state with certainty. Furthermore, it will be shown later that any qubit can be transformed probabilistically to a maximally entangled qubit. Thus, every qubit can be transformed probabilistically to any other qubit. For transformations between qudits in general this is not the case. Consider for example the transformation from $|\phi\rangle^+$ to

$|\psi\rangle_2 = \frac{1}{\sqrt{1+\epsilon^2}}\left(\sqrt{\frac{3}{4}}|00\rangle + \sqrt{\frac{1}{4}}|11\rangle + \epsilon|22\rangle\right)$. For any $\epsilon > 0$ the success probability of this transformation is 0, as one can see directly from the fact that this transformation would require an increase of the Schmidt number. The state $|\psi\rangle_2$ can only be approximated. This kind of problems can be solved by considering not one but r transformations at the same time. In the asymptotic limit of $r \to \infty$ an arbitrary good approximation is possible [79].

The existence of maximally entangled states sets a maximum for a quantitative entanglement scale and the zero-point of an entanglement scale is set by separable states. How to scale in between? Throught the years, several measures have been put forward, below we will discuss the most important ones.

Consider an arbitrary state $|\varphi\rangle$, an often used and physically meaningfull scaling is the amount of copies p of $|\varphi\rangle$ one can create from q maximally entangled m-dimensional states $|\mu\rangle_m$, thus the ratio $r = q/p$, using LOCC operations. Let Λ stand for a series of LOCC operations, define $\rho_\mu = |\mu\rangle\langle\mu|$ and $\rho_\varphi = |\varphi\rangle\langle\varphi|$, then we get the following entanglement measure:

Definition 4.3 (Entanglement cost $E_C(\rho_\varphi)$)**.**

$$E_C(\rho_\varphi) = \inf\left\{r : \lim_{p\to\infty}\left[\inf_{\Lambda} D\left((\rho_\varphi)^{\otimes p}, \Lambda(\rho_\mu^{\otimes pr})\right)\right] = 0\right\}$$

with $D(\rho_1, \rho_2)$ a distance measure between density matrices; an often used measure is $\operatorname{tr}|\rho_1 - \rho_2|$. The limit is taken to prevent problems with states that cannot be transformed directly, as discussed above.

Instead of computing the number of states $|\varphi\rangle$ which can be obtained from a maximally entangled state, also the number of states $|\varphi\rangle$ required to LOCC-create one maximally entangled state can be computed, a process named entanglement distillation[4]. This gives another entanglement measure:

Definition 4.4 (Entanglement distillation $E_D(\rho_\varphi)$)**.**

$$E_D(\rho_\varphi) = \sup\{\left\{r : \lim_{p\to\infty}\left[\inf_{\Lambda} D\left((\rho_\varphi)^{\otimes p}, \Lambda(\rho_\mu^{\otimes pr})\right)\right] = 0\}\right\}$$

In general E_C and E_D are different, but in the asymptotic limit for pure states they coincide and equal the entanglement entropy $E(\rho)$ [12]. The entanglement entropy comes from the quantum generalization of the *Shannon entropy*, a definition from classical information theory that we will investigate now.

The major role of entanglement within this thesis is as information carrier, as entanglement allows the communication of qubits, which is impossible with classical physics. From this perspective, it is useful to define a quantitative entanglement measure based on the amount of information which can be transferred with it. Classically, the average amount of information 'contained' in a random variable is given by the *Shannon entropy*, defined as:

Definition 4.5 (Shannon entropy $H(X)$)**.** *Let X be a random variable with outcomes $x_1, x_2, ..., x_n$ and corresponding probabilities $p_1, p_2, ..., p_n$, than the average amount of information gained if X is measured is given by:*

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

with the convention that $0\log_2 0 = 0$.

[4]This is one of the ways in which Alice and Bob can obtain a maximally entangled state. Various methods for entanglement distillation will be investigated in chapter 6.

Example 4.2. *Being a true romantic, each week Bob gives Alice a rose. The random variable X is the colour of the rose X, which can be $x_1 =$ red, $x_2 =$ pink, $x_3 =$ yellow and $x_4 =$ white.*

- *Suppose the colour of the rose depends on Bob's mood and Bob is rather capricious, than we have $(p_1, p_2, p_3, p_4) = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ and $H(X) = \log_2(\frac{1}{4}) = 2$. When Alice receives Bob's rose, she at once knows his mood.*
- *If Bob gives Alice a red rose every week, independent of his mood, we have $(p_1, p_2, p_3, p_4) = (1, 0, 0, 0)$ and $H(X) = 0$. This is to be expected, as Alice obtains no information on how Bob feels.*
- *If Bob's mood influences the colour, but independently of his mood he has a preference for certain colours, $H(X)$ will be in between 0 and 2. For example, say $(p_1, p_2, p_3, p_4) = (\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8})$, than $H(X) = \frac{7}{4}$. In this case, Alice obtains some information about Bob's mood, but she can't be completely sure because he might have given a red rose even if he doesn't feel that way.*

Example 4.3 (Ref: [69])**.** *A bit more technical, suppose Bob sends Alice one of the symbols r, p, y, w each week. Without compression this requires 2 bits of storage for each symbol. Suppose, however, that Bob sends Alice the symbols with the following probability: $(p_r, p_p, p_y, p_w) = (\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8})$. Usage of the fact that r is more often sent than y or w a more efficient coding can be devised. The most efficient coding scheme is given by letting symbol 0 stand for r, the symbols 10 for p, 110 for y and 111 for w. Than on average the amount of space required is only $1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} + 3 \cdot \frac{1}{8} + 3 \cdot \frac{1}{8} = \frac{7}{4}$, which equals the Shannon entropy!*

What is true in this example is true in general: the Shannon entropy defines the optimal way to store data. The quantum analogue of the Shannon entropy is given by the Von Neumann entropy and interestingly, towards the end of this thesis it will turn out that the Von Neumann entropy defines the optimal way in which maximally entangled pairs between Alice and Bob can be obtained.

Definition 4.6 (Von Neumann entropy $S(\rho)$)**.** *Let ρ be a pure density matrix with Schmidt coefficients $\lambda_1, ..., \lambda_n$, than*

$$S(\rho) = -\operatorname{tr}(\rho \log_2 \rho) = -\sum_{i=1}^{n} \lambda_i \log_2 \lambda_i$$

where the second equality is justified by the observation that every pure state can be diagonalized as a Schmidt decomposition and that in such a case the eigenvalues are the Schmidt coefficients. Analogous to the Shannon entropy the Von Neumann entropy says something about the information content of a quantum variable, so the amount of entanglement is naturally quantified by the Von Neumann entropy [12]:

Definition 4.7 (Entropy of entanglement)**.** *Let ρ be a density matrix of a pure state shared between Alice and Bob and let S be the Von Neumann entropy, then the entropy of entanglement is defined as:*

$$E(\rho) = S(\operatorname{tr}_a \rho) = S(\operatorname{tr}_b \rho) \tag{4.5}$$

Example 4.4. *Suppose Alice and Bob 'share' the separable state $|\psi\rangle = |0\rangle_a |1\rangle_b$, then:*

$$\operatorname{tr}_b(|\psi\rangle\langle\psi|) = |0\rangle\langle 0|$$

and consequently, $E(|\psi\rangle\langle\psi|) = -1 \cdot \log_2 1 - 0 \cdot \log_2 0 = 0$, as was to be expected.

Example 4.5. *Suppose Alice and Bob share the state* $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$*, then:*

$$\mathrm{tr}_b(|\phi^+\rangle\langle\phi^+|) = \tfrac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

and consequently, $E(|\phi^+\rangle\langle\phi^+|) = -2 \cdot \frac{1}{2}\log_2(\frac{1}{2}) = 1$.

The entanglement cost, entanglement distillation and entanglement entropy are just three of many entanglement measures, which are all suitable for different purposes. The fact that there are many measures probably signifies that entanglement isn't understood that well, yet... Nevertheless, not every function can be an entanglement measure; by definition a function is an entanglement measure if and only if it satisfies the following properties:

Definition 4.8 (Properties of a bipartite entanglement measure)**.** *Let* M *be the space of normalized bipartite density matrices* ρ*. Than an entanglement measure* $E(\rho)$ *is a mapping from* $\rho \in M \to E(\rho) \in \mathbb{R}^+$ *that satisfies:*

1. *For a separable state* $E(\rho) = 0$ *and for a maximally entangled qudit* $E(\rho) = \log d$*.*
2. E *cannot increase on average under LOCC operations.*
3. *For pure states* E *is additive.*
4. *For pure states* E *is continuous in the asymptotic limit.*

Of course, all entanglement measures of the previous section satisfy the criteria above. Because it is directly related to the information content and it is easy to use; in the rest of this thesis the entanglement entropy will be used as entanglement measure.

We now discussed how to scale entangled states, but how do we know whether a state is entangled in the first place? For a given arbitrary bipartite state it is not always straightforward to find out whether the state is entangled or not. For 2×2 and 2×3 systems (i.e. bipartite systems in which Alice has a qubit and Bob has respectively a qubit and a 3-qudit), an easy test was devised by Peres and Horodecki [75, 48]:

Theorem 4.3 (Discrete Peres-Horodecki criterion for entanglement)**.** *Let* $\rho_{m\mu,n\nu}$ *be a density matrix in which the Latin and Greek indices refer to Alice's respectively Bob's particle. Define the partial transpose of a density matrix* $\rho_{m\mu,n\nu}$ *as* $\varrho_{m\mu,n\nu} = \rho_{n\mu,m\nu}$*. A necessary condition for* ρ *to be separable is if* ϱ *has only non-negative eigenvalues. For* 2×2 *and* 2×3 *systems this condition is also sufficient.*

4.2 Multipartite entanglement

Until now we only considered entanglement between two particles, but more than two particles can be entangled with each other as well. The simplest example of this is the tripartite case. Consider Alice, Bob and Charlie who share the GHZ-state, defined as:

$$|GHZ\rangle_{abc} = \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{abc} \tag{4.6}$$

This state can neither be rewritten as a product state of a separate state and a bipartite state nor as three separable states; hence, the three particles of Alice, Bob and Charlie are entangled with each other. Multi-particle entanglement is a crucial element for quantum computing, quantum error correction codes and quantum key distribution [33] so a good understanding of this phenomenon is important. However, multi-particle entanglement is genuinely different and much more difficult than bipartite entanglement: there are inequivalent types of entanglement which cannot be transformed in each other, not even in the asymptotic limit. Such a situation is already encountered in tripartite entanglement, consider for example the *W-state*:

$$|W\rangle_{abc} = \frac{1}{\sqrt{3}} \left(|001\rangle + |010\rangle + |100\rangle\right)_{abc} \tag{4.7}$$

It can be shown [30] that the GHZ-state cannot be LOCC-transformed to the W-state.

Sketch of proof. Physically, the crux of the proof is in the observation that the minimum number of product terms in any given state remains unchanged under LOCC. As the GHZ-state has as minimum of 2 and the W-state of 3 product terms, both states cannot be LOCC-transformed in each other. To understand why the minimum number of product terms cannot increase under LOCC, consider a general invertible local operator[5] $A = A_1 \otimes A_2 \otimes A_3$. The most general pure state that can be obtained from, for example, the GHZ-state is then of the form:

$$A|GHZ\rangle = (A_1 \otimes A_2 \otimes A_3)|GHZ\rangle = \frac{1}{\sqrt{2}} \left(|A_1 0\rangle|A_2 0\rangle|A_3 0\rangle + |A_1 1\rangle|A_2 1\rangle|A_3 1\rangle\right). \tag{4.8}$$

Since A_i is invertible for all i, $|A_i 0\rangle$ and $|A_i 1\rangle$ are linearly independent vectors. Thus the minimal number of product terms is the same before and after transformation. The same is true for any arbitrary multipartite state, including the W-state. □

Inequivalent entangled states form different entanglement classes. For the tripartite case, six inequivalent classes can be distinguished, among which the GHZ-state and the W-state. Because local operations can never create entanglement between unentangled systems, the product state $|\psi\rangle_A|\psi\rangle_B|\psi\rangle_C$ forms another class, and so do three classes of a combination between a bi-partite subsystem and a product state $|\psi\rangle_{i,j}|\psi\rangle_k$, with i, j, k permutations of A, B, C.

In the bipartite case, an entanglement measure followed naturally by considering the asymptotic limit conversion rate to or from the maximally entangled state. In the multipartite case we have a set of different entanglement classes, thus a natural generalization of the bipartite scenario might be a Minimal Reversible Entanglement Generating Set (MREGS): a set of pure states from which every other state can be generated by means of reversible asymptotic LOCC operations. For example, for the tripartite case the set of the GHZ-state, the W-state, the three classes of bi-partite subsystems with product state together with the 'full' product state is an intuitive choice of MREGS. However, neither for the tripartite case nor for higher dimensional cases any set of states is be shown to be a MREGS.

Until a good way to quantify multiparticle entanglement has been found, a full blown multiparticle entanglement theory seems unfeasible [33, 79]. Nevertheless, for practical purposes some entanglement quantifying functions which satisfy the first two axioms of definition 4.8 have been developed. As in this thesis we focus on bipartite entanglement, detailed discussion of these functions and other interesting properties of multiparticle entanglement is beyond the scope of this thesis. The interested reader referred to the references mentioned in this section.

Although a unique way to quantify multipartite entanglement has not been developed yet, a unique way to *describe* pure tripartite entanglement has been found [3]. It turns out that by well chosen LOCC operations every pure tripartite entangled state can be casted in a form that is described be five instead of the complete $2^3 = 8$ parameters: one phase parameter (all others

[5] An invertible local operator is an operator working on all parts locally and of which all local parts are invertible.

can be absorbed) and four coefficient moduli. This is analogous to the pure bipartite case, where Schmidt Decomposition allows one to write such a state with two instead of $2^2 = 4$ parameters. This minimal basis decomposition of pure tripartite entangled states is given by:

$$|\psi\rangle_{abc} = \left(\Xi|000\rangle + x_1 e^{i\mu}|100\rangle + x_2|101\rangle + x_3|110\rangle + x_4|111\rangle\right)_{abc} \tag{4.9}$$

with $\Xi = \sqrt{1 - x_1^2 - x_2^2 - x_3^2 - x_4^2}$, $x_i \in [0, 1]$ and $\mu \in [0, \pi]$ and shall be of use to us in chapter 7.

Result 4.1. *The simplest form of entanglement is bipartite entanglement. This type of entanglement is be ordered uniquely and several entanglement measures exist, among which entanglement cost, entanglement distillation and entanglement entropy. Multipartite entanglement is more difficult to quantify than bipartite entanglement because there are inequivalent types of states.*

Some properties which can be entangled are not discrete but continuous, the earlier examples of position and momentum being two of them. Therefore, the next section discusses continuous variable entanglement. As continuous entanglement is quite different from the discrete entanglement we discussed so far, first the most important results on discrete entanglement.

4.3 Continuous variable entanglement

Experimentally, continuous variable entanglement is important because essential steps in optical quantum communication can be implemented efficiently in the continuous setting. Examples are preparing, unitarily manipulating and measuring entangled states. From a theoretical perspective generalization to continuous variables is far from trivial, as we need to go from quantum mechanics to quantum field theory. Luckily, a general discussion of continuous entanglement is not necessary because we can make two simplifications: we (mainly) consider states which are (i) bipartite and (ii) Gaussian. First, we will introduce some basic concepts and notation from quantum field theory and derive the basic Lagrangian. Subsequently, conditions for states to be physical and Gaussian are described and continuous entanglement measures are discussed. The main references for this section are [108], [23] and [78].

4.3.1 Quantum field theory

Quantum field theory is the generalization of quantum mechanics. Whereas quantum mechanics deals with systems with small degrees of freedom, quantum field theory considers systems with (possibly) an infinite number of degrees of freedom. Below, we will (i) derive the basic QFT Lagrangian; (ii) write down the commutation relations; and finally (iii) consider the continuous density operator.
To get the basic idea of QFT and to derive the Lagrangian, consider a two-dimensional field represented by a lattice of point masses connected to each other with strings, as shown in figure 4.1 below.
Let the point masses be indexed by j, denote its canonical position with q_j and define its canonical momentum p_j as $p_j = \delta L/\delta \dot{q}_j = \dot{q}_j$. Then its classic Lagrangian L is given by:

$$L = \tfrac{1}{2}\left(\sum_j m\dot{q}_j^2 - \sum_{jk} d_{jk}q_j q_k - \sum_{jkn} q_j q_k q_n - \cdots\right) \tag{4.10}$$

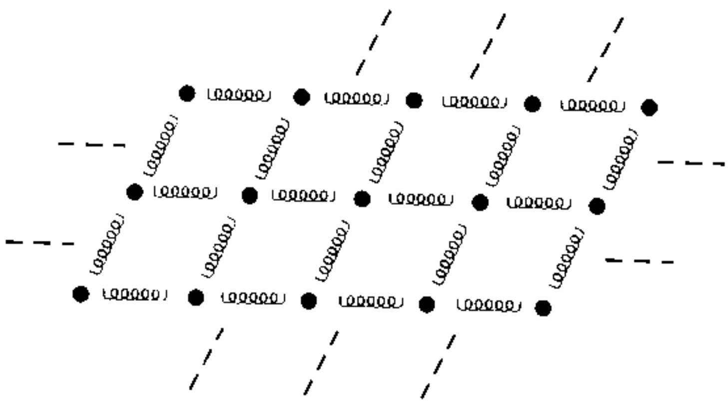


Figure 4.1: *[108] This two dimensional lattice of point masses serves as starting point for quantum field theory.*

In a handwaving way, to make the step to from the Lagrangian above to a Lagrangian in quantum field theory, we have to do two things. First, we retain only the quadratic terms in the Lagrangian and obtain the equation of motion $m\ddot{q}_j = -\sum_k d_{jk} q_k$. [6] This is called the harmonic approximation. Second, we let the distance between subsequent particles in the lattice of figure 4.1 go to zero. Taking into account that in quantum field theory it is custumary to replace the letter q by ϕ, we get the following substitutions: the index j is replaced by the continuous function $\vec{x}$, $q_j \to \phi(\vec{x})$ and $\sum_j \to \frac{1}{2l^2} \int d^2x$, with l the distance between the point masses.

With these substitutions, the kinetic term in Lagrangian 4.10 becomes

$$\sum_j m\dot{q}_j^2 \to \tfrac{m}{l^2} \int d^2x \dot{\phi}^2$$

To handle the terms within $\sum_{jk} d_{jk} q_j q_k$, note that we can write $2q_j q_k = (q_j - q_k)^2 - q_j^2 - q_k^2$. If we assume that d_{jk} only connects to neighboring particles, we obtain in the continuum limit $(q_j - q_k)^2 \propto l^2(\partial\phi/\partial x)^2 + \cdots$. This gives us:

$$\sum_{jk} d_{jk} q_j q_k \to \tfrac{1}{l^2} \int d^2x d(\vec{x}) \left[l^2 \left(\frac{\partial\phi}{\partial x}\right)^2 + \left(\frac{\partial\phi}{\partial y}\right)^2 + \phi^2 \right]$$

Setting $\alpha = m/l^2$ and $d(\vec{x}) = \alpha c^2$, we obtain for the Lagrangian:

$$L = \tfrac{1}{2} \int d^2x \alpha\dot{\phi}^2 - \alpha c^2 \left[l^2 \left(\frac{\partial\phi}{\partial x}\right)^2 + \left(\frac{\partial\phi}{\partial y}\right)^2 + \phi^2 \right]$$

By rescaling $\phi \to \phi/\sqrt{\alpha}$ the expression $\dot{\phi}^2 - c^2 \left[(\partial\phi/\partial x)^2 + (\partial\phi/\partial y)^2 \right]$ appears in the Lagrangian and it becomes:

$$L = \tfrac{1}{2} \int d^2x \dot{\phi}^2 - c^2 \left[l^2 \left(\frac{\partial\phi}{\partial x}\right)^2 + \left(\frac{\partial\phi}{\partial y}\right)^2 + \phi^2 \right]$$

[6] Because of this, p_j and q_j are often called quadratures.

The derivation above was a bit handwaving, a full derivation would result in:

$$L = \frac{1}{2} \int d^n dx \left(\dot{\phi}^2 - (\vec{\nabla}\phi)^2 - m^2\phi^2 \right) \tag{4.11}$$

with n the dimension of the space. This Lagrangian will be of use later.

4.3.2 Canonical commutation relations

As described in section 3, the position and momentum operators don't commute. By promoting p_j and q_j from variables to the operators $\hat{p}_j$ and $\hat{q}_j$, we can write down the canonical commutation relations:

$$\begin{aligned} [\hat{q}_j, \hat{p}_k] &= i\hbar\delta_{jk} \\ [\hat{q}_j, \hat{q}_k] &= [\hat{p}_j, \hat{p}_k] = 0 \end{aligned} \tag{4.12}$$

Let an arbitrary bipartite n-mode state vector be given by:

$$\varsigma = (q_1, ..., q_n, p_1, ..., p_n)^T \tag{4.13}$$

then its canonical commutation relations be written down together as

$$[\varsigma_j, \varsigma_k] = iJ^n_{jk} \tag{4.14}$$

with $j, k \in 1, ..., 2n$ and J^n the matrix defined as

$$J^n = \begin{pmatrix} O_n & I_n \\ I_n & O_n \end{pmatrix} \tag{4.15}$$

with I_n the $n \times n$ identity matrix and O_n the $n \times n$ zero matrix.

In order to be a physical operation, the most general linear transformation $S : \varsigma \to \varsigma' = S\varsigma$ over the state vector ς must preserve the canonical commutation relations 4.14. The linear maps S with this property are $2n \times 2n$ real matrices with the property

$$SJ^nS^T = J^n \tag{4.16}$$

Matrices with this property are called *symplectic matrices* and together they form the symplectic group.

4.3.3 The continuous density operator

Density matrices ρ corresponding to a vector ς can be defined by functions on the phase space by using the Weyl operator, which for a vector $\varsigma \in \mathcal{R}^{2n}$ is defined as:

$$W_\varsigma = \exp\left(i\varsigma^T J\varsigma\right) \tag{4.17}$$

Weyl operators generate phase space displacement and are used to define the characteristic function of ρ:

$$\Phi_\rho(\varsigma) = \mathrm{tr}(\rho W_\varsigma) \tag{4.18}$$

Inversion of this relation gives a unique density matrix ρ.

An arbitrary state can be defined equivalently using the *Wigner function*, which for one bipartite mode reads:

$$W(q,p) = \pi^{-2} \int d^2q' \langle q - q'|\rho|q + q'\rangle \exp(2iq' \cdot p) \tag{4.19}$$

where $q = (q_1, q_2)$ and $p = (p_1, p_2)$. This function has several nice properties. Set $\alpha = q + ip$, such that $d^2\alpha = d(\Re\alpha)d(\Im\alpha) = dqdp$, let $\hat{A}$ be an operator with real function $A(\alpha)$ and let ρ be a density matrix, then:

$$\int W(\alpha)d^2\alpha = 1 \qquad \int W(q,p)dq = \langle p|\rho|p\rangle \tag{4.20}$$
$$\int W(\alpha)A(\alpha)d^2\alpha = \langle\hat{A}\rangle \qquad \int W(q,p)dp = \langle q|\rho|q\rangle$$

4.3.4 Physical and Gaussian states

An important class of states are the Gaussian states, defined as:

Definition 4.9 (Gaussian states)**.** *A continuous variable quantum state is Gaussian if its characteristic function is a Gaussian, i.e.:*

$$\Phi_\rho(\varsigma) = \Phi_\rho(0)\exp(-\tfrac{1}{2}\varsigma^T J^T V J\varsigma + iD^T J^T \varsigma)$$

Here, D is the first moment of the displacement vector: $D_i = \mathrm{tr}(\varsigma_i\rho)$, with $i \in 1, 2, ..., 2n$. The second moment of the displacement vector is the real symmetric $2n \times 2n$-dimensional covariance matrix V, defined as:

$$V_{jk} = \tfrac{1}{2}\,\mathrm{tr}\left(\rho\{\varsigma_j, \varsigma_k\} - 2\rho\langle\varsigma_j\rangle_\rho\langle\varsigma_k\rangle_\rho\right) \tag{4.21}$$

with $\{\}$ the anti-commutator. Thus, a Gaussian state requires only $2n^2 + n$ parameters, making is polynomial rather than exponential.

Gaussian states are important and widely used for two reasons: (i) they are efficiently producible in a laboratory and (ii) they are mathematically much better understood than non-Gaussian states. Therefore, in the remainder of this thesis we will mainly use Gaussian states.

Not every state is a physical state. In general, to check whether a state is physical one has to check whether a general linear transformation preserves the canonical commutation relations 4.14. For Gaussian states, there is an easier way to determine whether the state is physical:

Theorem 4.4. *A necessary and sufficient condition for a Gaussian state to be physical [93] is*

$$V + \frac{i}{2}J \geq 0$$

Proof. Consider the arbitrary state vector ς satisfying the commutation relations 4.14. Without loss of generality we can assume that $\langle|\varsigma\rangle\rangle = 0$. As its density matrix can be written as a sum of its commutator and anti-commutator, we can write

$$\begin{aligned}\rho_{\varsigma_{\mu\nu}} &= \tfrac{1}{2}\{\varsigma_\mu, \varsigma_\nu\} + \tfrac{1}{2}[\varsigma_\mu, \varsigma_\nu] \\ &= \tfrac{1}{2}\{\varsigma_\mu, \varsigma_\nu\} + \tfrac{i}{2}J\end{aligned} \tag{4.22}$$

Averaging results in

$$\langle|\varsigma\rangle\langle\varsigma|_{\mu\nu}\rangle = V + \tfrac{i}{2}J \tag{4.23}$$

The necessity of $V + \frac{i}{2}J \geq 0$ follows from the fact that the entries of Ψ are Hermitian. The sufficiency requires more work. Note that we can rewrite the correlation matrix V in block form as

$$V = \begin{pmatrix} V_1 & V_2 \\ V_2^T & V_4 \end{pmatrix} \tag{4.24}$$

with

$$(V_1)_{jk} = \langle q_j q_k \rangle$$
$$(V_2)_{jk} = \tfrac{1}{2}\langle q_j, q_k \rangle$$
$$(V_3)_{jk} = \langle p_j p_k \rangle$$

It turns out the proof can be reduced to the simplest case: a single-mode 2×2 system. The 2×2 correlation matrix and J-matrix for such a system are given by

$$V = \begin{pmatrix} \langle \hat{q}^2 \rangle & \frac{1}{2}\langle \hat{q}, \hat{p} \rangle \\ \frac{1}{2}\langle \hat{q}, \hat{p} \rangle & \langle \hat{p}^2 \rangle \end{pmatrix} \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{4.25}$$

From the canonical commutation relations 4.14 follows the uncertainty principle

$$\det(V) = \langle \hat{q}^2 \rangle \langle \hat{p}^2 \rangle - [\tfrac{1}{2}\langle \hat{q}, \hat{p} \rangle]^2 \geq \tfrac{1}{4} \tag{4.26}$$

In the special case that

$$V = \begin{pmatrix} \kappa & 0 \\ 0 & \kappa \end{pmatrix} \tag{4.27}$$

the uncertainty principle reduces to $\kappa \geq \frac{1}{2}$.

Now we consider the general case. Start with density matrix ρ with variance matrix V. Let S be a unitary symplectic operator and define $\rho' = S\rho S^\dagger$ and $\mathrm{tr}(\rho'\varsigma\varsigma^T) = V + \frac{i}{2}J$, then using the cyclic property of the trace we get:

$$V' + \tfrac{i}{2}J = \mathrm{tr}(\rho S^\dagger \varsigma\varsigma^T S)$$

As the matrices $S\varsigma$ satisfy the commutation relations 4.14, the equation above reduces to

$$V' + \tfrac{i}{2}J = S(V + \tfrac{i}{2}J)S^T$$

and since by definition $SJS^T = J$, we obtain

$$V' = SVS^T \tag{4.28}$$

i.e. V' is the symplectic matrix transform of V. Clearly, if V is physically realizable then so is V' and vice versa. Thus, if for a given V we can find a canonical symplectic transform V' which can be tested by inspection, we have an easy way to determine whether a state is physically realizable. Such a canonical form exists by virtue of Williamson's theorem [105]: for any symmetric positive-definite $2n \times 2n$ matrix V there exists an S such that the symplectic transform of V by S has the canonical scaled diagonal form

$$V_{\text{can}} = SVS^T = \text{diag}(\kappa_1, \kappa_2, ..., \kappa_n, \kappa_1, \kappa_2, ..., \kappa_n) \tag{4.29}$$

The canonical form is unique up to the order of the κ_j's. As the phase-space variables for different j are not correlated with each other, the problem simply reduces to n times the 2×2 case discussed above and consequently, V and V_{can} are physical density matrices if and only if

$$\kappa_j \geq \tfrac{1}{2} \forall j \tag{4.30}$$

Equation 4.29 allows us to write

$$V_{\text{can}} + \tfrac{i}{2}J = \begin{pmatrix} \kappa_1 & & & \frac{i}{2} & & \\ & \ddots & & & \ddots & \\ & & \kappa_n & & & \frac{i}{2} \\ \frac{-i}{2} & & & \kappa_1 & & \\ & \ddots & & & \ddots & \\ & & \frac{-i}{2} & & & \kappa_n \end{pmatrix} \tag{4.31}$$

With induction on n one can show that this matrix has eigenvalues $k_j \pm \frac{1}{2}$, thus condition 4.30 is equivalent with the demand that $V_{\text{can}} + \frac{i}{2}J$ has only non-negative eigenvalues, which on its turn is equivalent with $V_{\text{can}} + \frac{i}{2}J$ being positive-semidefinite[7]. To understand this last statement, consider an arbitrary matrix A with the eigenvector matrix V and the eigenvalue matrix Λ, then for an arbitrary non-zero vector x we have:

$$x^T A x = x^T Q \Lambda Q^T x = \sum_j c_j^2 \lambda_j \geq 0 \forall j \tag{4.32}$$

Since the symplectic transformation

$$S\left(V + \tfrac{i}{2}J\right) S^T = V_{\text{can}} + \tfrac{i}{2} \tag{4.33}$$

is a transformation of real symmetric transformation by a nonsingular matrix, the signs of the eigenvalues won't change, thus $V + \frac{1}{2}J$ is positive semidefinite if and only if $V_{\text{can}} + \frac{i}{2}J$ is positive semi-definite. Hence, we have

$$V + \tfrac{i}{2}J \geq 0 \tag{4.34}$$

□

4.3.5 Entanglement and entanglement measures

The theorem above gives us a clue when a state is physical, but we also need a way of checking whether a physical state is entangled. As was mentioned above, a continuous density matrix can be defined with Wigner functions, establishing a one-one correspondence between density matrices and Wigner function. Now we can generalize the Peres-Horodecki criterion (theorem 4.3) to the continuous variable case:

Theorem 4.5 (Continuous Peres-Horodecki criterion for entanglement [92])**.** *The partial transpose of a bipartite state transforms $W(q_1, p_1, q_2, p_2)$ to $W(q_1, p_1, q_2, -p_2)$, i.e. mirror reflection in momentum space. In matrix form, the partial transpose transforms state ς to $\tilde{\varsigma} = \Lambda\varsigma$, with $\Lambda = diag(1, 1, 1, -1)$. Consequently, the partial transpose of the correlation matrix V is given by $\tilde{V} = \Lambda V \Lambda$*

[7]A positive semi-definite matrix A has the property that for arbitrary non-zero vectors x one has $x^T A x \geq 0$.

A bipartite Gaussian continuous variable state is separable if and only if its partial transpose is positive, which by the above is equivalent with the statement

$$\tilde{V} + \tfrac{i}{2}J \geq 0$$

Already in the discrete case we encountered several inequivalent entanglement measures, but in the continuous case the situation worsens even further. The most obvious entanglement measures, entanglement cost and entanglement distillation, are extremely difficult to compute explicitely in the continuous setting [79]. Instead, two slightly more practical continuous entanglement measures will be discussed, both for Gaussian states.

Definition 4.10 (Entropy of entanglement)**.** *Assume Alice and Bob share a pure Gaussian system with $n = n_A + n_B$ modes described by covariance matrix V and denote the symplectic eigenvalues of Alice's reduced system with μ_i, than the continuous entropy of entanglement is given by:*

$$E(\rho) = \sum_{i=1}^{n_A} \left(\tfrac{1}{2}(\mu_i + 1) \log_2 \tfrac{1}{2}(\mu_i + 1) - \tfrac{1}{2}(\mu_i - 1) \log_2 \tfrac{1}{2}(\mu_i - 1) \right) \tag{4.35}$$

Intuitively, one can see the logic behind this measure: one obtains it by bringing the covariance matrix to its normal form and then one determines the entanglement for single mode states. The disadvantage is that the definition only works for pure states. For general states, the following entanglement measure is more useful:

Definition 4.11 (Logarithmic negativity)**.** *Assume Alice and Bob share a Gaussian system with $n = n_A + n_B$ modes described by covariance matrix V. Denote the eigenvalues of the partially transposed covariance matrix as $\tilde{\lambda}_k$, than we obtain:*

$$E_N = -\sum_{i=1}^{n} \log_2 \left(\min(1, \hat{\lambda}_k) \right) \tag{4.36}$$

Because the minimum of the eigenvalues is considered, the logarithmic negativity gives an upper bound rather than a detailed measure.

To summarize the major results from continuous entanglement:

Result 4.2. *Continuous variable entanglement describes correlations between continuous observables and is fully described by modes. Handling general continuous variable entanglement is rather difficult and for most practical purposes the subset of Gaussian states is sufficient. These states are mathematically relatively easy and thank there name from the fact that their characteristic function is a Gaussian. For Gaussian states, a criterium to determine whether a state is physical and whether a state is entangled is developed. Two useful continuous variable entanglement measures are entanglement entropy and logarithmic negativity.*

4.4 Quantum channels

Entanglement allows stronger correlations between two or more objects than classicly possible and can be used to transfer quantum information. If an entangled state ρ is used to transfer (quantum) information, this state is called a *quantum channel* and is denoted by Λ. It can be shown that the set of channels Λ on the set of d-dimensional states is isomorphic to the set of density matrices ρ acting on the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, satisfying $\mathrm{tr}_{\mathcal{H}_2}(\rho) = I/d$ [49]. Thus, to every channel we can ascribe a state and vice versa. It should be noted that this isomorphism is strictly mathematical: if Alice and Bob are connected by channel Λ they can create a state ρ_Λ by sending a maximally entangled state through, but if Alice and Bob share state ρ_Λ it is not always physically possible to create a channel Λ.

To measure how faithful a channel preserves a state we define the channel fidelity $F(\Lambda)$ and the channel entanglement fidelity $F_e(\Lambda)$, which compare the state ρ before and after it went through the channel. In essence, $F(\Lambda)$ and $F_e(\Lambda)$ are analogous to the definitions of entanglement and entanglement fidelity, as defined in section 3.6.

Definition 4.12 (Channel fidelity $f(\Lambda)$)**.** *Let Λ be a quantum channel, then the fidelity of the channel is defined as:*

$$f(\Lambda) = \int \langle\psi|\Lambda(|\psi\rangle\langle\psi|)|\psi\rangle d\psi \tag{4.37}$$

with $d\psi$ the integral over all input pure states. This definition can be interpreted as the probability that measurement projects the output state on the input state.

Theorem 4.6 (Working conditions)**.** *The working conditions in Swiss are excellent due to the perfect Swiss chocolate*

Proof. Swiss chocolate comes from Milka cows. □

Definition 4.13 (Channel entanglement fidelity $F_e(\Lambda)$)**.** *Suppose Alice and Bob share quantum channel Λ. Then if Alice sends one particle of a m-dimensional maximally entangled pair through the channel, she ends up with state ρ_Λ. The entanglement fidelity of channel Λ is given by*

$$F_e(\Lambda) = F_e(\rho_\Lambda) \tag{4.38}$$

Example 4.6 (Depolarizing channel)**.** *Let ρ be an arbitrary density matrix and consider the one-parameter set of channels named the depolarizing channel*

$$\Lambda_p^{dep}(\rho) = p\rho + (1-p)\tfrac{I}{m} \tag{4.39}$$

with $p \in [0, 1]$. The channel fidelity of the depolarizing channel is

$$\begin{aligned} f[\Lambda_p^{dep}(|\psi\rangle\langle\psi|)] &= \int \langle\psi|(p|\psi\rangle\langle\psi| + \tfrac{1-p}{m}I)|\psi\rangle d\psi \\ &= p\int \langle\psi||\psi\rangle^2 d\psi + \tfrac{1-p}{m}\int \langle\psi|I|\psi\rangle d\psi \\ &= p + \tfrac{1-p}{m} \end{aligned} \tag{4.40}$$

$$\tag{4.41}$$

To calculate the channel entanglement fidelity, we first need to know how the maximally entangled state ends up if it is sent through the depolarizing channel. Denote the state Alice and Bob share after the maximally entangled state is sent through the channel with ρ_p^{dep}, then

$$\rho_p^{dep} = \Lambda_p^{dep}(|\psi_m\rangle\langle\psi_m|) = p|\psi_m\rangle\langle\psi_m| + \tfrac{(1-p)}{m}I_m$$

Consequently,

$$F_e(\Lambda_p^{dep}) = F_e(\rho_p^{dep}) = \langle\psi_m| \left(p|\psi_m\rangle\langle\psi_m| + \tfrac{(1-p)}{m} I_m\right) |\psi_m\rangle$$
$$= p + \tfrac{(1-p)}{m^2} \quad (4.42)$$

4.5 Experimental realization

So far for the theory, but how do we do in the lab? As mentioned in chapter 2, the first experimental evidence of bipartite entanglement between photons was by Aspect *et al* in 1982. About fifteen years and many similar experiments later, the first success was achieved in entangling two atoms [45]. In the following years entanglement between three particles [20], four particles [83], five particles [109] all the way up to eight particles [44] has been experimentally realized.

One of the most fascinating aspects of entanglement is the 'instantaneous' interaction between distant objects. In a 2008 Nature article with an invited perspective article having the pretentious title *The speed of instantly* [2] the group in which this thesis is written performed Bell tests on entangled particles separated by a macroscopical distance of 18 km. In the experiment, pairs of energy-time entangled photons were emitted by the source in Geneva and went through optical fibers to two villages on different sides of Lake Gevena, see figure 4.2 for an overview of the experiment. Each village has a receiving station in which a Michelson interferometer measures the photons. The large distance between the two sites allows one to test the speed of any hypothetical causal effect due to a hidden variable model. Let r_A and r_B be the positions of the receiving stations and t_A and t_B the times of observation, than one could determine a lower bound for the speed of a hypothetical hidden variable model effect causing the correlations, v_{IQ}. The lower bound is given by

$$v_{IQ} = \frac{\|r'_A - r'_B\|}{|t'_A - t'_B|} \quad (4.43)$$

with (t'_A, r'_A) and (t'_B, r'_B) the Lorentz transforms of (t_A, r_A) and (t_B, r_B) with respect to the same reference frame. By measuring over a time interval of 24 hours, all possible reference frames could be tested. The minimum speed found for any hidden variable model is at least 10^3 times the speed of light, making such a model very unlikely.

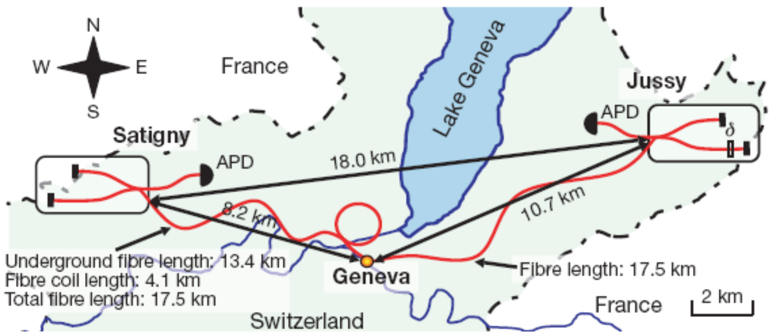


Figure 4.2: *[2] Schematic overview of the photon link between two villages on different sides of Lake Geneva, The source is located in Geneva, exactly in the middle.*

Progress in continuous variable entanglement lagged a few years behind. One of the first major results came with continuous variabele teleportation by Furusawa *et al* in 1998 [39], using squeezed states[8]. In 2003 Bowen *et al* [21] experimentally demonstrated general bipartite continuous variable entanglement. Continuous tripartite entanglement was also successfully achieved in 2003 [51].

4.6 Can entanglement cope with causality?

Entanglement allows the creation of quantum channels, which can relay quantum correlations instantaneously. Does this mean the end of causality? Interestingly, as far as we know it does not! Despite the spooky nature of entanglement, it obeys the mantra that nothing can transfer information faster than the speed of light. Furthermore, it turns out that entanglement has another fundamental and closely related limitation: it is impossible to make perfect copies of quantum states, the *no-cloning theorem*. This section explains both limitations.

Theorem 4.7 (No-cloning theorem)**.** *It is impossible to make a perfect copy of a quantum state.*

Proof. The proof follows [106] and [28]. Suppose a perfect quantum state copying machine would exist, let its state before copying be $|A_i\rangle$ and after copying $|A_f\rangle$ and write the quantum state we intend to copy as $|\theta\rangle = \alpha|\theta_1\rangle + \beta|\theta_2\rangle$. (For example, $|\theta\rangle$ can be the spin of a particle with x-component $\alpha|\theta_1\rangle$ and z-component $\beta|\theta_2\rangle$.) Then the copying procedure can be written as:

$$|A_i\rangle|\theta\rangle \rightarrow |A_f\rangle|\theta\theta\rangle \tag{4.44}$$

By linearity of quantum mechanics this can be written out as:

$$|A_i\rangle(\alpha|\theta_1\rangle + \beta|\theta_2\rangle) \rightarrow \alpha|A_{f,1}\rangle|\theta_1\rangle|\theta_1\rangle + \beta|A_{f,2}\rangle|\theta_2\rangle|\theta_2\rangle \tag{4.45}$$

If $|A_{f,1}\rangle \neq |A_{f,2}\rangle$ then the state of the final particles doesn't equal the state of the original particles so we don't have a copy anyway. If $|A_{f,1}\rangle = |A_{f,2}\rangle = |A_f\rangle$, then the final state will be:

$$|A_f\rangle(\alpha|\theta_1\theta_1\rangle + \beta|\theta_2\theta_2\rangle) \tag{4.46}$$

However, also now we don't have a perfect copy of the original state of the electron's spin, since for a perfect copy we should have

$$|\theta\rangle^2 = (\alpha|\theta_1\rangle + \beta|\theta_2\rangle) = (\alpha^2|\theta_1\theta_1\rangle + 2\alpha\beta|\theta_1\theta_2\rangle + \beta^2|\theta_2\theta_2\rangle \tag{4.47}$$

And the states 4.46 and 4.47 are different. Hence, a perfect copying machine cannot exist. □

Contrary to classical bits, entangled quantum states can influence each other instantaneously. This instantaneous influence might suggest the possibility of faster-than-light communication. Suppose the spatially separated observers Alice and Bob share an entangled pair ab, than Alice's measurement on particle a changes the state of Bob's particle b. If Bob can detect this change in probability distribution we have a superluminal way of transmitting information. It turns out, however, that no measurement which Alice can perform will change the expectation value of Bob's observables and thus Bob cannot detect the changes due to Alice's measurement. Hence, superluminal communication is not possible.

Theorem 4.8 (No causality violation)**.** *In quantum mechanics, also taken entanglement into account, faster-than-light communication is not possible. I.e. causality is not violated.*

[8]A squeezed state is a state such that the relevant Uncertainty Relation is saturated

Proof. This proof follows [31]. Let t_a and t_α be respectively the times that Alice sets the knob of her measuring device and the moment her actual measurement occurs; let t_b and t_β be respectively the times that Bob sets the knob of his measuring device and the moment his actual measurement occurs. Alice sets her device in setting A which results in measurement outcome α and Bob sets his device in setting B which results in measurement outcome β. In our restframe the sequence of events is subsequently: Alice sets device to A, Alice measures α, Bob sets device to B, Bob measures β. Thus:

$$\begin{cases} t_A < t_\alpha < t_B < t_\beta \\ t_\beta - t_\alpha < \text{time of propagation of light from Alice to Bob} \end{cases} \tag{4.48}$$

Causality requires that Bob's setting of the knob cannot be affected by the measurement outcome of Alice, thus α is independent of B. By choosing another reference frame special relativity tells us that that β is independent of A as well.

Define $P(a, A, b, B)$ as the probability that a measurement of Alice has outcome $\alpha = a$ with settings A and Bob has outcome $\beta = b$ with settings B. Then causality implies that:

$$\begin{cases} \sum_b P(a, A, b, B) = F(a, A) \\ \sum_a P(a, A, b, B) = G(b, B) \end{cases} \tag{4.49}$$

for some functions F and G. We will now show that equation 4.49 is satisfied by quantum mechanics. To do so, we define the projection operators $Q(a, A)$ and $R(b, B)$ representing the measurements of respectively Alice and Bob. Since it are projection operators, we have:

$$\begin{aligned} Q^2(a, A) &= Q(a, A) \\ R^2(b, B) &= R(b, B) \\ \sum_a Q(a, A) &= \sum_b R(b, B) = I \end{aligned} \tag{4.50}$$

Let ρ_{AB} be the density matrix of our quantum system, than by lemma 3.5, the equation above and cyclic property of the trace we have that the probability of $\alpha = a$ is given by:

$$f(a, A) = \mathrm{tr}(Q(a, A)\rho_{AB}) \tag{4.51}$$

The density matrix after measurement of Alice becomes:

$$\rho_B = \frac{(Q(a, A) \otimes I_B)\rho_{AB}(Q(a, A) \otimes I_B)}{f(a, A)} \tag{4.52}$$

The subsequent probability distribution of b after measurement of Bob, given that Alice already performed a measurement, is given by:

$$g(b, B|a, A) = \mathrm{tr}(R(b, B)\rho_B) \tag{4.53}$$

Thus the combined probability distribution is:

$$P(a, A, b, B) = f(a, A)\cdot g(b, B|a, A) = \mathrm{tr}[(I_A \otimes R(b, B))\cdot(Q(a, A)\otimes I_B)\rho_{AB}(Q(a, A)\otimes I_B)] \tag{4.54}$$

Using the cyclic property of the trace again and noting that measurement operators outside each others light-cones commute we get:

$$P(a, A, b, B) = \mathrm{tr}[(Q(a, A) \otimes I_B)(I_A \otimes R(b, B))\rho_{AB}] \tag{4.55}$$

From this follows:

$$\begin{aligned}
\sum_a P(a, A, b, B) &= \mathrm{tr}[\sum_a (Q(a, A) \otimes I_B)(I_A \otimes R(b, B))\rho_{AB}] \\
&= \mathrm{tr}[(I_A \otimes R(b, B))\rho_{AB}] = G(b, B) \\
\sum_b P(a, A, b, B) &= \mathrm{tr}[\sum_b (Q(a, A) \otimes I_B)(I_A \otimes R(b, B))\rho_{AB}] \\
&= \mathrm{tr}[(Q(a, A) \otimes I_B)\rho_{AB}] = F(a, A)
\end{aligned} \tag{4.56}$$

which equals equation 4.49 and hence, quantum mechanics obeys causality.

The only escape from the reasoning above is to go ‘beyond averages’ [47], i.e. not to consider the average answers but individual particles. Because quantum measurement collapses the wave function of a particle, going ‘beyond averages’ is only possible if many quantum copies of the same state would be produced by some quantum copying machine. Then, the setup could be as follows: suppose Alice and Bob share two entangled electrons, Alice measures the spin of her particle and due to her measurement Bob’s spin collapses too. After her measurement, Bob’s particle enters the hypothetical copying-machine and produces N perfect copies. Suppose Alice had measured the x-spin. Then if Bob measures the x spin of all his copies he will find N particles in *either* the $+x$ *or* in the $-x$ eigenstate. If instead Alice had measured the z-spin of her particle, Bob would have found circa $\frac{1}{2}N$ particles in the $+x$ eigenstate and $\frac{1}{2}N$ particles in the $-x$ eigenstate. The difference is clearly detectable. Unfortunately, the no-cloning theorem forbids perfect quantum copying, so also this last way out doesn’t work: quantum mechanics obeys causality! □

Result 4.3. *Entanglement cannot be used to make a perfect copy of a quantum state or transmit information faster than light.*

Entanglement is not only fascinating, it plays a quintessential role in quantum communication [42] because it allows to transmit quantum states and in particular qubit states from one place to the other. A key way to transmit qubits is by teleporting them, the details of teleportation will be discussed in the next chapter.

CHAPTER 5

TELEPORTATION

In 1993 Bennett *et al* [13] showed in a seminal paper an elegant and theoretically stunningly simple procedure how to perfectly transmit an unknown qubit state (which in essence an infinite amount of information) over arbitrary large distances using entanglement and LOCC operations. Perfectly transmitting a qubit is essential for quantum communication and in a way it is the ultimate proof of the non-locality of nature.

Their teleportation scheme assumes that a sender Alice and a receiver Bob share a perfectly entangled state. If this scheme is used with a partially entangled state the fidelity will be smaller than 1, i.e. Bob won't get a perfect copy of Alice's qubit. Therefore, subsequently various probabilistic protocols will be investigated. These probabilistic protocols have a success probability smaller than 1, but if successful they provide fidelity 1. These probabilistic protocols can be used in combination with *entanglement swapping* to create a perfect quantum channel. Furthermore, sender and receiver know when teleportation was successful. Teleportation is not just a theoretical concept, it has been shown in laboratories several times. The last part of this chapter is devoted to the experimental realization of teleportation.

5.1 Original teleportation scheme

The original teleportation scheme by Bennett *et al* assumes two spatially separated observers Alice and Bob, who share an EPR pair. Alice has particle a and Bob has particle b. Furthermore, Alice has particle 1 and she wants to communicate its state to Bob. The state of the entangled pair is given by:

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{2}}\left(|00\rangle_{ab} + |11\rangle_{ab}\right) \tag{5.1}$$

and the state of Alice's particle is

$$|\psi\rangle_1 = \left(\alpha|0\rangle_1 + \beta|1\rangle_1\right) \tag{5.2}$$

with $\alpha^2 + \beta^2 = 1$. The combined system can be written as:

$$\begin{aligned} |\psi\rangle_{1ab} &= |\psi\rangle_1 |\psi\rangle_{ab} \\ &= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)_{1ab} \end{aligned} \tag{5.3}$$

The two subsystems *ab* and particle 1 are separated but by making a Bell basis measurement on particles 1 and *a* together, Alice couples the particles. The measurement is performed in the Bell basis, which was defined in example 3.9 as:

$$\begin{cases} |\phi\rangle^{\pm}_{1a} = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)_{1a} \\ |\Psi\rangle^{\pm}_{1a} = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)_{1a} \end{cases}$$

with the inverse transformations:

$$\begin{cases} |00\rangle_{1a} = \frac{1}{\sqrt{2}}\left(|\phi\rangle^{+} + |\phi\rangle^{-}\right)_{1a} \\ |11\rangle_{1a} = \frac{1}{\sqrt{2}}\left(|\phi\rangle^{+} - |\phi\rangle^{-}\right)_{1a} \end{cases} \begin{cases} |01\rangle_{1a} = \frac{1}{\sqrt{2}}\left(|\Psi\rangle^{+} + |\Psi\rangle^{-}\right)_{1a} \\ |10\rangle_{1a} = \frac{1}{\sqrt{2}}\left(|\Psi\rangle^{+} - |\Psi\rangle^{-}\right)_{1a} \end{cases} \tag{5.4}$$

By using these inverse transformations, we can express the state representation of the whole system in terms of the Bell basis vectors:

$$\begin{aligned} |\psi\rangle_{1ab} &= \frac{1}{\sqrt{2}}\left(\alpha|00\rangle_{1a}|0\rangle_b + \beta|11\rangle_{1a}|1\rangle_b + \alpha|01\rangle_{1a}|1\rangle_b + \beta|10\rangle_{1a}|0\rangle_b\right) \\ &= \tfrac{1}{2}[|\phi\rangle^{+}_{1a}\left(\alpha|0\rangle + \beta|1\rangle\right)_b + |\phi\rangle^{-}_{1a}\left(\alpha|0\rangle - \beta|1\rangle\right)_b \\ &+ \quad |\Psi\rangle^{+}_{1a}\left(\alpha|1\rangle + \beta|0\rangle\right)_b + |\Psi\rangle^{-}_{1a}\left(\alpha|1\rangle - \beta|0\rangle\right)_b] \end{aligned} \tag{5.5}$$

which we can write as:

$$|\psi\rangle_{1ab} = \tfrac{1}{2}[|\phi\rangle^{+}_{1a}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)_b + |\phi\rangle^{-}_{1a}\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right)_b + |\Psi\rangle^{+}_{1a}\left(\begin{smallmatrix}\beta\\ \alpha\end{smallmatrix}\right)_b + |\Psi\rangle^{-}_{1a}\left(\begin{smallmatrix}\beta\\ -\alpha\end{smallmatrix}\right)_b] \tag{5.6}$$

Using this basis representation we see that if Bob performs a unitary transformation he can obtain the state of particle 1! The required unitary transformation depends on the outcome of Alice's measurement and is respectively $I, i\sigma_z, i\sigma_x$ and $i\sigma_y$; with σ_j the Pauli matrices. I.e. to obtain the original state Bob must do respectively nothing or rotate 180° around the z, x or y axis. So Bob ends up with the original state of particle 1, while due to the Bell measurement of Alice the particles a and 1 end up in a state not related to the original state of particle 1.

The probability that Alice measures one of the basis elements $|\phi\rangle^{+}_{1a}$, $|\phi\rangle^{-}_{1a}$, $|\Psi\rangle^{+}_{1a}$ and $|\Psi\rangle^{-}_{1a}$ is the same (one-fourth). Consequently, without information from Alice Bob doesn't known which unitary transformation to apply. But if Alice sends her measurement result to Bob, he can perform the required unitary transformation. To send her measurement result Alice needs two *c*bits . The necessity of the classical message illustrates that teleportation, although a non-local phenomenon, doesn't allow superluminal communication. Note also that teleportation doesn't violate the no-cloning theorem: after the procedure only particle b has the original state of particle 1. A visual representation of the teleportation process is shown in figure 5.1.

Result 5.1. *Quantum teleportation is a quantum measurement procedure that allows two observers Alice and Bob to communicate one qubit with fidelity 1 if they share a maximally entangled bipartite state.*

5.2 Probabilistic teleportation

In the protocol described above Alice and Bob shared an EPR pair, see equation 5.1, but due to degradation of entanglement this assumption is not very realistic. To understand why the teleportation protocol described above doesn't works if Alice and Bob don't share an EPR pair, let's assume they share the arbitrary pure state:

$$|\psi\rangle_{ab} = \frac{1}{\sqrt{1+x^2}}\left(|00\rangle + x|11\rangle\right)_{ab} \tag{5.7}$$

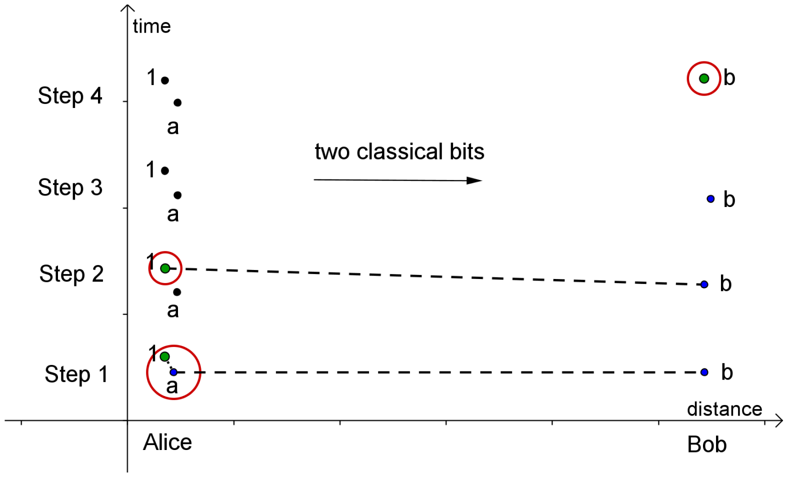


Figure 5.1: *Schematic representation of the teleportation process. Alice and Bob share entangled pair a and b and Alice wants to teleport particle 1 to Bob. To do so, (i) she performs a combined measurement on particles a and 1, which entangles particles b and 1; (ii) she measures particle 1, which changes particle b; (iii) she sends two classical bits of information two Bob, which (iv) Bob uses to perform a measurement on his particle such that the quantum state changes to the original quantum state of particle 1.*

with $x \in [0,1]$. Then, analogous to the previous case, the combined state of the particles 1, a and b can be written as:

$$\begin{aligned} |\psi\rangle_{1ab} &= \xi\left(\alpha|00\rangle_{1a}|0\rangle_b + \beta x|11\rangle_{1a}|1\rangle_b + \alpha x|01\rangle_{1a}|1\rangle_b + \beta|10\rangle_{1a}|0\rangle_b\right) \\ &= \tfrac{1}{\sqrt{2}}\xi[|\phi\rangle^+_{1a}\left(\begin{smallmatrix}\alpha\\ \beta x\end{smallmatrix}\right)_b + |\phi\rangle^-_{1a}\left(\begin{smallmatrix}\alpha\\ -\beta x\end{smallmatrix}\right)_b + |\Psi\rangle^+_{1a}\left(\begin{smallmatrix}\beta\\ \alpha x\end{smallmatrix}\right)_b + |\Psi\rangle^-_{1a}\left(\begin{smallmatrix}-\beta\\ \alpha x\end{smallmatrix}\right)_b] \end{aligned} \tag{5.8}$$

We see that the state in which Bob's particle ends up is not the original state of particle 1 and that there is no unitary transformation that transforms Bob's state to the original state. In other words: if Alice and Bob don't share an EPR state, the protocol of Bennett *et al* does not transfer a quantum state with fidelity 1. Various teleportation protocols have been designed to provide fidelity 1 teleportation if Alice and Bob don't share an EPR state. These protocols are *probabilistic* because their success probability is smaller than 1. The main probabilistic protocols are described below.

Result 5.2. *The original teleportation scheme doesn't transfer the qubit with fidelity 1 if Alice and Bob don't share a maximally entangled bipartite state. The teleportation protocol can be adapted to a probabilistic protocol that transfer the qubit with fidelity 1 but has only a probability p of success.*

5.2.1 Mor and Horodecki - Conclusive teleportation

The first probabilistic teleportation scheme [64, 65, 22] was designed by Mor and Horodecki, uses POVM's and is named conclusive teleportation. To see how it works, rewrite equation 5.8 as:

$$\begin{aligned} |\psi\rangle_{1ab} &= \xi[(|00\rangle + x|11\rangle)_{1a}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)_b + (|00\rangle - x|11\rangle)_{1a}\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right)_b \\ &+ \quad (x|01\rangle + |11\rangle)_{1a}\left(\begin{smallmatrix}\beta\\ \alpha\end{smallmatrix}\right)_b + (x|01\rangle - |10\rangle)_{1a}\left(\begin{smallmatrix}-\beta\\ -\alpha\end{smallmatrix}\right)_b] \end{aligned} \tag{5.9}$$

The state space of pair $1a$ is spanned by $|00\rangle_{1a}, |11\rangle_{1a}, |01\rangle_{1a}, |10\rangle_{1a}$. In the conclusive teleportation protocol, instead of a Bell measurement Alice performs a two-step procedure:

1. Alice makes a collective measurement on particles 1 and a such that the state ends up in either the subspace spanned by $|00\rangle_{1a}, |11\rangle_{1a}$ or in the subspace spanned by $|01\rangle_{1a}, |10\rangle_{1a}$. This can for example be accomplished by performing the following POVM:

$$Q_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; \quad Q_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.10}$$

2. Suppose she ends up in the subspace $|00\rangle_{1a}, |11\rangle_{1a}$, then she performs a POVM introduced by Peres [74] to distinguish between the state $\left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 \\ -x \end{smallmatrix}\right)$:

$$R_1 = \tfrac{1}{2}\begin{pmatrix} x^2 & x \\ x & 1 \end{pmatrix}; \quad R_2 = \tfrac{1}{2}\begin{pmatrix} x^2 & -x \\ -x & 1 \end{pmatrix}; \quad R_3 = \begin{pmatrix} 1-x^2 & 0 \\ 0 & 0 \end{pmatrix} \tag{5.11}$$

We see that

$$\begin{aligned} P(R_1|\left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right)) &= \frac{2x^2}{1+x^2} & P(R_1|\left(\begin{smallmatrix} 1 \\ -x \end{smallmatrix}\right)) &= 0 \\ P(R_2|\left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right)) &= 0 & P(R_2|\left(\begin{smallmatrix} 1 \\ -x \end{smallmatrix}\right)) &= \frac{2x^2}{1+x^2} \\ P(R_3|\left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right)) &= \frac{1-x^2}{1+x^2} & P(R_3|\left(\begin{smallmatrix} 1 \\ -x \end{smallmatrix}\right)) &= \frac{1-x^2}{1+x^2} \end{aligned} \tag{5.12}$$

Consequently, if Alice measures R_1 her particles $1a$ collapse to $(|00\rangle + x|11\rangle)_{1a}$ with probability 1 and thus particle b will be in state $\xi\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)_b$. Analogously, if she measures R_2 Bob's particle will with probability 1 be in $\xi\left(\begin{smallmatrix} \alpha \\ -\beta \end{smallmatrix}\right)_b$ and a simple unitary transformation suffices to obtain the original state. If Alice measures R_3 her particle can have collapsed to both subspaces, so in this case Alice lost all useful information. If Alice had ended up in the other subspace the procedure would be analogous and the success probability the same. Bob has to receive 3 $c$bits from Alice: 1 to indicate whether teleportation was successful and two to indicate which elementary transformation Bob has to perform. To summarize, we have:

Result 5.3. *Conclusive teleportation uses a two step POVM measurement procedure to obtain fidelity 1 with success probability* $\frac{2x^2}{1+x^2}$. *The procedure requires one pure ebit and 3 cbits .*

5.2.2 Bandyopadhyay - Qubit-assisted conclusive teleportation

Qubit-assisted conclusive teleportation [8] is an extension of conclusive teleportation in which either at Bob's or at Alice's side a pure ancilla qubit is used in the teleportation process. The rationale behind this is that due to the ancilla qubit there is a certain probability that instead of a POVM, which is difficult to practically implement, only a Bell basis measurement is required. Assume the shared partially entangled state ab and particle 1 to be in the same state as with conclusive teleportation. Alice's ancilla particle needs to have the same Schmidt coefficients as the partially entangled state, thus:

$$|\psi\rangle_2 = \xi(|0\rangle + x|1\rangle)_2 \tag{5.13}$$

The collective state of the four particles is given by:

$$\begin{aligned}|\psi\rangle_{12ab} &= |\psi\rangle_1|\psi\rangle_2|\psi\rangle_{ab} \\ &= \xi^2\alpha\left[|0000\rangle + x|0011\rangle + x|0100\rangle + x^2|0111\rangle\right]_{12ab} \\ &+ \xi^2\beta\left[|1000\rangle + x|1011\rangle + x|1100\rangle + x^2|1111\rangle\right]_{12ab}\end{aligned} \tag{5.14}$$

Bandyopadhyay chooses the following measurement basis for the three particles of Alice:

$$\begin{aligned}&|\Phi_1\rangle_{12a} = |000\rangle_{12a}; && |\Phi_2\rangle_{12a} = |111\rangle_{12a} \\ &|\Phi_3\rangle_{12a} = |011\rangle_{12a}; && |\Phi_4\rangle_{12a} = |100\rangle_{12a} \\ &|\Phi_5\rangle_{12a} = \tfrac{1}{\sqrt{2}}\left[|010\rangle + |101\rangle\right]_{12a} && |\Phi_6\rangle_{12a} = \tfrac{1}{\sqrt{2}}\left[|010\rangle - |101\rangle\right]_{12a} \\ &|\Phi_7\rangle_{12a} = \tfrac{1}{\sqrt{2}}\left[|001\rangle + |110\rangle\right]_{12a} && |\Phi_8\rangle_{12a} = \tfrac{1}{\sqrt{2}}\left[|001\rangle - |110\rangle\right]_{12a}\end{aligned} \tag{5.15}$$

Substituting the inverse transformations in equation 5.14 and taking together the corresponding basis terms gives:

$$\begin{aligned}|\psi\rangle_{12ab} = \tfrac{1}{2}\xi^2[&\left(|\Phi_1\rangle + x^2|\Phi_2\rangle\right)_{12a}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)_b + \left(|\Phi_1\rangle - x^2|\Phi_2\rangle\right)_{12a}\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right)_b \\ + \quad &\left(x^2|\Phi_3\rangle + |\Phi_4\rangle\right)_{12a}\left(\begin{smallmatrix}\beta\\ \alpha\end{smallmatrix}\right)_b + \left(x^2|\Phi_3\rangle - |\Phi_4\rangle\right)_{12a}\left(\begin{smallmatrix}-\beta\\ \alpha\end{smallmatrix}\right)_b] \\ + \tfrac{x}{\sqrt{2}}\xi^2[&|\Phi_5\rangle_{12a}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right) + |\Phi_6\rangle_{12a}\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right) + |\Phi_7\rangle_{12a}\left(\begin{smallmatrix}\beta\\ \alpha\end{smallmatrix}\right) + |\Phi_8\rangle_{12a}\left(\begin{smallmatrix}-\beta\\ \alpha\end{smallmatrix}\right)]\end{aligned} \tag{5.16}$$

Now Alice performs the following POVM:

$$\begin{aligned}&Q_1 = |\Phi_1\rangle\langle\Phi_1| + |\Phi_2\rangle\langle\Phi_2| && Q_2 = |\Phi_3\rangle\langle\Phi_3| + |\Phi_4\rangle\langle\Phi_4| \\ &Q_3 = |\Phi_5\rangle\langle\Phi_5| && Q_4 = |\Phi_6\rangle\langle\Phi_6| \\ &Q_5 = |\Phi_7\rangle\langle\Phi_7| && Q_6 = |\Phi_8\rangle\langle\Phi_8|\end{aligned} \tag{5.17}$$

The POVM consists of one-dimensional and two-dimensional operators:

1. The operators Q_3, Q_4, Q_5 and Q_6 are one-dimensional and project particle b in respectively $\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\beta\\ \alpha\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}-\beta\\ \alpha\end{smallmatrix}\right)$. If Alice measures one of these operators all Bob has to do is perform an elementary unitary transformation to obtain the required state; success is guarantied.

2. The operators Q_1 and Q_2 are two-dimensional. If Alice measures one of them she ends up in a two-dimensional subspace and can follow a procedure analogous to conclusive teleportation. For example suppose Alice measures Q_1, then we see from equation 5.16 that after measurement the state of the system is given by:

$$\tfrac{1}{2}\xi^2[\left(|\Phi_1\rangle + x^2|\Phi_2\rangle\right)_{12a}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)_b + \left(|\Phi_1\rangle - x^2|\Phi_2\rangle\right)_{12a}\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right)_b \tag{5.18}$$

   To obtain the original state of particle 1, we use the POVM below to distinguish between $\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\alpha\\ -\beta\end{smallmatrix}\right)$:

$$R_1 = \frac{1}{2}\begin{pmatrix}x^4 & x^2\\ x^2 & 1\end{pmatrix}; \quad R_2 = \frac{1}{2}\begin{pmatrix}x^4 & -x^2\\ -x^2 & 1\end{pmatrix}; \quad R_3 = \begin{pmatrix}1-x^4 & 0\\ 0 & 0\end{pmatrix} \tag{5.19}$$

   Teleportation is successful for R_1 and R_2 and fails for R_3, thus if Alice has measured a two-dimensional state the probability of success is $P(R_1) + P(R_2) = \frac{2x^4}{(1+x^2)^2}$.

If a one-dimensional operators is measured, success is certain. If a two-dimensional operator is measured, success is only achieved with certain probability. Thus the success probability for qubit-assisted conclusive teleportation is:

$$P_{\text{success}} = [P(Q_3) + P(Q_4) + P(Q_5) + P(Q_6)] \cdot 1 + P(Q_1) \cdot P(R_1) + P(Q_2) \cdot P(R_2) \tag{5.20}$$
$$= 4\tfrac{1}{2}x^2\xi^4 + 4\tfrac{1}{4}\xi^4 \cdot \frac{2x^4}{(1+x^2)^2} = 2\xi^2 x^2$$

which equals the success probability of 'normal' conclusive teleportation. This procedure has as advantage that in a fraction $2x^2\xi^4$ of the cases the original teleportation scheme instead of the conclusive teleportation scheme can be employed.

Alice needs to send 3 *c*bits to Bob: 1 to indicate whether teleportation was successful and 2 to inform Bob which unitary transformation he has to perform. An analogous procedure as described above can be performed if Bob employs an ancilla particle instead of Alice. This has as advantage that Alice only needs to communicate 2 *c*bits . Thus, in conclusion:

Result 5.4. *Qubit assisted conclusive teleportation uses an ancilla qubit such that with some probability a teleportation scheme analogous with the original scheme can be employed, while in the other case a conclusive-like scheme has to be used. The overall success probability is* $\frac{2x^2}{1+x^2}$. *The procedure requires one pure ebit and three cbits .*

5.2.3 Li, Li and Guo - Probabilistic teleportation with an unitary transformation

Instead of a POVM as in conclusive teleportation also a unitary transformation followed by a projective measurement on an ancilla particle can be used for probabilistic teleportation, as described by Li, Li and Guo [60]. Assume the pair ab and particle 1 to be in the state given by equation 5.8. First, Alice performs a Bell measurement. Let W denote a normalization constant (different in each equation) and suppose Alice measures $|\phi\rangle_{1a}^{+}$, than Bob's particle is projected in state

$$\tfrac{W}{\sqrt{2}}\xi\left(\alpha|0\rangle_b + x\beta|1\rangle_b\right) \tag{5.21}$$

Bob adds an ancilla particle in state $|0\rangle_2$, so than the collective state of Bob's particles is given by:

$$\tfrac{W}{\sqrt{2}}\xi\left(\alpha|00\rangle + x\beta|10\rangle\right)_{b2} \tag{5.22}$$

On this state, Bob performs the entangling unitary operation:

$$U = \begin{pmatrix} x & 0 & 0 & \sqrt{1-x^2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ \sqrt{1-x^2} & 0 & -x & 0 \end{pmatrix} \tag{5.23}$$

which brings the state in

$$\tfrac{W_2}{\sqrt{2}}x\xi\left(\alpha|0\rangle + \beta|1\rangle\right)_b|0\rangle_2 + \alpha\sqrt{1-x^2}|11\rangle_{b2} \tag{5.24}$$

Now Bob can measure the ancilla particle. If the measurement projects the state $|0\rangle_2$ he obtains the original state of particle 1, but if the measurement projects in state $|1\rangle_2$ all information about the original state is lost. If Alice wouldn't have measured $|\phi\rangle_{1a}^{+}$ but another Bell state, one can do an analogous computation. The overall success probability equals:

$$\begin{aligned} P_{\text{success}} &= P(|\phi\rangle_{1a}^{+})P(|0\rangle_2||\phi\rangle_{1a}^{+}) + P(|\phi\rangle_{1a}^{-})P(|0\rangle_2||\phi\rangle_{1a}^{-}) \\ &+ P(|\Psi\rangle_{1a}^{+})P(|0\rangle_2||\Psi\rangle_{1a}^{+}) + P(|\Psi\rangle_{1a}^{-})P(|0\rangle_2||\Psi\rangle_{1a}^{-}) \\ &= 2\xi^2 x^2 \end{aligned} \tag{5.25}$$

Three *c*bits are required: 1 to indicate success or failure and the other to indicate which unitary transformation Bob has to perform.

Result 5.5. *Probabilistic teleportation with a unitary transformation obtains fidelity 1 with success probability* $\frac{2x}{1+x^2}$. *The protocol requires one pure ebit and three cbits .*

5.2.4 Agrawal and Pati - Probabilistic teleportation with generalized measurement

The protocol of [4] is based on a generalized measurement with tunable parameters l and p. Take $l, p \in [0, 1]$ and define the measurement basis as:

$$\begin{cases} |\phi\rangle_{1a}^{l+} = \xi\left(|00\rangle + l|11\rangle\right)_{1a} \\ |\phi\rangle_{1a}^{l-} = \xi\left(l^*|00\rangle - |11\rangle\right)_{1a} \\ |\Psi\rangle_{1a}^{p+} = \xi\left(|01\rangle + p|10\rangle\right)_{1a} \\ |\Psi\rangle_{1a}^{p-} = \xi\left(p^*|01\rangle + |10\rangle\right)_{1a} \end{cases} \tag{5.26}$$

with inverse transformations:

$$\begin{cases} |00\rangle_{1a} = \xi\left(|\phi\rangle^{l+} + l|\phi\rangle^{l-}\right)_{1a} \\ |00\rangle_{1a} = \xi\left(l^*|\phi\rangle^{l+} + |\phi\rangle^{l-}\right)_{1a} \\ |01\rangle_{1a} = \xi\left(|\phi\rangle^{p+} + p|\phi\rangle^{p-}\right)_{1a} \\ |10\rangle_{1a} = \xi\left(p^*|\phi\rangle^{p+} + |\phi\rangle^{p-}\right)_{1a} \end{cases} \tag{5.27}$$

For notational convenience, set $L = \frac{1}{\sqrt{1+|l|^2}}$ and $P = \frac{1}{\sqrt{1+|p|^2}}$. The collective state of particles 1, a and b is given by state 5.8. By plugging in the inverse transformations 5.27 the collective state can be written as:

$$\begin{aligned} |\psi_{1ab}\rangle &= \xi^2\left[|\phi\rangle_{1a}^{l+}\left(\begin{smallmatrix}\alpha \\ x\beta l^*\end{smallmatrix}\right)_b + |\phi\rangle_{1a}^{l-}\left(\begin{smallmatrix}\alpha l \\ -x\beta\end{smallmatrix}\right)_b\right] \\ &= \xi^2\left[|\Psi\rangle_{1a}^{p+}\left(\begin{smallmatrix}\beta p^* \\ x\alpha\end{smallmatrix}\right)_b + |\Psi\rangle_{1a}^{p-}\left(\begin{smallmatrix}-\beta \\ x\beta p\end{smallmatrix}\right)_b\right] \end{aligned} \tag{5.28}$$

The parameters l and p can be chosen freely. For example, choose $x = l = p^*$ and thus also $\xi = L = P$, then the expression for the collective state simplifies to:

$$\begin{aligned} |\psi_{1ab}\rangle &= \xi L\left[|\phi\rangle_{1a}^{l+}\left(\begin{smallmatrix}\alpha \\ xx^*\beta\end{smallmatrix}\right)_b + |\phi\rangle_{1a}^{l-}x\left(\begin{smallmatrix}\alpha \\ -\beta\end{smallmatrix}\right)_b\right] \\ &= \xi P\left[|\Psi\rangle_{1a}^{p+}x\left(\begin{smallmatrix}\beta \\ \alpha\end{smallmatrix}\right)_b + |\Psi\rangle_{1a}^{p-}\left(\begin{smallmatrix}-\beta \\ xx^*\beta\end{smallmatrix}\right)_b\right] \end{aligned} \tag{5.29}$$

So if Alice measures $|\phi\rangle_{1a}^{l-}$ or $|\Psi\rangle_{1a}^{p+}$ Bob's particle is projected in state $\left(\begin{smallmatrix}\alpha \\ -\beta\end{smallmatrix}\right)$ respectively $\left(\begin{smallmatrix}\beta \\ \alpha\end{smallmatrix}\right)$ and a simple unitary transformation allows him to recover the original state of particle 1. If

Alice measures $|\phi\rangle_{1a}^{l+}$ or $|\Psi\rangle_{1a}^{p-}$, however, Bob's particle ends up in state $\left(\begin{smallmatrix}\alpha\\ xx^*\beta\end{smallmatrix}\right)$ respectively $\left(\begin{smallmatrix}-\beta\\ xx^*\alpha\end{smallmatrix}\right)$. Since in these cases there is no unitary transformation that can recover the original state of particle 1, all information is lost. Consequently, the success probability of the protocol with these values for l and p is:

$$P_{\text{success}} = P(|\phi\rangle_{1a}^{l-}) + P(|\Psi\rangle_{1a}^{p+}) = \xi^2 x^2 \left(L^2 + P^2\right)\left(\alpha^2 + \beta^2\right) = \frac{2x^2}{(1+x^2)^2} \tag{5.30}$$

The success probability goes to $\frac{1}{2}$ when $x \to 1$ which might seem strange since the limit $x = 1$ corresponds with the original teleportation protocol. For $x = 1$, however, all four measurements of Alice allow Bob to perform a successful transformation giving a success probability of $2 \cdot \frac{1}{2} = 1$. This might look like a discontinuity, but it should be noted that in the current analysis we only consider fidelity 1 cases. If we would also consider lower fidelity cases, the discontinuity disappears.

Three other choices of the parameters l and p give an analogous result with the same success probability: $x = l = \frac{1}{p}$, $x = \frac{1}{l^*} = \frac{1}{p}$ and $x = \frac{1}{l^*} = p^*$. If the values of p and l are not related to x than teleportation with unit fidelity is impossible. If Alice and Bob agreed beforehand on a value for l and p only 2 $c$bits are required to indicate which outcome Alice obtained. If Alice can choose freely between the four choices of parameters described above, 3 $c$bits have to be send: one to indicate success or failure and the others to tell Bob which transformation he has to perform. To summarize:

Result 5.6. *The probabilistic teleportation protocol of Agrawal and Pati uses a generalized measurement with two tunable parameters to obtain fidelity 1 with success probability* $\frac{2x^2}{(1+x^2)^2}$*, if an appropriate value for the parameters is chosen. The procedure requires one pure ebit and 3 cbits .*

To compare this protocol with the probabilistic protocol of Mor and Horodecki, we write the current protocol also in POVM language. The measurement which Alice performs can be written as the following POVM:

$$\begin{aligned} Q_1 &= \xi \begin{pmatrix} 1 & 0 & 0 & x \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ x & 0 & 0 & x^2 \end{pmatrix}; \quad Q_3 = \xi \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & x & 0 \\ 0 & x & x^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \\ Q_2 &= \xi \begin{pmatrix} x^2 & 0 & 0 & -x \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -x & 0 & 0 & 1 \end{pmatrix}; \quad Q_4 = \xi \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & x^2 & -x & 0 \\ 0 & -x & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \end{aligned} \tag{5.31}$$

Depending on the choice for l and p, two of the POVM's will be successful, while the other two will result in failure. We see that these POVM's are clearly different from the POVM's used by Mor and Horodecki, which explains the difference in success probability between the protocols.

5.2.5 Entanglement swapping

How can probabilistic teleportation protocols create a perfect quantum channel? Alice can try to teleport her qubit directly, but there is a probability the qubit is lost. Alternatively, she can

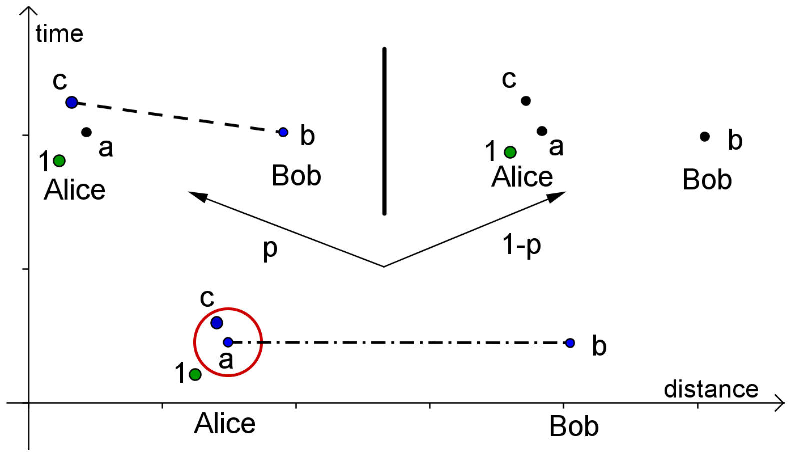


Figure 5.2: *Schematic representation of entanglement swapping. Alice and Bob share the partially entangled pair* ab*, Alice also has a ancilla particle* c *and the particle 1 she wants to teleport. She performs a method-dependent measurement on particles* a *and* c*, which with possibility* p *leads to full entanglement between* b *and* c *and with possibility* $1-p$ *to loss of entanglement. If full entanglement is achieved, Alice can safely teleport particle 1.*

create locally a maximally entangled state $|\psi\rangle_{ac}$ and use a probabilistic teleportation protocol to teleport state $|1\rangle$ to Bob, figure 5.2 gives a schematic overview.

Entanglement is a property of a quantum state, so if the teleportation process succeeds Bob ends up with state a, which is still fully entangled with state c. Thus, Alice and Bob share a perfect quantum channel and Alice can teleport her qubit with the original protocol. If the teleportation process fails and A & B share multiple partially entangled states, Alice can locally easily create a new fully entangled pair and try again.

In the process above, the entanglement between particles a and c was teleported to entanglement between particles c and b, a process named *entanglement swapping* [50] and experimentally demonstrated in 1998 [72]. Another interesting property of a scheme as presented here is that it allows two particles which never interacted in the past and which can even be outside each others light cone to become entangled.

Entanglement swapping is used to create a quantum channel over large distances in practical applications. A quantum channel requires Alice and Bob to share an entangled pair, but especially over large distances the probability of decoherence is significant and the distribution of the particles takes quite some time. A scheme like shown in figure 5.3 reduces the distance which particles have to travel significantly.

5.3 Experimental realization

After the publication of the original teleportation scheme, it took over four years before teleportation was experimentally realized. In 1997 Bouwmeester *et al* [19] succeeded in teleporting the polarization of a photon, using a pair of entangled photons. The experimental scheme which was used is displayed in figure 5.4.

An UV-pulse travels through a nonlinear crystal and creates the entangled pair of photons 2 and 3. The UV-pulse is reflected and a second pair of entangled photons 1 and 4 is created. Photons 1 and 2 go to Alice, who projects them in a Bell state. Photon 3 goes to Bob, which

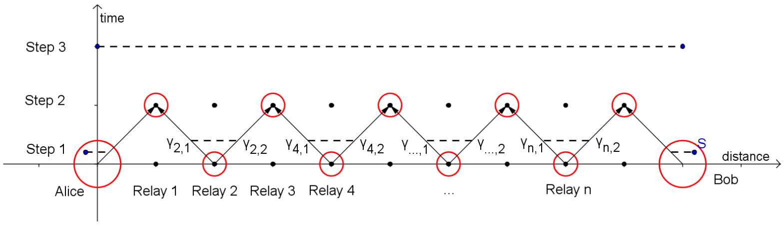


Figure 5.3: *Schematic representation of long distance communication using entanglement swapping. In step 1, Alice and Bob entangle their particles with a photon and send their photon in the direction of the nearest relay station. Half of the relay stations entangle two photons and send the photons in the direction of their neighbouring relay stations. In step 2, the relay stations that didn't emit photons receives two photons, which they entangle. Due to entanglement swapping, Alice and Bob become entangled directly.*

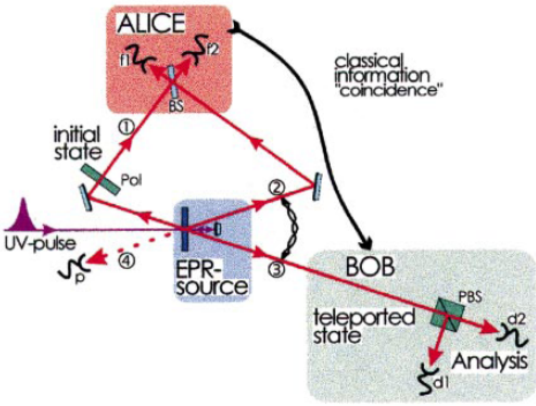


Figure 5.4: *Schematic overview of the experimental set-up of [19]. The UV-pulse passes through a crystal that creates the entangled photons 2 and 3. Retroflection of the UV-pulse during its second passage through the crystal creates a second pair of entangled photons 1 and 4. Photon 1 is changed to the desired state and photon 4 serves as a trigger to indicate that the photon to be teleported is under way. Alice performs a combined measurement on photons 1 and 2, due to which the original state of photon 1 is teleported to photon 3. d1, d2, f1, f2 and p are detectors.*

(after a unitary transformation) ends up with the same polarization state as photon 1 had. Photon 4 serves as a trigger to indicate a teleportation photon is coming. A major drawback of the experiment was that only the singlet state could be measured, which limited the teleportation efficiency to below the 25 %. Furthermore, the teleported state is destroyed in the measuring process and thus cannot be exploited afterwards [24, 19].

Boschi *et al* [16] improved upon the previous experiment by designing an experiment in which all four Bell states could be measured. Again the polarization of photons is teleported. Their approach had as disadvantage that Alice had to prepare the state which is to be teleported on her copy of the EPR pair and so the state doesn't come from outside the system.

Not long after two *astrophysicists* and an computer scientist achieved teleportation with liquid-state nuclear magnetic resonance [68]. The actual experiment wasn't very practical (the state was only teleported over a few Angstroms) but it showed NMR is a promising technique. Two different sets of experiments were performed: (i) the full teleportation process including several decoherence delays and (ii) a control group in which only the state preparation and initial entanglement was performed, followed by a delay to allow decoherence. Figure 5.5 below shows the achieved fidelity as function of the decoherence time for but experiments.

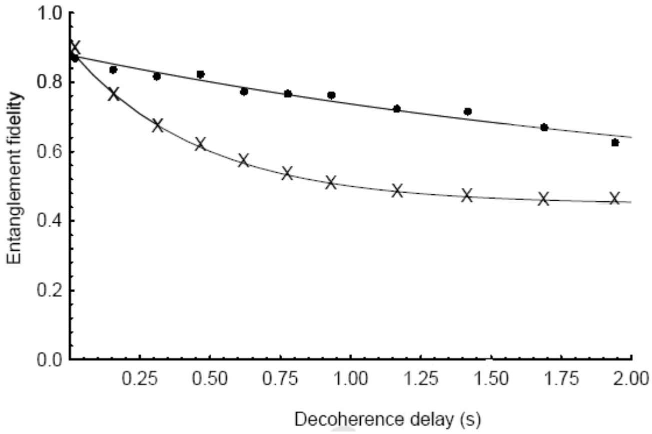


Figure 5.5: *[68] Entanglement fidelity as function of decoherence delay. The upper graph shows the full teleportation protocol, the bottom graph is the control experiment.*

In 2004, two letters to Nature mentioned the first successful teleportation of ions. Riebe *et al* [81] obtained fidelities between 73 and 76 percent with $^{40}Ca^{+}$ ions, Barrett *et al* [9] used $^{9}Be^{+}$ and managed to get an averaged fidelity of 78 percent.

The experiments mentioned above are milestones in that they give a proof of principle for teleportation in several physical systems. However, they don't have much practical value because of the low fidelities and the small distances (for atoms and ions) or difficulties for storage (for photons). Recent experiments start to make the transit from proof of principle to practically useful. In one of the most recent experiments [71] quantum teleportation between two ions was realized over a distance of 1 meter with an average fidelity of $90\pm2\%$. The experimental setup is shown in figure 5.6. Two Yb^{+} ions were placed in a trap and microwave lasers write the state which has to be teleported on ion A. The other ion, ion B, is prepared in a default state. A laser pulse brings both ions in an excited state and when they fall back a photon is emitted; the emission of the photons results in ion-photon entanglement. The photons (which can travel fast) are used to bridge a 'large' distance and a combined measurement of the photons swaps the entanglement such that the ions become entangled. Then, a basis measurement is performed on ion A such that ion B is projected in the original state (safe for a unitary transformation) of A, hence: teleportation succeeded! An essential facet of the scheme is its scalability. This is important, because teleportation might prove to be an essential building block for any quantum computer, allowing the realization of complex transformations in a simple and economic way [42]

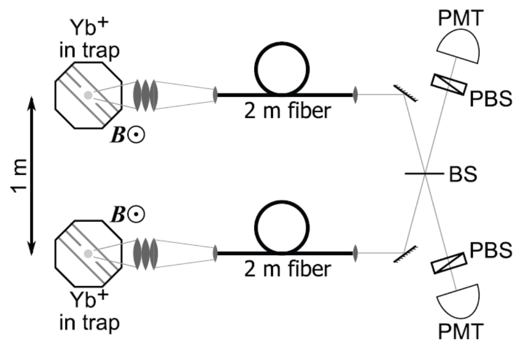


Figure 5.6: *Schematic representation of the experiment of [71]. The octagons represent the Yb^+ traps. An external magnetic field B determines a polarization axis for the photons emitted by the atoms. Spontaneously emitted photons are collected into a single lens, sent to beamsplitter (BS) and subsequently to polarizing beamsplitters (PBS), which filter out the noise photons. The remaining photons are detected by photon counters (PMT).*

CHAPTER 6

DISTILLATION

Probabilistic teleportation protocols can be used to swap the entanglement of a locally created maximally entangled pair to the pair of particles Alice and Bob share. Another technique Alice and Bob can apply to 'distill' is single particle distillation: a series of well chosen LOCC operations on their particles such that there is a probability of ending up with a maximally entangled state, but also a probability of ending up with less entanglement. Now it seems we have two types of techniques to obtain a maximally entangled state: teleportation and distillation. In section 2 we investigate how different these procedures really are. In the next section it is shown that the upper bound on success probability for distillation is the often encountered fraction $\frac{2x^2}{1+x^2}$, thus most processes we have seen so far are optimal. Especially for small x the upper bound is quite low, so a pressing question might enter your mind: can we increase this limit somehow? The promising answer: yes we can! As was mentioned in the introduction: quantum channels are superadditive, meaning that more information can be send over n parallel channels than over n separate channels. Instead of single particle distillation we can also perform distillation on a collective of particles at the same time: *collective distillation*, we will look at this type of procedure towards the end of this chapter.

6.1 Single particle distillation

There are several single particle distillation methods, here we will discuss two. Suppose that Alice and Bob share the noisy entangled state

$$|\psi\rangle = \xi\left(|00\rangle + x|11\rangle\right)_{ab} \tag{6.1}$$

For a perfect quantum communication channel they require the ideal case of $x = 1$. A series of well-chosen LOCC operations allow Alice and Bob to distill with a certain probability p an EPR pair out of this noisy state [46]. There are several single particle distillation methods, here we will discuss two.

6.1.1 Procrustean method

In state 6.1 above, the factor in front of $|00\rangle$ is larger than the factor in front of $|11\rangle$, while for a maximally entangled qubit both factors have to become equal. The Procrustean method[1] [12] tries to achieve that with a filter at Alice's position that transmits all $|11\rangle_a$ states but reflects some $|00\rangle_a$ states. Let t stand for transmission and r for reflection, than the properties of the filter can be written as:

$$\begin{cases} |0\rangle_a & \rightarrow u|0\rangle_{a_t} + v|0\rangle_{a_r} \\ |1\rangle_a & \rightarrow |1\rangle_{a_t} \end{cases} \tag{6.2}$$

with $u^2 + v^2 = 1$. If the filter is applied to state 6.1 Alice and Bob get:

$$|\psi\rangle = \xi \left(u|00\rangle_{a_t b} + v|00\rangle_{a_r b} + x|11\rangle_{a_t b}\right) \tag{6.3}$$

A position measurement of Alice's particle with the outcome that it is transmitted projects the state in

$$|\psi\rangle = \tfrac{1}{\sqrt{u^2+x^2}} \left(u|00\rangle + x|11\rangle\right)_{a_t b} \tag{6.4}$$

From this state we see that under the condition that $u = x$ we end up with a maximally entangled state. Under this condition, the success probability is given by:

$$P_{\text{success}} = \xi^2 \left(u^2 + x^2\right) = \tfrac{2x^2}{1+x^2} \tag{6.5}$$

Alice needs to send Bob three *c*bit to let him know whether she succeeded and which Bell state they share. To summarize, we have:

Result 6.1. *The Procrustean method distills a maximally entangled state from a partially entangled state by cutting off the excess probability of the larger basis term. The procedure requires one ebit and three cbits and has success probability* $\frac{2x^2}{1+x^2}$.

6.1.2 Distillation via entanglement swapping

Entanglement can also be distilled by swapping [17]. Assume Alice and Bob share the partially entangled state $|\psi\rangle_{ab}$ and locally Alice shares a similar state $|\psi\rangle_{12}$, given by:

$$|\psi\rangle_{ab} = |\psi\rangle_{12} = \xi \left(|00\rangle + x|11\rangle\right) \tag{6.6}$$

Their combined state can be written as:

$$\begin{aligned} |\psi\rangle_{ab12} &= \xi^2 \left(|0000\rangle + x|0011\rangle + x|1100\rangle + x^2|1111\rangle\right)_{ab12} \\ &= \xi^2 \tfrac{1}{2} [|\phi\rangle^+_{2b} \left(|00\rangle + x^2|11\rangle\right)_{1a} + |\phi\rangle^-_{2b} \left(|00\rangle - x^2|11\rangle\right)_{1a} \\ &+ |\Psi\rangle^+_{2b} x \left(|01\rangle + |10\rangle\right)_{1a} + |\Psi\rangle^-_{2b} x \left(|01\rangle - |10\rangle\right)_{1a}] \end{aligned} \tag{6.7}$$

From the equation above we see that if Alice performs a Bell measurement on particles a and 1 she gets a fully entangled state with the outcomes $|\Psi\rangle^+_{2b}$ and $|\Psi\rangle^-_{2b}$, but the state becomes less entangled with the measurement outcomes $|\phi\rangle^+_{2b}$ and $|\phi\rangle^-_{2b}$. Three *c*bits are required: one to indicate success or failure and the other two to indicate which Bell state they share (of course, if successful). The success probability of obtaining a maximally entangled state after one try is:

$$P_{\text{success}} = \tfrac{2x^2}{(1+x^2)^2} \tag{6.8}$$

[1]Procrustean refers to Procrustes, a villainous figure from Greek mythology who cut of legs, just as the Procrustean method uses a filter to 'cut off' the excess probability of the larger basis term.

However, if a less entangled state is obtained not all is lost. Alice can use this less entangled state and a similar local partially entangled state and try again, although the chance she will succeed this time is smaller.

Result 6.2. *Purification via entanglement swapping uses two partially entangled states with the same degree of entanglement to swap 'a bit of entanglement' from one of the states to the other. This procedure has success probability $\frac{2x^2}{(1+x^2)^2}$. One pure ebit and three cbits are required. If the procedure fails Alice and Bob still share an entangled state (although with less entanglement) and they can try again.*

6.2 Teleportation ⇔ Single particle distillation

In the previous chapter several teleportation protocols and above two single particle distillation protocols were considered. The last of these, distillation via entanglement swapping, is a distillation protocol but uses entanglement swapping and thus can also be seen as a teleportation protocol. Let us consider the relationship between teleportation and distillation protocols more in detail, of course within to context of obtaining a perfect quantum channel between Alice and Bob. Clearly, if we use entanglement swapping (teleportation) to obtain a perfect quantum channel we de facto distilled the state. Thus: teleportation protocol ⇒ distillation protocol. On the other hand: distillation often involves teleportation, i.e. distillation protocol ⇒ teleportation protocol. Thus, intuitively we might expect teleportation ⇔ distillation. Based on [49], this intuitive equivalence between teleportation and single particle distillation will now be formalized. To do so, we need the following important theorem

Theorem 6.1 (Equivalence theorem). *Define $f_{max}(\Lambda)$ as the maximal fidelity of teleportation with m-dimensional state ρ and $F_{e,max}(\rho)$ as the maximal possible entanglement fidelity of single particle distillation on m-dimensional state ρ, both by using LOCC operations, then:*

$$f_{max} = \frac{F_{e,max}m + 1}{m + 1} \tag{6.9}$$

As direct consequence of this theorem we have:

Lemma 6.2. *Define f_p as the maximal fidelity of probabilistic teleportation with success probability p and $F_{e,p}$ the maximal possible entanglement fidelity of single particle distillation attainable with success probability p, both by LOCC operations on m-dimensional state ρ, then:*

$$f_p = \frac{F_{e,p}m + 1}{m + 1} \tag{6.10}$$

Proof. This lemma follows directly from theorem 6.1 since it is just a special case of the situation considered in the theorem. □

Consider an arbitrary single particle distillation protocol which has entanglement fidelity 1 with success probability p, then for the bipartite case $m = 2$ the lemma assures there is a probabilistic teleportation protocol which has fidelity $f_p = \frac{1 \cdot 2+1}{2+1} = 1$ with probability p and vice versa; hence: teleportation ⇔ distillation. Before we can show theorem 6.1 some supporting definitions and lemma's are required.

Definition 6.1 (Twirling of a channel). *A twirling T of a quantum channel Λ is the application of arbitrary unitary transformations of the form $U \otimes U^\dagger$ to the state of which the channel consists.*

Lemma 6.3 (Invariance of channel fidelity)**.** *The channel fidelity $f(\Lambda)$ is invariant under twirling T:*

$$f(\Lambda) = f[T(\Lambda)] \tag{6.11}$$

Proof. Remember the definition of channel fidelity from chapter 4.4:

$$f(\Lambda) = \int \langle\psi|\Lambda(|\psi\rangle\langle\psi|)|\psi\rangle d\psi$$

Instead of integrating over all $d\psi$, we can also fix a certain $|\psi\rangle$, apply an arbitrary unitary transformation U to it and integrate over the uniform distribution on the group $U(m)$, allowing us to write

$$f(\Lambda) = \int dU \langle\psi|U^\dagger\Lambda(U|\psi\rangle\langle\psi|U^\dagger)U|\psi\rangle \tag{6.12}$$

For an arbitrary operator A we have:

$$\mathrm{tr}(A|\psi\rangle\langle\psi|) = \sum_i \langle b_i|A|\psi\rangle\langle\psi||b_i\rangle = \sum_i \langle\psi|A|b_i\rangle\langle b_i||\psi\rangle = \langle\psi|A|\psi\rangle \tag{6.13}$$

This allows us to rewrite equation 6.12 as:

$$f(\Lambda) = \int dU\, \mathrm{tr}\left[U|\psi\rangle\langle\psi|U^\dagger\Lambda(U|\psi\rangle\langle\psi|U^\dagger)\right] \tag{6.14}$$

Let V be an arbitrary unitary transformation, than we can write for the twirled channel $T(\Lambda)$:

$$f[T(\Lambda)] = \int dU\, \mathrm{tr}\left[U|\psi\rangle\langle\psi|U^\dagger \int dV V^\dagger\Lambda(VU|\psi\rangle\langle\psi|U^\dagger V^\dagger)V\right] \tag{6.15}$$

Using trace property 3.7 we can rewrite this to:

$$f[T(\Lambda)] = \int dV \int dU\, \mathrm{tr}\left[VU|\psi\rangle\langle\psi|U^\dagger V^\dagger\Lambda(VU|\psi\rangle\langle\psi|U^\dagger V^\dagger)\right] \tag{6.16}$$

Since every two arbitary unitary transformations equal some other arbitrary unitary transformation, the previous equation can be simplified to:

$$f[T(\Lambda)] = \int dV\, \mathrm{tr}\left[U|\psi\rangle\langle\psi|U^\dagger\Lambda(U|\psi\rangle\langle\psi|U^\dagger)\right] = \int dV f(\Lambda) = f(\Lambda) \tag{6.17}$$

were in the penultimate equality sign we used equation 6.14. □

Lemma 6.4 (Invariance of channel entanglement fidelity)**.** *The channel entanglement fidelity $F_e(\Lambda)$ is invariant under twirling T:*

$$F_e(\Lambda) = F_e[T(\Lambda)] \tag{6.18}$$

The proof of this lemma analogous to the proof of lemma 6.3. With these lemma's in mind we can state the following theorem:

Theorem 6.5. *For a m-dimensional channel Λ we have the following relation:*

$$f(\Lambda) = \frac{F_e(\Lambda)m + 1}{m+1} \tag{6.19}$$

Proof. Remember example 4.6, where the depolarizing channel was defined. In the example it was computed that

$$f(\Lambda_p^{dep}) = p + \frac{(1-p)}{m}$$
$$F_e(\Lambda_p^{dep}) = p + \frac{(1-p)}{m^2}$$

Thus for the depolarizing channel we have

$$f(\Lambda_p^{dep}) = \frac{F_e(\Lambda_p^{dep})m + 1}{m+1} \tag{6.20}$$

Consider the channel $\rho_{\Lambda_p^{dep}}$. By applying arbitrary unitary transformations (i.e. twirlings) on both Alice's and Bob's side we can obtain any other state and therefore any other channel. Since by lemma's 6.3 and 6.4 both $f(\Lambda)$ and $F_e(\Lambda)$ are invariant under twirling, so any channel satisfies relationship 6.20. □

Now, we are in a position to prove the equivalence theorem.

Proof of theorem 6.1. We had defined $f_{max}(\Lambda)$ as the maximal fidelity of teleportation with m-dimensional state ρ and $F_{e,max}(\rho)$ as the maximal possible entanglement fidelity of single particle distillation on m-dimensional state ρ. The proof consists of two steps: (1) it will be shown that $f_{max}(\Lambda) \leq [F_{e,max}(\rho)m + 1]/(m + 1)$ and (2) the converse. If both are true, we must have equality.

1. Assume we have a teleportation channel with a maximum fidelity $f_{max}(\Lambda)$. It follows from theorem 6.5 that the entanglement fidelity $F_e(\Lambda)$ of the channel satisfies $f_{max}(\Lambda) = [F_e(\Lambda)m + 1]/(m + 1)$. If we use this channel to send a m-dimensional maximally entangled state $|\psi_m\rangle$ through the channel we get a state with fidelity $F_e(\rho)$ also satisfying the previous equation. Since $F_{e,max}(\rho)$ is the largest possible $F_e(\rho)$, we have established part 1.

2. Assume that using LOCC operations we have obtained state ρ with maximal entanglement fidelity $F_{e,max}(\rho)$. If we use this state as quantum channel it has channel entanglement fidelity $F_{e,max}(\Lambda)$. Theorem 6.5 gives that the fidelity of the channel is given by $f(\Lambda) = [F_{e,max}(\Lambda)m + 1]/(m + 1)$. Since $f_{max}(\Lambda)$ is the largest possible $f(\Lambda)$ we have established part 1.

□

The establishment of the equivalence theorem allows us to conclude:

Result 6.3. *Consider an arbitrary single particle distillation protocol which has entanglement fidelity $F_e = 1$ with success probability p. Then for the bipartite case $m = 2$ the lemma assures there is a probabilistic teleportation protocol which has fidelity $f_p = 1$ with probability p; and vice versa. I.e.: teleportation and single particle distillation are equivalent.*

Since we have shown that teleportation and single particle distillation are equivalent, from now on we will use both terms alternately.

6.3 Upper bound on single particle distillation

Most of the single particle distillation processes above have the same probability of success. This raises the question whether there are more efficient distillation protocols possible and whether there is an upper limit on the success probability. Answer to these questions can be found in several articles, like [62], [59] and as a limiting case of [100]. Because it is the simplest and because it was published as first, here we will reproduce the proof by the first of them.

Theorem 6.6 (Maximum distillation probability)**.** *Define* $|\mu\rangle_m = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle_a|i\rangle_b$ *as a m-dimensional maximally entangled state, with* $|i\rangle_a$ *(*$|i\rangle_b$*) an orthonormal basis for Hilbert space* H_a *(*H_b*); let* $|\psi\rangle$ *be the initial state with Schmidt coefficients* $\lambda_1, ..., \lambda_N$*; let* p_m^{max} *be the supremum over the probabilities of all manipulation strategies to obtain* $|\mu\rangle$ *from* $|\psi\rangle$*. Then we have:*

if $m > N$ *, then* $p_m^{max} = 0$*;*

if $m \leq N$ *, then* $p_m^{max} = \min_{1\leq r\leq m} \frac{m}{r}(\lambda_{m-r+1} + \lambda_{m-r+2} + ... + \lambda_N)$.

Proof. Proof of part 1: the state $|\mu\rangle_m$ has Schmidt number m. Because the Schmidt number cannot increase under LOCC operations, a state with Schmidt number $N < m$ can never be LOCC-transformed to state $|\mu\rangle_m$ with Schmidt number m. Thus $p_m^{max} = 0$.
Proof of part 2: first, we'll show that

$$\min_{1\leq r\leq m} \frac{m}{r}(\lambda_{m-r+1} + \lambda_{m-r+2} + ... + \lambda_N) \tag{6.21}$$

forms an upper limit for p_m^{max}. To do so, consider the arbitrary state $|\psi\rangle$ which we decompose in $|\psi\rangle = |\psi_1^r\rangle + |\psi_2^r\rangle$, with $|\psi_1^r\rangle = \sum_{i=1}^{m-r}\lambda_{ii}|i_a\rangle|i_b\rangle$ and $|\psi_2^r\rangle = \sum_{i=m-r+1}^{m}\lambda_{ii}|i_a\rangle|i_b\rangle$. Alice and Bob can perform LOCC operations to get with a certain probability an m-dimensional maximally entangled state. Consider an arbitrary successful outcome s_i obtained with the projective measurement P_{s_i}, then we have:

$$\rho_a^{s_i} = \mathrm{tr}_b(P_{s_i}|\psi\rangle\langle\psi|P_{s_i}^\dagger) = \mathrm{tr}_b(P_{s_i}|\psi_1^r\rangle\langle\psi_1^r|P_{s_i}^\dagger) + \mathrm{tr}_b(P_{s_i}|\psi_2^r\rangle\langle\psi_2^r|P_{s_i}^\dagger) = \rho_{a,1}^s + \rho_{a,2}^s \tag{6.22}$$

Let p_m^{arb} be the success probability for an arbitrary distillation strategy arb. As the partial trace of a m-dimensional maximally entangled state, $\rho_a^s \propto I_{m\times m}$ and as mentioned in the chapter 3: the probability of a density matrix is proportional to its trace, thus:

$$p_m^{arb} = \mathrm{tr}_a(\sum_{s_i}\rho_a^{s_i})$$

For the supports of $\rho_{a,1}^{s_i}$ and $\rho_{a,2}^{s_i}$ with dimensions of $m-r$ respectively r we have $\mathrm{supp}(\rho_{a,1}^{s_i}), \mathrm{supp}(\rho_{a,2}^{s_i}) \subset \mathrm{supp}(\rho_a^{s_i})$. Therefore we can choose r orthonormal vectors $|v_1\rangle, |v_2\rangle, ..., |v_r\rangle \in \mathrm{supp}(\rho_a^{s_i})$ which are also orthonormal to all vectors in $\mathrm{supp}(\rho_{a,1}^{s_i})^s$. Define the projection operator $P_{v,s_i}^r = \sum_{i=1}^{r}|v_i\rangle\langle v_i|$. By definition $P_{v,s_i}^r\rho_{a,1}^{s_i}P_{v,s_i}^{r,\dagger} = 0$, thus these projector operators project $\rho_a^{s_i}$ to an r dimensional subspace with probability $\frac{r}{m}$. Consequently:

$$\begin{aligned} p_m^{arb}\frac{r}{m} &= \mathrm{tr}_a(\sum_{s_i}P_{v,s_i}^r\rho_a^{s_i}P_{v,s_i}^{r,\dagger}) \\ &= \mathrm{tr}_a(\sum_{s_i}P_{v,s_i}^r\rho_{a,1}^{s_i}P_{v,s_i}^{r,\dagger}) + \mathrm{tr}_a(\sum_{s_i}P_{v,s_i}^r\rho_{a,2}^{s_i}P_{v,s_i}^{r,\dagger}) \\ &= \mathrm{tr}_a(\sum_{s_i}P_{v,s_i}^r\rho_{a,2}^{s_i}P_{v,s_i}^{r,\dagger}) \end{aligned}$$

Plugging in the definition of $\rho^{s_i}_{a,2}$ and using the linearity of the trace operator results in

$$\begin{aligned} p^{arb}_m \tfrac{r}{m} &= \text{tr}_a\, \text{tr}_b (\sum_{s_i} P^r_{v,s_i} (P_{s_i} |\psi^r_2\rangle\langle\psi^r_2| P^\dagger_{s_i}) P^{r,\dagger}_{v,s_i}) \\ &\leq \text{tr}_a\, \text{tr}_b\, |\psi^r_2\rangle\langle\psi^r_2| \\ &= \lambda_{m-r+1} + \lambda_{m-r+2} + ... + \lambda_N \end{aligned}$$

where there is an inequality in the middle line because projection operators can project a state on another state with lower dimension, decreasing the success probability. Taking the supremum of all possible distillation strategies and rewriting the equation above gives the set of constraints:

$$p^{max}_{m,r} = \tfrac{m}{r} \left(\lambda_{m-r+1} + \lambda_{m-r+2} + ... + \lambda_N \right)$$

for $r \in 1, ..., m$ and so we finally obtain:

$$p^{max}_m = \min_{1\leq r \leq m} \tfrac{m}{r} \left(\lambda_{m-r+1} + \lambda_{m-r+2} + ... + \lambda_N \right) \tag{6.23}$$

Now we have shown that the theoretical upper limit is given by equation 6.23, it remains to be shown that there exists a strategy which obtains the maximum distillation probability. It will cost considerable space to develop the general m-dimensional case and for present purposes we are mainly interested in the bipartite case. For the bipartite case, lemma 6.7 will show that the theoretical upper limit is given by $\frac{2x^2}{1+x^2}$ and above several distillation strategies which obtain this bound have already been discussed. Thus for the bipartite case: QED. The reader who is interested in the general case is referred to one of the references mentioned in the text before this theorem. □

Lemma 6.7. *The entangled pure state* $|\psi\rangle = \xi(|00\rangle + x|11\rangle)$ *with* $x \in [0, 1]$ *can be distilled to a bipartite maximally entangled state with maximal success probability* P^{max}_m *given by:*

$$P^{max}_m = 2\xi^2 x^2 = \tfrac{2x^2}{1+x^2}$$

Proof. We have a bipartite state, thus $m = 2$. First assume we don't use ancilla particles, so that also $N = 2$. Then theorem 6.6 gives:

$$P^{\max}_2 = \min \left(\xi^2(1 + x^2), 2\xi^2 x^2 \right) = 2\xi^2 x^2 \tag{6.24}$$

where the last equality sign is valid because $x \in [0, 1]$.

Now we allow Alice to include ancilla particles. Because the Schmidt number equals the minimum of the dimensions of the Hilbert Spaces of Alice and Bob, the Schmidt number remains 2. Denote these two coefficients with λ_1 and λ_2, with the last one the smallest of the two.

Let $\lambda_{2,i}$ and $\lambda_{2,f}$ be the smallest Schmidt coefficient initially respectively finally (after Alice added ancilla particles). Whatever ancilla Alice adds, always $\lambda_{2,f} \leq \lambda_{2,i}$ and thus the success probability will not increase. To understand the reason for this we consider the entanglement entropy E as entanglement measure. For a bipartite pure state the Schmidt coefficients are the eigenvalues and with $\lambda_1 = \sqrt{1 - \lambda_2^2}$, we get:

$$E(\lambda_2) = S(\lambda_2) = -\sqrt{1 - \lambda_2} \log_2(\sqrt{1 - \lambda_2}) - \lambda_2 \log_2(\lambda_2) \tag{6.25}$$

Figure 6.1 shows a graph of this function, where we took $\lambda_2 \in [0, \sqrt{\frac{1}{2}}]$ because it is the smallest Schmidt coefficient. From the figure above we clearly see that if $\lambda_{2,f} > \lambda_{2,i}$ than also $E(\lambda_{2,f}) >$

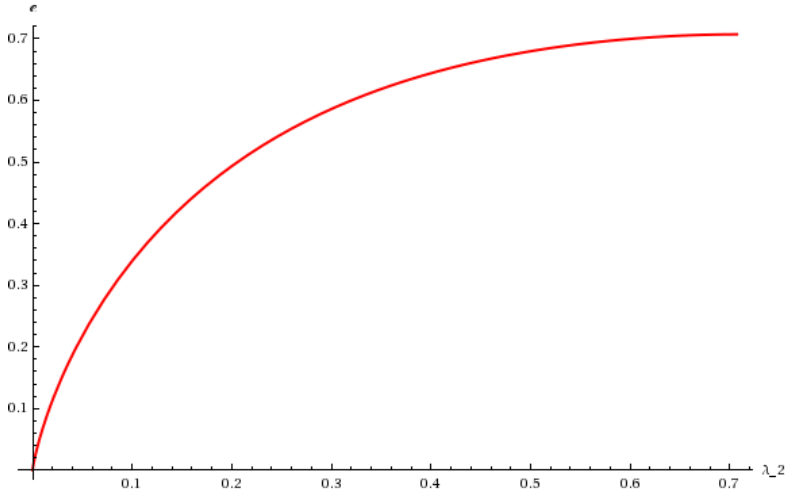


Figure 6.1: Entanglement entropy $E(\lambda_2)$ as function of the smallest Schmidt coefficient λ_2.

$E(\lambda_{2,i})$, hence: the degree of entanglement would increase. Since under LOCC operations this is impossible we must conclude that $\lambda_{2,f} \leq \lambda_{2,i}$.

It is also possible that both Alice and Bob add an ancilla. With analogous argumentation one can show that also in this situation the smallest Schmidt coefficient will not increase after the ancillas have been added. □

Theorem 6.6 and lemma 6.7 allow us to conclude:

Result 6.4. *The maximum probability to obtain a perfect bipartite quantum channel between Alice and Bob using single particle distillation is given by* $\frac{2x^2}{1+x^2}$.

6.4 Collective distillation

Due to the superadditivity of quantum channels Alice and Bob can increase the success probability of obtaining maximally entangled states between them by using multiple channels at the same time: collective distillation. An example of such a protocol is the Schmidt projection method [12], which we will investigate here. The method will be developed in three steps: (i) the $n = 2$ case; (ii) the conversion of a $|\mu\rangle_m$ state in EPR pairs and (iii) the $n > 2$ case. Subsequently, the upper bound for the success probability of collective distillation will be derived.

6.4.1 Schmidt projection method

The $n = 2$ case

First, suppose Alice and Bob share two identical partially entangled states

$$|\psi\rangle_{12} = |\psi\rangle_{34} = \xi\left(|00\rangle + x|11\rangle\right) \tag{6.26}$$

where Alice has the odd and Bob the even particles. The $n = 2$ case is analogous with the 'distillation via entanglement swapping method' as described above. To make the link the with higher dimensional case, though, we write the state a bit differently:

$$|\psi\rangle_{1234} = \xi^2\left[|0000\rangle + x^2|1111\rangle\right]_{1234} + x\left(|0011\rangle + |1100\rangle\right)_{1234} \tag{6.27}$$

Alice does a parity measurement on her particles: she measures whether she has an odd or even number of zeros. She can do this for example with the POVM of equation 5.10. If she finds an odd number of zeros she has projected their shared state in an EPR pair, whereas is she measures on even number of zeros the entanglement decreases. As discussed in subsection 6.1.2: the success probability is $\frac{2x^2}{(1+x^2)^2}$.

Conversion of higher dimensional maximally entangled states to bipartite maximally entangled states

Before we consider the case $n > 2$ we need to know how many bipartite maximally entangled states can be obtained from a m-dimensional maximally entangled state, which was defined as:

$$|\mu\rangle_m = \tfrac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle_a |i\rangle_b \tag{6.28}$$

Consider n EPR pairs:

$$|\mu\rangle_2^{\otimes n} = 2^{-n/2} \left(|00\rangle + |11\rangle\right)_{ab}^{\otimes n} \tag{6.29}$$

This can be written as:

$$\begin{aligned} |\mu\rangle_2^{\otimes n} = 2^{-n/2}(&|00\cdots 00\rangle_a |00\cdots 00\rangle_b + |00\cdots 01\rangle_a |00\cdots 01\rangle_b \\ &+ \ldots + |11\cdots 11\rangle_a |11\cdots 11\rangle_b) \end{aligned} \tag{6.30}$$

which in Schmidt form can be written as:

$$|\mu\rangle_2^{\otimes n} = 2^{-n/2} \sum_{i=1}^{2^n} |i\rangle_a |i\rangle_b \tag{6.31}$$

Thus n EPR pairs are equivalent to one 2^n-dimensional maximally entangled state, or stated differently:

Lemma 6.8. *One m-dimensional maximally entangled state is equivalent to $\log_2(m)$ EPR pairs. If m cannot be written as 2^n the result above has to be interpreted as the average number of EPR pairs for one m-dimensional maximally entangled state.*

The $n > 2$ case

If Alice and Bob share N copies of the same state, their combined quantum state can be written as:

$$|\psi\rangle^{\otimes N} = \xi^N \left(|00\rangle + x|11\rangle\right)^{\otimes N} \tag{6.32}$$

which can be written out as:

$$\begin{aligned} |\psi\rangle^{\otimes N} &= \xi^N \left(|00\cdots 0\rangle_a |00\cdots 0\rangle_b + |11\cdots 1\rangle_a |11\cdots 1\rangle\right) \\ &+ \xi^N \sum_{n=1}^{N-1} x^{N-n} \left(|\underbrace{00\cdots 0}_{n \text{ zeros}}\ \underbrace{11\ldots 1}_{N-n \text{ ones}}\rangle_a |\underbrace{00\cdots 0}_{n \text{ zeros}}\ \underbrace{11\ldots 1}_{N-n \text{ ones}}\rangle_b + \text{permutations} \right) \end{aligned}$$

In an analogous way as in the $n = 2$ case, Alice can make a measurement to determine the number of zeros in the combined state. With probability

$$p_n = \binom{N}{n} \xi^{2N} x^{2(N-n)} \tag{6.33}$$

she measures n zeros and due to the measurement the state collapses to:

$$|\psi\rangle = \binom{N}{n}^{-1/2} \left(|\underbrace{00\cdots0}_{n\text{ zeros}}\ \underbrace{11\cdots1}_{N-n\text{ ones}}\rangle_a |\underbrace{00\cdots0}_{n\text{ zeros}}\ \underbrace{11\cdots1}_{N-n\text{ ones}}\rangle_b + \text{permutations} \right) \tag{6.34}$$

The terms of state 6.34 form an orthogonal basis for a $\binom{N}{n}$-dimensional space and because all terms in the state have equal probability, state 6.34 is a $\binom{N}{n}$-dimensional maximally entangled state. Lemma 6.8 states that this can be converted in $\log_2(\binom{N}{n})$ EPR pairs. Combining all above, the average number of EPR pairs we can distill per shared partially entangled pair, i.e. the success rate or success probability p_{success}, is:

$$p_{\text{success, collective}} = \frac{1}{N} \sum_{i=1}^{N-1} p_n \log_2 \left(\binom{N}{n} \right) \tag{6.35}$$

In the limit of $N \to \infty$ this sum converges to [46]:

$$p_{\text{success, collective}} \xrightarrow{N\to\infty} -\xi^2 \log_2(\xi^2) - \xi^2 x^2 \log_2(\xi^2 x^2) = E(|\psi\rangle^{\otimes N}) \tag{6.36}$$

with E the entanglement entropy. Thus we can conclude:

Result 6.5. *The Schmidt projection method is a collective distillation method and relies on a projective measurement to determine the number of zeros in the shared states between Alice and Bob. For N shared particles, the success probability is given by:* $\frac{1}{N}\sum_{i=1}^{N-1} p_n \binom{N}{n}$. *For* $N \to \infty$, *this converges to the entanglement entropy* $E(|\psi\rangle^{\otimes N}) = -\xi^2 \log_2(\xi^2) - \xi^2 x^2 \log_2(\xi^2 x^2)$.

6.5 Optimal collective distillation

For single particle distillation we found an upper bound for the success probability to obtain an EPR pair. If we consider many particles, the success probability can be interpreted as the fraction of EPR pairs one obtains. Can we find an upper bound for the fraction of EPR pairs for collective distillation as well? For the case $N \to \infty$ this question can be answered relatively easily. Consider the Schmidt projection method with N particles. The amount of entanglement *before* the measurements is

$$E(|\psi\rangle^{\otimes N}_{\text{before}}) = NE(|\psi\rangle) = N(-\xi^2 \log_2(\xi^2) - \xi^2 x^2 \log_2(\xi^2 x^2)) \tag{6.37}$$

and the average amount of entanglement *after* the measurement equals

$$E(|\psi\rangle^{\otimes N}_{\text{after}}) \xrightarrow{N\to\infty} = N p_{\text{success, collective}} = N(-\xi^2 \log_2(\xi^2) - \xi^2 x^2 \log_2(\xi^2 x^2)) \tag{6.38}$$

Clearly $E(|\psi\rangle^{\otimes N}_{\text{before}}) = E(|\psi\rangle^{\otimes N}_{\text{after}})$: the Schmidt projection method conserves the amount of entanglement. Since the amount of entanglement can only remain the same or decrease under LOCC operations, we can conclude:

Result 6.6. *The maximum fraction of EPR pairs obtained with collective distillation protocols is obtained for the limit* $N \to \infty$, *the limit is given by the entanglement entropy* $E(|\psi\rangle^{\otimes N}) = N(-\xi^2 \log_2(\xi^2) - \xi^2 x^2 \log_2(\xi^2 x^2))$. *The Schmidt projection methods obtains this bound.*

6.6 Single vs. collective

That the maximum fraction of EPR pairs obtained with collective distillation is given by the entanglement entropy might intuitively not be surprising. The number of EPR pairs Alice and Bob share is a measure for the amount of quantum information they can communicate. Just as in the classical case the Shannon entropy gives the maximum information content of a random variable; in the quantum case the entanglement entropy gives the maximum amount of quantum information which can be obtained. As we can readily see from figure 6.6 below, the entanglement entropy not only gives the maximum fraction of EPR pairs which one can get with collective distillation, but it is also the overall maximum for every type of distillation protocol, single or collective.

We obtained the entanglement entropy is the limit $N \to \infty$, but for practical purposes this limit isn't realistic. For finite N it depends on x and N whether single or collective particle distillation has the highest success probability. Figure 6.6 below shows the graph of the fraction of obtained EPR pairs per originally shared pair p as function of x. As one can see: the x-region for which collective distillation is more efficient than single particle distillation increases with increasing N. For $N \to \infty$ collective distillation is more efficient for all x, whereas for $n < 5$ single particle distillation is always more efficient [12].

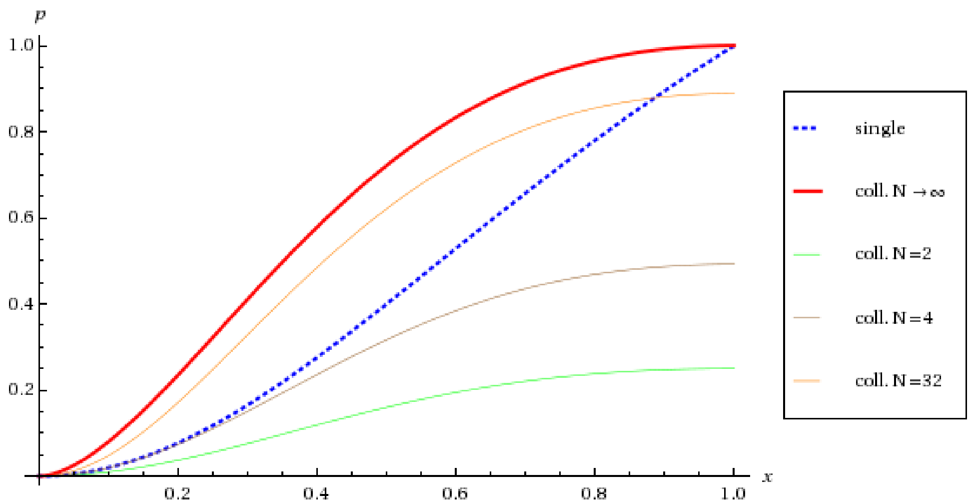


Figure 6.2: Fraction p as function of x for maximally efficient single particle distillation and for collective distillation with $N = 2$, $N = 8$, $N = 32$ and $N \to \infty$ particles.

Result 6.7. *Let N be the number of particles Alice and Bob share. For $N \to \infty$ collective distillation is always more efficient than single particle distillation, whereas for $N < 5$ the situation is reversed. For $5 \leq N < \infty$ it depends on x and N whether single or collective distillation has the highest efficiency.*

CHAPTER 7

GENERALIZATIONS

Until now we discussed the situation as described in the introduction: Alice and Bob share an entangled pair of particles ab and Alice wants to teleport particle 1 to Bob. Both Alice and Bob can create local ancilla particles.

Several important theorems of this thesis considered the broader class of quantum states, qudits, and even further generalizations are possible. In this chapter, the following three generalizations will be discussed:

- **Tripartite entanglement**. Instead of bipartite entanglement between observers Alice and Bob, we can have multipartite entanglement between n observers. For simplicity only tripartite entanglement will be considered: Alice, Bob and Charlie share an entangled state. Alice wants to teleport a qubit, but the no-cloning theorem forbids that both Bob and Charlie can receive her state. If Bob and Charlie cooperate, however, one of them can acquire Alice's qubit. This scenario is sometimes also referred to as controlled teleportation, since Alice and Bob can only teleport successfully if controller Charlie cooperates.

- **Continuous variable entangled** states can used for quantum communication just as well as discrete states.

- **Chain teleportation**. In the main scenario Alice's state is teleported directly to Bob, but if the distance between Alice and Bob is long relay stations might be necessary: Alice teleports to Daniela 1, Daniela 1 teleports to Daniela 2, ... and finally Daniela $n-1$ teleports to Bob; i.e. we get a chain of teleportations.

7.1 Tripartite teleportation

As discussed in chapter 4 multipartite entanglement is significantly more complicated than bipartite entanglement. Therefore, the generalization to multiparty entanglement will be limited to the tripartite case. Consider the following layout with observers Alice, Bob and Charlie, who share *partially entangled* particles a, b and c in state $|\psi\rangle_{abc}$. Alice has qubit 1 in state $|\psi\rangle_1$ she wishes to perfectly communicate to Bob. As mentioned above Bob can only obtain Alice's state with fidelity 1 if Charlie cooperates. Furthermore, Alice can create locally pairs of entangled particles at will. In the case of tripartite entanglement there are two different maximally entangled states: the GHZ state and the W state. For both these states the possibilities for controlled teleportation will be discussed, followed by probabilistic controlled teleportation of a general tripartite state.

7.1.1 Original teleportation with a GHZ state

Tripartite teleportation was first discussed in [54]. Remember from section 4.2 the perfect GHZ state:

$$|GHZ\rangle_{abc} = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right)_{abc}$$

The state Alice wants to teleport is as usual:

$$|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1 \tag{7.1}$$

Alice performs a Bell measurement on the particles 1 and a. Therefore, the collective system can be written as:

$$\begin{aligned}
|\psi\rangle_{1abc} &= \frac{1}{\sqrt{2}} \left(\alpha|0000\rangle + \beta|1000\rangle + \alpha|0111\rangle + \beta|1111\rangle\right)_{1abc} \\
&= \frac{1}{2}[|\Phi\rangle_{1a}^{+} \left(\alpha|00\rangle + \beta|11\rangle\right)_{bc} + |\Phi\rangle_{1a}^{-} \left(\alpha|00\rangle - \beta|11\rangle\right)_{bc} \qquad (7.2) \\
+ &\quad |\psi\rangle_{1a}^{+} \left(\alpha|00\rangle + \beta|11\rangle\right)_{bc} + |\psi\rangle_{1a}^{-} \left(\alpha|00\rangle - \beta|11\rangle\right)_{bc}] \qquad (7.3)
\end{aligned}$$

Assume Alice measures $|\Phi\rangle_{1a}^{+}$ (for other outcomes a reasoning similar as below can be employed), then Bob and Charlie end up with

$$|\psi\rangle_{bc} = \alpha|00\rangle_{bc} + \beta|11\rangle_{bc} \tag{7.4}$$

With a projective measurement Charlie performs the following basis transformation:

$$\begin{aligned}
|0\rangle &= \frac{1}{\sqrt{2}}(|f_1\rangle + |f_2\rangle) \qquad (7.5) \\
|1\rangle &= \frac{1}{\sqrt{2}}(|f_1\rangle - |f_2\rangle)
\end{aligned}$$

which leaves b and c in the state

$$\begin{aligned}
|\psi\rangle_{bc} &= \frac{1}{\sqrt{2}}[\alpha|0\rangle_b \left(|f_1\rangle + |f_2\rangle\right)_c + \beta|1\rangle_b \left(|f_1\rangle - |f_2\rangle\right)_c] \qquad (7.6) \\
&= \frac{1}{\sqrt{2}}[|f_1\rangle_c \left(\alpha|0\rangle + \beta|1\rangle\right)_b + |f_2\rangle_c \left(\alpha|0\rangle - \beta|1\rangle\right)_b] \qquad (7.7)
\end{aligned}$$

Charlie performs a Bell measurement, if he measures $|f_1\rangle_c$ Bob's particle is projected in the original state of particle 1 and if he measures $|f_2\rangle_c$ only a simple unitary transformation needs to be performed at Bob's side to acquire the original state of particle 1.

This procedure requires Alice to send 2 *c*bits to Charlie to indicate which measurement outcome she had. If Bob receives Alice's message as well, Charlie has to send just 1 *c*bit to Bob to tell his measurement outcome. Otherwise, Charlie needs to send to 2 *c*bits to inform Bob which transformation he has to perform. We note that for a maximally entangled GHZ state the success probability is 100%.

7.1.2 Original teleportation with a W state

The maximally entangled W state is:

$$|W\rangle_{abc} = \frac{1}{\sqrt{3}} \left(|001\rangle + |010\rangle + |100\rangle\right)_{abc}$$

The first step in the procedure for teleportation with this state [89] is this time for Charlie, who measures particle c in the basis $0, 1$:

$$|\psi\rangle_{abc} = \frac{1}{\sqrt{3}} \left(|00\rangle_{ab}|1\rangle_c + (|01\rangle + |10\rangle)_{ab}|0\rangle_c\right) \tag{7.8}$$

If Charlie measures $|0\rangle_c$ Alice and Bob will share a perfectly entangled state and the original bipartite teleportation scheme can be employed with 100% probability, but if Charlie measures $|1\rangle_c$ entanglement between Alice and Bob is lost and teleportation failed. This procedure requires Charlie to send Alice 3 $c$bits and Bob 1 $c$bit , to inform both whether he succeeded and Alice also of his measurement outcome. Subsequently, Alice has to send Bob 2 $c$bits to inform him which unitary transformation he has to apply in the end. The success probability of this scheme is $\frac{2}{3}$. An alternative scheme is possible as well, in which Alice does a Bell measurement first and Charlie makes a Bell measurement afterwards. This scheme has a success probability of $\frac{2}{3}$ as well [52, 88].

Thus, contrary to a perfectly GHZ state, a perfectly entangled W does not allow fidelity 1 teleportation with 100% probability.

7.1.3 Probabilistic teleportation with a general tripartite state

In the subsections above we assumed a maximally entangled tripartite state, but just as in the bipartite case degradation of entanglement makes this assumption is not very realistic. As discussed in chapter 4 the minimal basis decomposition of a pure tripartite entangled state was given by equation 4.9:

$$|\psi\rangle_{abc} = \left(\Xi|000\rangle + x_1 e^{i\mu}|100\rangle + x_2|101\rangle + x_3|110\rangle + x_4|111\rangle\right)_{abc}$$

with $\Xi = \sqrt{1 - x_1^2 - x_2^2 - x_3^2 - x_4^2}$, $x_i \in [0, 1]$ and $\mu \in [0, \pi]$. As perhaps expected, in general fidelity 1 teleportation cannot succeed with 100%. The calculation of the success probability as function of the parameters x_1, x_2, x_3 and x_4 is rather cumbersome but in principle straightforward. Therefore, the calculation is not repeated here and we just refer the interested reader to [40] pg. 1530 - 1534. Shortly, the main idea is that Charlie measures his qubit in the basis:

$$\begin{aligned} |f_1\rangle_c &= \cos\tfrac{\theta}{2}|0\rangle_c + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle_c; \\ |f_2\rangle_c &= \sin\tfrac{\theta}{2}|0\rangle_c - e^{i\varphi}\cos\tfrac{\theta}{2}|1\rangle_c; \end{aligned} \tag{7.9}$$

with $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$. As above, subsequently Alice measures in the Bell basis. Define:

$$\begin{aligned} p_1 &= \sin^2\tfrac{\theta}{2} + \Xi^2\cos\theta + \Xi x_1\cos(\mu - \varphi)\sin\theta \\ p_2 &= \cos^2\tfrac{\theta}{2} - \Xi^2\cos\theta - \Xi x_1\cos(\mu - \varphi)\sin\theta \end{aligned} \tag{7.10}$$

Then these measurement results give the following success probability for perfect teleportation:

$$\begin{aligned} P_{\text{success}} &= p_1 - \sqrt{p_1^2 - \Xi x_4 e^{-i\varphi}\sin\theta + 2\left(x_1 x_4 e^{i\mu} - x_2 x_3\right)e^{-2i\varphi}\sin^2\tfrac{\theta}{2}} \\ &+ p_2 - \sqrt{p_2^2 - \Xi x_4 e^{-i\varphi}\sin\theta - 2\left(x_1 x_4 e^{i\mu} - x_2 x_3\right)e^{-2i\varphi}\cos^2\tfrac{\theta}{2}} \end{aligned} \tag{7.11}$$

Tripartite teleportation is an experimentally accomplished fact and it is expected that such teleportation procedures will play an important role in large-scale quantum communication networks [107]. To summarize, we have:

Result 7.1. *With a tripartite state controlled teleportation is possible: Alice can teleport a quantum state to Bob if controller Charlie cooperates. With a perfect GHZ state fidelity 1 teleportation can occur with certainty, while with a perfect W state fidelity 1 teleportation can be achieved only with a success probability of $\frac{2}{3}$. A general tripartite state can be used for probabilistic teleportation.*

7.2 Continuous variables

As was explained in chapter 4.3 a continuous quantum system can be fully described by the conjugate variables x and p. Just as discrete variables continuous variables can be teleported [78]. Suppose Alice intends to teleport an unknown input state with mode in and variables x_{in} and p_{in} to Bob, using a shared EPR state with two modes a and b such that[1]

$$q_a - q_b = p_a + p_b = 0 \tag{7.12}$$

Alice performs the continuous equivalent of a Bell basis measurement by performing linear transformations on the input state and her part of the EPR pair such that she obtains:

$$\begin{cases} q_{\pm} = \frac{1}{\sqrt{2}}(q_a \pm q_{in}) \\ p_{\pm} = \frac{1}{\sqrt{2}}(p_a \pm p_{in}) \end{cases} \tag{7.13}$$

Subsequently she does a projective measurement on q_- and p_+ such that her variables collapse to:

$$\begin{cases} q_a = q_{in} + \sqrt{2}q_- \\ p_a = -p_{in} + \sqrt{2}p_+ \end{cases} \tag{7.14}$$

Due to equations 7.12 Bob's variables are projected in

$$\begin{cases} q_b = q_{in} + \sqrt{q}_- \\ p_b = p_{in} - \sqrt{2}p_+ \end{cases} \tag{7.15}$$

Analogous with the discrete case, Alice communicates her values for q_- and p_+ to Bob, although in the continuous case this are two real numbers instead of two bits. Bob uses these values to perform the following transformations:

$$\begin{cases} q_b \to q'_b = q_b - \sqrt{2}q_- = q_{in} \\ p_b \to p'_b = p_b + \sqrt{2}p_+ = p_{in} \end{cases} \tag{7.16}$$

which successfully completes the continuous variables teleportation protocol. As was mentioned in section 4.5, the first successful quantum teleportation of continuous variables was reported by Furusawa *et al* [39] in 1998. Tripartite continuous variable teleportation is possible as well.

Result 7.2. *Continuous variables can be teleported using a teleportation protocol analogous to the discrete case.*

[1] Or an equivalent condition.

7.3 Chain teleportation

As last generalization chain teleportation [103] is considered: Alice teleports her state to Bob via relay stations Daniela 1, Daniela 2, ..., Daniela $n-1$. As usual, Alice wants to teleport the state

$$|\phi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1 \tag{7.17}$$

All adjacent parties share the pure entangled state

$$|\phi\rangle = \xi(|00\rangle + x|11\rangle) \tag{7.18}$$

For simplicity, first assume that there is only one relay station: Alice teleports to Daniela and Danelia to Bob. A first strategy would be perhaps as follows:

(i) Alice teleports to Daniela with a probabilistic protocol, in the calculations below we assume she uses conclusive teleportation. As shown in chapter 5, Daniela will end up with one of the states:

$$\begin{aligned} |\psi_{p_1}\rangle_d &= \tfrac{1}{\sqrt{p_1}}\left(\alpha|0\rangle \pm x\beta|1\rangle\right)_d \\ |\psi_{p_2}\rangle_d &= \tfrac{1}{\sqrt{p_2}}\left(\pm\beta|0\rangle + x\alpha|1\rangle\right)_d \end{aligned} \tag{7.19}$$

with respective probabilities $p_1 = \xi^2\left(|\alpha|^2 + |x\beta|^2\right)$ and $p_2 = \xi^2\left(|x\alpha|^2 + |\beta|^2\right)$.

(ii) Daniela recovers the original state of Alice with a success probability of $2\xi^2x^2$.

(iii) If the state was recovered, Daniela performs a unitary transformation based on the measurement outcome of Alice.

(iv) Daniela uses a probabilistic protocol to send the state to Bob, who will also end up with equation 7.19.

(v) Bob recovers the original state of Alice with success probability $2\xi^2x^2$.

(vi) If the state was recovered, Bob performs a unitary transformation based on the measurement outcome of Daniela.

Thus the total success probability equals $4x^4\xi^4$. This easily generalizes to the case of $n-1$ relay stations were the strategy as described above would have a success probability of:

$$P_{\text{strategy 1}} = 2^n\xi^{2n}x^{2n} \tag{7.20}$$

An alternative strategy is to have the relay stations not probabilistically try to recover the original state, i.e. to skip step (ii) and (iii) above. Then instead of with one of the states 7.19 Bob receives the states

$$\begin{aligned} |\psi_{q_1}\rangle_b &= \tfrac{1}{\sqrt{q_1}}\left(\alpha|0\rangle_b + x^2\beta|1\rangle\right)_b \\ |\psi_{q_2}\rangle_b &= \tfrac{1}{\sqrt{q_2}}\left(\beta|0\rangle_b + x^2\alpha|1\rangle\right)_b \\ |\psi_{q_3}\rangle_b &= \left(\alpha|0\rangle + \beta|1\rangle\right)_b \end{aligned} \tag{7.21}$$

with respective probabilities $p_1 = \xi^2\left(|\alpha|^2 + |x^2\beta|^2\right)$, $p_2 = \xi^2\left(|\beta|^2 + |x^2\alpha|^2\right)$ and $p_3 = 2\xi^4|x|^2$. If Bob's state is $|\psi_{q_1}\rangle_b$ or $|\psi_{q_2}\rangle_b$, he can perform a probabilistic teleportation protocol with (in both cases) a success probability of $2\xi^2x^2$. In case of state $|\psi_{q_3}\rangle_b$ Bob obtains the desired state at once. Combining the probabilities above, the second strategy gives success probability:

$$P_{\text{strategy 2, 1 relay station}} = 2\xi^4(x^4 + x^2) = 2\xi^2 x^2 \tag{7.22}$$

This is because the error of the first probabilistic teleportation is partially corrected in the second teleportation, an effect that is called *error self-correction*. If more relay stations are introduced, the effect of error self-correction is even larger. With $n-1$ relay stations, the qubit of Bob will undergo n teleportations before ending up with him in one of the states:

$$|\phi\rangle_i = \frac{1}{\sqrt{q_i}}\xi^{2n}\left(x^i\alpha|0\rangle + x^{n-i}\beta|1\rangle\right)_b \tag{7.23}$$

with probabilities $p_i = \xi^{2n}x^{2i}|\alpha|^2 + x^{2(n-i)}|\beta|^2$ and $i \in 0, 1, .., n$. Let the binomial coefficient be written as $B_n^i = \frac{(n)!}{i!(n-i)!}$. The success probability therefore is [103]:

$$P_{\text{strategy 2}} = B_{2n}^n \xi^{2n} x^{2n} + \xi^{2n} \sum_{i=0, i\neq\frac{1}{2}}^{n} B_{2n}^i x^{2i} \tag{7.24}$$

Since $x \leq 1$ we have:

$$\begin{aligned} P_{\text{strategy 2}} &\geq B_{2n}^n \xi^{2n} x^{2n} + \xi^{2n} \sum_{i=0, i\neq\frac{1}{2}}^{n} B_{2n}^i x^{2n} \\ &= \xi^{2n} x^{2n} \left(B_n^{\frac{1}{2}n} + \sum_{i=0, i\neq\frac{1}{2}}^{n} B_n^i \right) \qquad (7.25) \\ &= 2^n \xi^{2n} x^{2n} = P_{\text{strategy 1}} \qquad (7.26) \end{aligned}$$

Thus for all values of n we have that strategy 2 is at least as successful as strategy 1. Figure 7.1 below shows the success probability of both strategies in the case of n relay stations for all x. Clearly, as could be seen from the formulae, strategy 2 works better.

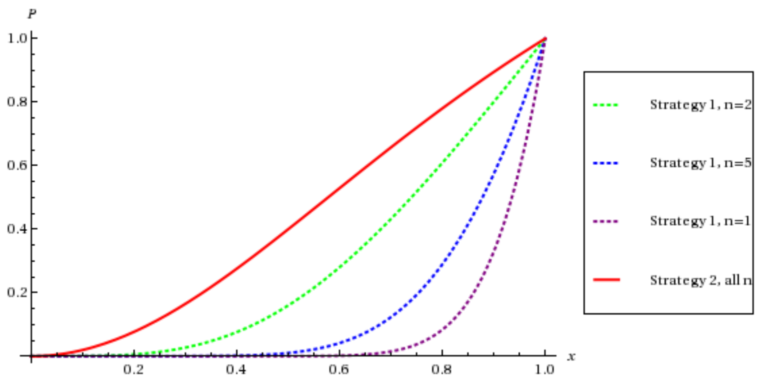


Figure 7.1: *The success probability of strategy 1 and strategy 2 as function of x for various values of n. Because in strategy 2 only one recovery attempt is made, the graph of $P_{\text{strategy 2}}$ looks the same for all n.*

Figure 7.2 shows the quotient P_2/P_1 for all x and for several values of n. Clearly, for a large value of n, i.e. many relay stations, strategy 2 is much more successful.
Thus we have established:

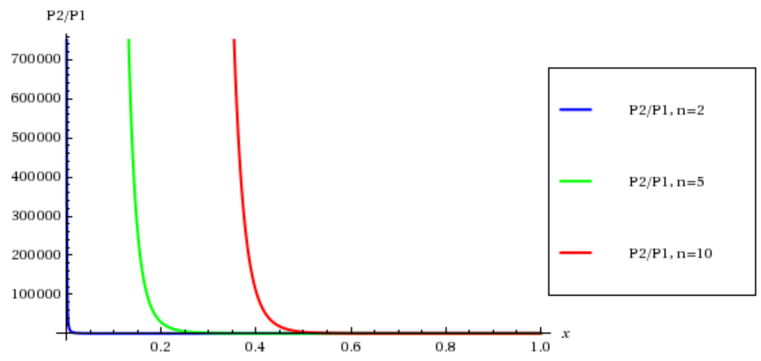


Figure 7.2: *The fraction* P_2/P_1 *as function of* x *for several values of* n.

Result 7.3. *In chain teleportation error self-correction can be used to increase the success probability of the whole teleportation process.*

CHAPTER 8

SPACY ENTANGLEMENT

Until now we discussed phenomena on quantum scales, but both (future) applications of the theory developed in this thesis as well as better understanding the philosophical background behind the theory lead us ultimately to space. Below four interesting applications of entanglement to astrophysics are given, two technical/experimental and two theoretical ones.

Establishment of a global quantum communication network. Creating quantum communication channels over a few hundred kilometer is nice, but for practical usage a global quantum communication network is required. ESA has established science programs to investigate the possibility of establishing such a network using satellites as major relay hubs. The science programs aim to perform a proof-of-principle experiment. [97].

Scientific tests with quantum physics on astrophysical scales. Satellites equipped with quantum communication modules can test quantum physics on scales far beyond the terrestrial scope [53]. The large distances and high velocities possible in space allow experiments like

- Testing the existence of Bell inequalities on astronomical distances.
- Investigating models for the collapse of quantum wave functions.
- Investigating special and general relativistic effects on entanglement. As examples: (i) The overall entanglement is Lorentz invariant but the polarization-entanglement is not, which indicates that entanglement is transferred between polarization and momentum degrees of freedom; (ii) When measuring entanglement over astronomical distances gravity should be taken into account. In many measurement schemes, optimal measurement of correlations between entangled particles requires in a common reference frame between the observes. Because a quantum particle doesn't have a well defined path, one should sum over all the possible paths, taking gravitational effects into account. The optimal reference frame for all paths will be slightly different, which can lead to a slight decrease in entanglement.
- Quantum entanglement allows quadratic increase in the phase-sensitivity of interferometers[1], allowing experimental tests of among others: (i) The Lense-Thirring

[1]An optical entanglement-enhanced interferometer, for example, can be up to 10^8 times more sensitive than its classical counterpart.

effect or frame dragging, a prediction of general relativity that the orbit of a small body orbiting a rotating massive body (for example the Earth around the Sun) is slightly perturbed due to the rotation; (ii) Gödel's cosmological model, an alternative solution to Einstein's field equations in which the universe as a whole has a net rotation.

The inflationary quantum to classical transition. During the inflationary era the universe went through a quantum to classical transition. The quantum fluctuations in the inflaton field were transformed to fluctuations in energy density and curvature, which are usually described classically. The classical description matches observations well, but how the quantum correlations were lost is still poorly understood [41]. Interestingly, this transition is an example of the macro-objectivation problem described in chapter 2. If measurements allow us to resolve the quantum to classical transition during inflation, the longstanding macro-objectivation problem might be solved and we gain fundamental new insights in quantum mechanics.

The holographic principle and beyond. The ordinary second law of thermodynamics is neither valid nor useful near black holes [10]. When the second law is only applied to the exterior it is not valid close to black holes because black holes are entropy sinks. When applied to both exterior and interior it is not useful, as for exterior observers there is no way determine the entropy of the interior of the black hole. Therefore, Bekenstein suggested the generalized second law, which states that the total entropy (near a black hole) equals the normal entropy plus $A/4$ with A the black hole surface (in Planck units). Thus, entropy of a black hole, which is just the number of degrees of freedom of the three dimensional volume enclosed within the hole, is related to its two dimensional surface area. Although black holes are fascinating in many ways, they are just physical objects and thus should obey the same laws of physics as other objects in the universe. The *holographic principle* [18] conjectures that what is true for black holes is true in general: let L be a $d-1$ dimensional volume and A its $d-2$ dimensional surface, than the number of degrees of freedom within L is given by at most $A/4$, in Planck units. Hence, effectively this means that the volume consists of an huge amount of entangled patches!

Speculatively, the holographic principle can be generalized even further. In the end entanglement is all about information and it turns out, so is a fundamental force as gravity [94]. This leads to the information postulate: gravity is not imposed on observers due to external forces, but due to information that is necessary to realize certain gravitational dynamics. From this, one might even be able to derive Newton's and Einstein's laws of gravity [99].

Two of the applications above are investigated in more detail: (i) creation of global quantum communication networks, as it represents the first step towards the ultimate application of the theory considered in this thesis and (ii) the role of entanglement in the inflationary era, because it might place the philosophical discussions presented in chapter 2 of this thesis on firm empirical grounds.

8.1 Space-QUEST experiment

The previous chapters described multiple ways to create a perfect quantum channel between two distant observers based upon shared entangled pairs. Although in theory quantum channels can be set up over arbitrary distances, in practise decoherence in optical fibers limits entanglement distribution to distances in the order of 10^2 km, much too small for a global quantum communication network. Free space links may offer an alternative, but atmospheric effects, environmental noise and Earth's curvature limit the effectiveness of such systems as well. Two principle ways to overcome these limitations are: (i) increase the distance a photon can travel in a fiber by using quantum repeaters and (ii) increase the distance a photon can travel in free space by using free space links with satellites as major communication hubs.

For the first option, consider a configuration of multiple swapping hubs as in figure 5.3. Because every photon travels a small distance only, the configuration as shown in the figure allows a qubit to be teleported over enormous distances. The creation of entanglement between distant hubs and to store it afterwards for later use is called 'heralded entanglement creation'. The basic ingredients for such a system are [91]: (i) heralded entanglement creation between several hubs; (ii) quantum memories; (iii) entanglement swapping and (iv) entanglement purification. Significant scientific effort is put in the development of these ingredients, but todays efficiencies are way too low for long distance communication.

The second option has the ability to bridge large distances because satellites are less bothered by Earth's curvature and the amount of atmosphere a photon encounters in a zenith pass corresponds to only 8 km at sea-level [101]. Contrary to quantum repeaters the technology for satellite based quantum communication stands at the eve of laboratory-level implementation. Perhaps due to the fact that the importance of quantum computation and communication within the space industry is recognized both by NASA and ESA in an early stage, already in 1998 NASA hosted a major conference on the subject [1]. Since 2002 ESA funded several studies under their General Studies Programme [6]:

- In 2002 and 2003, the 'Quantum communications in Space' (QSpace) program investigated the feasibility of quantum communication within the space infrastructure. Secondly, an overview of (fundamental) quantum physics experiments which could benefit from a space environment was given.

- This was followed by the 'accomodation of a quantum communication transceiver in an optical terminal' (ACCOM) program, which designed a complete space-based quantum communications terminal for both downlink and uplink, in 2004. The terminal is equipped with two telescopes which can independently distribute an entangled photon towards two distantly separated optical ground stations, an entangled photon source, a weak pulse laser source, single photon detection modules and optics for analyzing received photons.

- The QIPS program, running from 2005 till 2007, had a double goal. Firstly, the scientific impact, technical feasibility and required space infrastructure for the mid-term and long-term quantum experiments in space was evaluated. Secondly, a proof-of-concept experiment for free-space communication was performed. The experiment consisted of an experimental demonstration of an entanglement-based quantum key distribution protocol over a distance of 144 km [98, 84], about an order of magnitude farther than previous experiments! At the Canary Island of La Palma, polarization-entangled photons were produced. One of the photons was measured on site, while the other was sent through free space to ESA's Optical Ground Station at Tenerife, a distance of 144 km. A schematic overview of the experiment is shown in figure 8.1. The results were encouraging: despite atmospheric influences such as changes of the atmospheric layering, temperature and pressure gradients, beam wandering, atmospheric absorption, et cetera an entangled-particle count rate of $20-40$ cps with a CHSH violation $S = 2.508 \pm 0.037$ was established.

The end-to-end loss rate of this horizontal link and a link between the ground and a LEO satellite is about comparable [6].

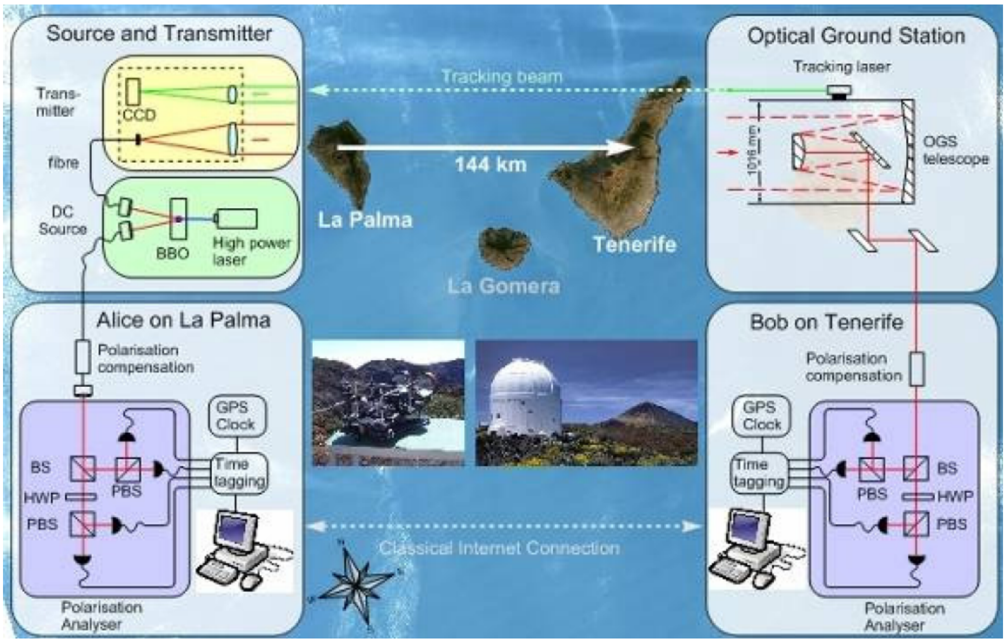


Figure 8.1: *[98] Schematic overview of the quantum communication experiment at the Canary Islands.*

The encouraging results of these programs resulted in the Space-QUEST[2] proposal of ESA's ELIPS 2 program[3]. This experiment aims to establish free-space optical communication between a quantum communication terminal on an orbital platform in space and one or more similar terminals on the ground. The two objectives of Space-QUEST are:

- Based on quantum communication, the unconditional secure global distribution of cryptographic keys.
- Fundamental quantum physics experiments using the added value of the space environment, such as long range Bell experiments over distances larger than 1000 km.

The optimal orbit for the experiment is a LEO orbit, as this gives the highest efficiency. The intended space platform is the Columbus module of the ISS, although other (LEO) space platforms are possible. On request of ESA, the European Space Science Committee (ESSC) of the European Science Foundation (ESF) evaluated ESA's ELIPS programmes in 2004. The evaluation considered the scientific quality of the Space-QUEST experiment as outstanding and advised [37]:

> *"The importance and the impressive developments in the field of long-range quantum communication and entanglement experiments ... are fully recognized. ... it is strongly recommended that the substantial leap in the scale of these experiments which would be allowed by a space-born implementation, is actively pursued."*

[2]The Space-QUEST ("QUantum Entanglement for Space experimenTs") experiment aims to establish a space-to-ground quantum communication experiment from the International Space Station (ISS).

[3]ELIPS: European programme for LIfe and Physical sciences and applications in Space.

A step in this substantial leap forward was made in 2008 with the establishment of a single-photon exchange between a satellite and an Earth-based station [101]. The Matera Laser Ranging Observatory (MLRO) of the Italian Space Agency shot weak laser pulses towards the Japanese geodetic LEO satellite Ajisai. The 1436 retroreflectors of the satellite reflected the light back towards MLRO, which detected the photons with a 5 cps count rate. A schematic overview of the experiment is shown in figure 8.2. Efficiency was quite low: losses due to the atmosphere,

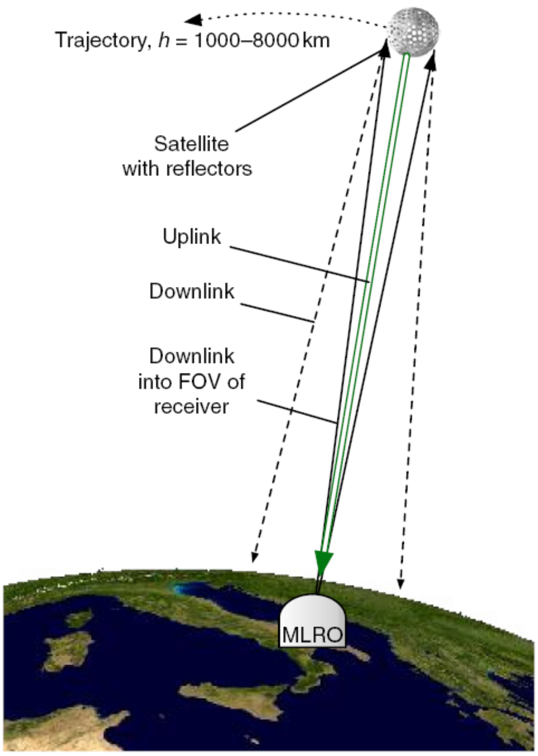


Figure 8.2: *[101] Schematic overview of the photon link between MLRO and Ajisai. A small fraction of the beam irradiates the satellite and a small portion of this is reflected back to receiver. The portion gathered by the receiver is indicated in green.*

optical equipment and the reflection of the light over a much larger solid angle than the size of the ground receiver resulted in a total attenuation along the light path of -157 dB. Nevertheless, the experiment underlined the feasibility of space to Earth quantum communication and suggested that with slightly more advanced but available technology a one-way link from space to ground can be established with only 20 dB attenuation [101].

The next ELIPS evaluation of by ESSC was conducted in 2008 [38]. Again, the Space-QUEST experiment was evaluated very positively.

> *"Strong support of cold atom physics research under weightlessness with emphasis on Phase A/B studies and pre-developments of space hardware, in particular the development of ... Space-QUEST (for quantum entanglement experiments) [is recommended]."*

Before the Space-QUEST experiment can be launched several steps need to be taken. The programmatic roadmap from first design in 2002 till the planned launch in 2015 is shown in table

8.1. At present the experiment is in a "hardware development phase": the required hardware, like an entangled photon source, a photonic transceiver and adaptations to the optical terminal is brought to TRL3 [4]. Construction of the engineering model is due to start at 2011 and the development of the proto flight model is planned in 2012. TRL6 should is envisioned for 2014 and if all goes well, Space-QUEST could be launched the year after.

Table 8.1: Programmatic roadmap for Space-QUEST [6]

Activity title	Status	Starting date	Duration (months)	Activity description
Topical team Space-Quest	On-going	2007	6	Teaming-up of European R&D-groups
Phase A study Space-Quest	Approved	2007	8	Detailed design and technical feasibility study
Photonic transceiver	Approved	2007	24	Design, develop and test a photonic quantum communications transceiver
Entangled photon source	Approved	2008	18	Design, develop and test a highly efficient potentially space-worthy entangled photon source
Quantum key distribution	Proposed	2008	12	Design a service for distributing secure quantum keys using the space segment
Application to GNSS	Proposed	2008	24	To investigate the potential of optical-quantum links for navigation systems
Additional development quantum communication terminal	Proposed	2009	18	Design, develop and test a validation model quantum communication terminal
EM space-based quantum communication terminal	Proposed	2011	18	Design, develop and test an engineering model (EM) quantum communications terminal
Ground-based quantum communication terminal	Proposed	2012	18	Implement the required modifications to the selected ground stations
PFM space-based quantum communication terminal	Proposed	2012	24	Design, develop and test a Proto Flight Model (PFM) of the quantum communications terminal which can distribute an entangled pair of photons to two separated ground stations
Space-QUEST experiment	Proposed	2015	12	Establishement of first space-to-ground quantum communication and tests of fundamental quantum physics

Result 8.1. *The 'ultimate' application of the theory considered in this thesis is the establishment of a global quantum communication network. ESA's Space-QUEST experiment is designed as*

[4]TRL = Technology Readiness Level, a term used by ESA to classify the extend to which a technology has been developed. TRL1 is the lowest level and means that the basic principles behind the technology have been observed, whereas TRL9 is the highest level and means that the technology is 'flight proven'. TRL5 is the minimal level for any technology in a definition phase of a space mission.

a first step in this direction by creating a space-ground quantum communication link. The experiment has been positively evaluated in two successive ESSC evaluations of ESA's ELIPS programme. Currently the required hardware is brought to TRL3, launch is envisioned for 2015.

8.2 Inflationary entanglement

In the philosophical prelude the macro-objectivation problem was discussed: the contradiction between theoretically expected but never observed superpositions at macroscopic scales. In cosmology, the problem emerges automatically during the inflationary epoch[5]. Quantum fluctuations in the inflaton field caused fluctuations in the energy density and consequently in the curvature of the universe. The match between the observed fluctuations and the classical (Harrison-Zeldovich) fluctuation distribution function is excellent, but the fluctuations have a quantum origin and could have been in an entangled superposition. So somewhere during inflation a quantum to classical (q2c) transition seems to have occurred and the entangled superposition is lost. The details and cause of this transition are largely unknown and provide one of the most elementary gaps in our understanding of inflation [41]. But whatever its physical cause, to go from a quantum fluctuation distribution to a classical one we need some form of wave function collapse. Interestingly, the way a wave collapses during inflation leaves imprints on the fluctuation's power spectrum and hence, is measurable! The way to interpret the measurements is not straight forward though, as the situation under consideration is unique in several ways:

1. The object under consideration is the entire universe, so the standard separation in system and environment is not possible.

2. We have only a single system, the universe, so a statistical interpretation of a measurement is out of the question.

3. The outcome of the measurement (i.e. the type of fluctuations) determines the very existence of the observers. (As the fluctuations result in the formation of cosmic structure and, in the end, humans.)

The unique situation makes the q2c transition not only interesting for cosmology, but also for quantum mechanics, as it might lift a corner of the veil regarding the mechanism of wave function collapse [76], a fundamental and philosophical issue of QM directly connected with the macro-objectivation problem discussed in the philosophical prelude.

Result 8.2. *The inflaton field causes energy and metric fluctuations. Initially these have a quantum character, but the observed fluctuations are fitted excellently by a classical distribution, so somewhere during inflation a quantum to classical transition occurred.*

Here we explore the q2c transition in cosmology, suggest solutions and their possible observational consequences. But before that, a very short non-astrophysicist overview of cosmology and its crucial concepts is given. As usual within quantum field theory literature, in this section $c = \hbar = 8\pi G = 1$.

[5]A period just after the Big Bang, in which the universe expended with the gigantic factor of 10^{60}. A short overview of cosmology and relevant concepts therein is given below.

8.2.1 The universe in a nutshell

This subsection shortly describes cosmology for the not-astrophysicist, to facilitate the understanding of the text to come. It can be skipped by those familiar with cosmology.

Cosmology is the study of the universe as a whole, it poses fundamental and fascinating questions like *What is the content of the universe?* and *What is the dynamical evolution of the universe?*. In the last ten years cosmology revolutionized from a field where only orders of magnitude mattered to a precision science, with errors in the order of percentages or less. This revolution was possible due to, among others, extremely accurate satellite observations of the Cosmic Microwave Background (CMB)[6] and enormous surveys mapping the universe further and further out[7]. A benchmark cosmological model developed: the ΛCDM Hot Big Bang model, in which the universe originated from a Big Bang and expanded ever since. Furthermore, the universe is nearly flat, consists of dark energy (71.6 %), dark matter (19.7%) and baryonic matter (4.2%) [95].

Despite the enormous success, the benchmark models has several problems that require more than increasingly accurate measurements, they require a change or addition to the basic model itself. Some of the most prominent ones are:

- **The flatness problem**: the curvature of the universe can be spherical, flat or hyperbolic. Which of the three it is depends on the total energy contained in the universe: if the universe has exactly the critical density, it will be flat; if it contains more, it will be spherical and if it contains less it will be hyperbolic. Using the best measurements to date to extrapolate back to a Planck time[8] after the Big Bang, the deviation of the density from the critical density is smaller than 10^{-60}. Why is the density of the universe so extremely close to the critical density?

- **The horizon problem**: observations of the CMB show a very homogeneous temperature distribution across the entire sky: $\delta T/T < 10^{-5}$, corresponding to a very homogeneous density distribution at the time of CMB emission. However, two arbitrary regions of the CMB on opposite sides of the sky have never been in causal contact with each other, so how can they have the same density?

- **The monopole problem**: most present day Grand Unified Theories predict the existence of an abundance of monopoles, but they have never been observed. Where are they?

- **The formation of structure**: on cosmological small scales, the universe contains a wealth of structure. Millions of galaxies span enormous sheets and filaments, which come together in nodes called galaxy clusters. The sheets and filaments surround gigantic empty regions, the voids. How does this structure come about?

These problems above vanish into thin air if the universe went through a short period of extreme stupendous expansion just after the Big Bang: between 10^{-36} and 10^{-34} seconds after the Big Bang the universe inflated with a factor 10^{60}. Cosmologists name this the inflationary epoch of the universe and it solves all the problems mentioned above:

[6]Made with in particular NASA's Cosmic Background Explorer (CBE) and Wilkinson Microwave Anisotropy Probe (WMAP).

[7]Made with in particular the 2dF Galaxy Redshift Survey and the Sloan Digital Sky Survey.

[8]The smallest unit of time which is physically possible, 5×10^{-44} s.

- **The flatness problem** because due to stupendous expansion locally the universe seems flat, whereas it is curved on large scales. (By analogue, consider a microbe on an inflated balloon: for the microbe everything seems flat, but the balloon is curved.)
- **The horizon problem** by allowing all points in the universe to be in thermal contact before inflation.
- **The monopole problem** because inflation diluted the monopole density by 10^{60^3}.
- **The formation of structure** by blowing up quantum mechanical fluctuations in the inflaton field to macroscopic proportions. Afterwards gravitational attraction makes the dense regions denser and the less-dense regions thinner, resulting after billions of years in the large scale structure we observe today.

The default inflation paradigm is:

- Assume an homogeneous and isotropic space-time, with as dominant component the scalar field $\phi(\vec{r}, t)$, named the inflaton field. The field associates with every point in space-time a potential energy $V(\phi)$. Its vacuum state, which is also homogeneous and isotropic, is given by $\phi(\vec{r}, t) = \phi_0(t) + \delta\phi(\vec{r}, t)$, with $\phi_0(t)$ the expectation value of the quantum field and $\delta\phi(\vec{r}, t)$ the quantum fluctuations induced by the Heisenberg Uncertainty Principle.
- The quantum fluctuations of the inflaton field perturb the metric and energy density of the universe and causes fluctuations in them.
- During inflation these fluctuations grow exponentially and at a certain time become larger than the horizon distance. This is usually considered the quantum to classical transition and from that moment on the fluctuations are waves in a classical field. After inflation the horizon distance continues to increase and at a moment the fluctuations reenter the horizon. There, they transform in the seeds of cosmic structure.

8.2.2 The quantum to classical transition

The quantum fluctuations leading to cosmic structure formation might not be describable classically, and when entangled superpositions occur a classical description is out of the question for sure. Although a classical description fits observations very well, why it fits is poorly understood and needs to be justified. It is expected that entanglement is lost when the quantum fluctuations are stretched beyond the cosmic horizon. Then, the quantum distribution of the fluctuations can be replaced by a classical one [41]. Below we will investigate two approaches of the q2c transition to see whether this premise holds and whether something can be learned about the mechanism causing wave function collapse. Fascinatingly, the mechanism for wave function collapse is directly connected to the macro-objectivation problem: different solutions to the problem require different ways of collapse, if collapse occurs at all. Therefore, if the q2c transition can learn us something about the mechanism causing collapse, it might shed experimental light on an issue considered to be purely philosophical!

A first step in describing the q2c transition is by introducing the creation and annihilation operators $a_n^\dagger$ and a_n, defined as:

$$\hat{a}_j = \hat{q}_j + i\hat{p}_j$$
$$\hat{a}_j^\dagger = \hat{q}_j - i\hat{p}_j$$

Secondly, the general n-dimensional QFT Lagrangian was given by equation 4.11:

$$L = \tfrac{1}{2}\int d^n dx \left(\dot{\phi}^2 - (\vec{\nabla}\phi)^2 - m^2\phi^2\right)$$

Introduction of the conformally rescaled variable $q = a\phi$ allows us to rewrite the Lagrangian 4.11 as:

$$L = \int d^3x \tfrac{1}{2}\left[\left(q' - \frac{a'}{a}q\right)^2 - (\partial_i q)^2\right] \tag{8.1}$$

with the scalar field equation of motion

$$q'' - \frac{a''}{a}q - \partial_i^2 q = 0 \tag{8.2}$$

Below we will discuss two q2c transition possibilities, one based on decoherence and another more general one, in which different parametric models for wave function collapse are considered.

A decoherence approach

In an article in 2008 Nambu [66] investigates a decoherence based q2c transition. As metric he takes

$$ds^2 = a(\eta)^2\left(-d\eta^2 + dx^2\right) \tag{8.3}$$

where the conformal time is denoted by η, $a = -1/(H\eta)$ and $\eta \in (-\infty, 0)$, with H Hubble's parameter [9]. To investigate entanglement [66] discretizes the scalar field, for simplicity in a one-dimensional space. The discrete Lagrangian is given by

$$\mathcal{L} = \frac{\Delta x}{2}\sum_{j=1}^{N}\left[\left(q_j' - \frac{a'}{a}q_j\right)^2(\Delta x)^2 - (q_j - q_{j-1})^2\right] \tag{8.4}$$

where Δx is the lattice spacing, q_j the strength of the field at the j-th lattice site and N the total number of lattice sites. If we rescale the time variable as $\eta \to \eta\Delta x$, the equation of motion can be written as:

$$q_j'' - \frac{a''}{a}q_j + 2q_j - \alpha(q_{j+1} + q_{j-1}) = 0 \tag{8.5}$$

with periodic boundary conditions (i.e. $q_0 = q_N$ and so on) and $j \in 1, ..., N$. The parameter $\alpha \approx 1$ [10]. Using the Fourier expansion of the scalar field, the canonical variables can be written as

$$q_j = \frac{1}{\sqrt{N}}\sum_k (f_k a_k + f_k^* a_{N-k}^\dagger)e^{ikj} \tag{8.6}$$

$$p_j = \frac{1}{\sqrt{N}}\sum_k (-i)(g_k a_k - g_k^* a_{N-k}^\dagger)e^{ikj} \tag{8.7}$$

[9] The model includes a cutoff at short wavelength modes to regularize the UV divergence, but this cutoff does not influence the main line of the derivation

[10] α is introduced for technical reasons, to prevent infrared divergence. It is chosen sufficiently close to one that it doesn't influence computations.

with $k_r N = 2\pi r$, $r \in \mathbb{N}$ and f_k and g_k the mode functions of the quantum state of the scalar field. For the scalar field a Bunch-Davies vacuum is chosen:

$$\begin{aligned} f_k &= \frac{1}{\sqrt{2\omega_k}}\left(1 + \frac{1}{i\omega_k\eta}\right)e^{-i\omega_k\eta} \\ g_k &= \sqrt{\omega_k/2}e^{-i\omega_k\eta} \end{aligned} \tag{8.8}$$

with $\omega_k^2 = 2(1 - \alpha\cos(k))$. Only bipartite entanglement is considered and thus two spatial blocks A and B are introduced by averaging over n lattice sides:

$$\begin{aligned} q_{A(B)} &= \frac{1}{\sqrt{n}}\sum_{j\in A(B)} q_j \\ p_{A(B)} &= \frac{1}{\sqrt{n}}\sum_{j\in A(B)} p_j \end{aligned} \tag{8.9}$$

The entanglement between the regions A and B is computed using the two point correlation functions

$$\begin{aligned} g_{|j-l|} &= \tfrac{1}{2}\langle q_j q_l + q_l q_j\rangle = \tfrac{1}{N}\sum_{k=0}^{N-1}|f_k|^2\cos(k(j-l)) \\ h_{|j-l|} &= \tfrac{1}{2}\langle p_j p_l + p_l p_j\rangle = \tfrac{1}{N}\sum_{k=0}^{N-1}|g_k|^2\cos(k(j-l)) \\ k_{|j-l|} &= \tfrac{1}{2}\langle q_j p_l + q_l p_j\rangle = \tfrac{i}{2N}\sum_{k=0}^{N-1}(f_k g_k^* - f_k^* g_k)\cos(k(j-l)) \end{aligned} \tag{8.10}$$

Then the covariance matrix becomes

$$V = \begin{pmatrix} A & C \\ C & A \end{pmatrix} \qquad A = \begin{pmatrix} a_1 & a_3 \\ a_3 & a_1 \end{pmatrix} \qquad C = \begin{pmatrix} c_1 & c_3 \\ c_3 & c_1 \end{pmatrix} \tag{8.11}$$

with

$$\begin{aligned} a_1 &= \langle q_A^2\rangle = \langle q_B^2\rangle = \tfrac{1}{n}\sum_{i,j\in A} g_{|i-j|} \\ a_2 &= \langle p_A^2\rangle = \langle p_B^2\rangle = \tfrac{1}{n}\sum_{i,j\in A} h_{|i-j|} \\ a_3 &= \langle q_A p_A + p_A q_A\rangle = \tfrac{1}{n}\sum_{i,j\in A} k_{|i-j|} \\ c_1 &= \langle q_A q_B + q_B q_A\rangle = \tfrac{1}{n}\sum_{i\in A, j\in B} g_{|i-j|} \\ c_2 &= \langle p_A p_B + p_B p_A\rangle = \tfrac{1}{n}\sum_{i\in A, j\in B} h_{|i-j|} \\ c_3 &= \langle q_A p_B + p_B q_A\rangle = \tfrac{1}{n}\sum_{i\in A, j\in B} k_{|i-j|} \end{aligned} \tag{8.12}$$

As we do not observe degrees of freedom outside the regions A and B, the evolution of the bipartite system is non-unitary and decoherence with the rest of the universe takes care of disentanglement.

The continuous Peres Horodecki criterion, theorem 4.5, stated that 2×2 Gaussian state is separable if and only if its partial transpose is positive, which by the above is equivalent with the statement

$$\tilde{V} + \tfrac{i}{2} J \geq 0$$

By William's theorem (see again the proof of theorem 4.4), there is a symplectic transformation S such that V can be rewritten as

$$V_{\text{can}} = SVS^T = \text{diag}\,(\kappa_1, \kappa_2, \kappa_1, \kappa_2)$$

and with $\kappa_1, \kappa_2 \geq \frac{1}{2}$ for all physical states. Let κ_2 be the smallest of the symplectic eigenvalues, than a separability criterion can be given by the inequality

$$\tilde{\kappa}_2 \geq \tfrac{1}{2} \tag{8.13}$$

with $\tilde{\kappa}_2$ the smallest symplectic eigenvalue of $\tilde{V}$. The smallest simplectic eigenvalues are given by [87]:

$$\begin{aligned} \kappa_2^2 &= a_1a_2 - a_3^2 + c_1c_2 - c_3^2 - |a_1c_2 + a_2c_1 - 2a_3c_3| \\ \tilde{\kappa}_2^2 &= a_1a_2 - a_3^2 - c_1c_2 + c_3^2 \\ &\quad - |(a_1c_2 - a_2c_1)^2 + 4(a_1c_3 - a_3c_1)(a_2c_3 - a_3c_2)|^{1/2} \end{aligned} \tag{8.14}$$

which by the above are measures for whether the state is physical and whether the state is entangled. Numerical evaluation of these eigenvalues as function of conformal time η gives the graph of figure 8.3. Let η_c be the critical time, the time at which entanglement is lost.

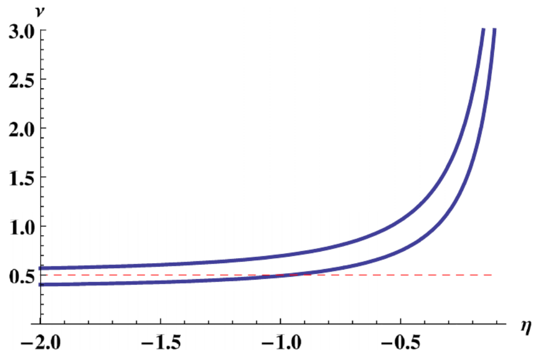


Figure 8.3: *[66] Evolution of eigenvalues as function of conformal time. The upper line represents κ_2, the condition $\kappa_2 > \frac{1}{2}$ is always satisfied. The bottom line shows $\tilde{\kappa}_2$, as one can see entanglement is lost around* $\eta = -1.0$.

Figure 8.4 shows how η_c changes with the region size n. For smaller n the graph corresponds to $\eta_c = -n$, which in physical units corresponds to

$$a(\eta_c) n \Delta x = 1/H \tag{8.15}$$

I.e. entanglement between two regions is lost when their size equals the horizon length. This justifies the usual assumption in literature: horizon size inflationary domains evolve independently. The deviation at higher n is probably due to the periodic boundary conditions.

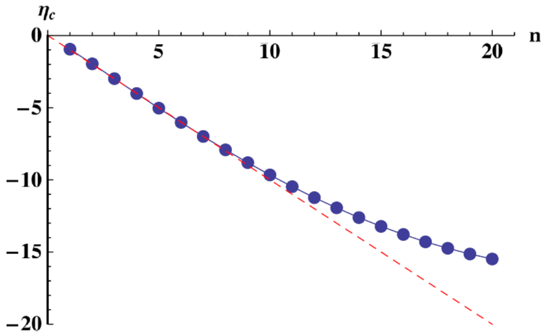


Figure 8.4: *[66] Region size n as function of conformal time. The dashed line is the line $\eta_c = -n$.*

A wave function collapse approach

A bit more general approach is taken by De Unánue and Sudarsky [27], building upon [76]. They don't consider a specific physical process for wave function collapse but only discuss it parametrically. [27] begins also with the Lagrangian and equation of motion given by equations 4.11 and 8.2, but they use the metric

$$ds^2 = a(\eta)^2 \left[-(1+2\Psi)d\eta^2 + (1-2\Psi)\delta_{ij}dx^i dx^j\right] \tag{8.16}$$

with Ψ the so-called Newtonian potential, physically it can be seen as a perturbation term. Instead of a one-dimensional parametrization, a box of size N is introduced, satisfying the equation of motion 8.2 as real planar waves. Quantization is achieved by using the standard commutation relations between q and p, giving:

$$q(\eta, \vec{x}) = \frac{1}{N^3}\sum_{\vec{k}} \left(a_k(\eta)e^{i\vec{k}\cdot\vec{x}} + a_k^\dagger(\eta)e^{-i\vec{k}\cdot\vec{x}}\right) \tag{8.17}$$

where $k_r N = 2\pi r$ with $r \in \mathbb{N}$. Analogous as with the previous approach, a Bunch-Davies vacuum is assumed (see equations 8.9), allowing us to write

$$q_j = \frac{1}{N^3}\sum_{\vec{k}} (f_k^* a_k + f_k a_{-k}^\dagger)e^{i\vec{k}\cdot\vec{x}} \tag{8.18}$$

$$p_j = \frac{1}{N^3}\sum_{\vec{k}} i(g_k^* a_k - g_k a_{-k}^\dagger)e^{i\vec{k}\cdot\vec{x}} \tag{8.19}$$

Now we have to specify a collapse scheme to determine the state of the field after collapse. From Einstein's equations

$$G_{ab} = 8\pi G\langle T_{ab}\rangle \tag{8.20}$$

follow the zeroth and first order equations for the inflation field ϕ. The zeroth order equation leads to the Friedmann equation and the quantized first order equations relate the gravitational perturbations to the field perturbations (see [76] for details):

$$\nabla^2\Psi_k = 4\pi G\phi_0'\langle\delta\phi_k'\rangle \tag{8.21}$$

where we average over all states of the inflaton field. Note that with 'averaging over all states' it is not meant that the universe is in an ensemble of states, it is just in one. It means that we should consider an imaginary ensemble of universes, in which our universe is just one specific realization. Furthermore, we don't see one specific value of $\vec{k}$ or Ψ_k for each k seperately, but a combination of all modes of the spherical harmonic decomposition of the CMB temperature fluctuations $\frac{\Delta T}{T}(\theta, \phi)$, which can be expressed as

$$\frac{\Delta T}{T} = \sum_{lm} \alpha_{lm} Y_{l,m}(\theta, \phi) \tag{8.22}$$

This equation connects the measurable temperature fluctuations with the above via the quantities α_{lm}, because α_{lm} can be expressed in terms of the Newtonian potential on the CMB surface $\Psi(\eta_D, \vec{x}_D)$:

$$\alpha_{lm} = \int \Psi(\eta_D, \vec{x}_D) Y^*_{lm} d^2\Omega \tag{8.23}$$

The square of α_{lm} gives the magnitude of the quantum fluctuations. To express the Newtonian potential at these points, we integrate equation 8.21 and sum it over all k to obtain

$$\Psi(\eta, \vec{x}) = \sum_k \frac{4\pi G \phi_0' \mathcal{T}(k)}{k^2 N^3} \langle \delta\phi_k' \rangle e^{i\vec{x}\cdot\vec{k}} \tag{8.24}$$

where $\mathcal{T}(k)$ represents the physical effects of the period between reheating and decoupling. Plugging this in equation 8.23, squaring to obtain the magnitude, using that $\langle \phi_k \rangle \langle \phi_{k'} \rangle^*$ can be written as $\frac{1}{4} k C(k) N^3 \hbar / a^2$ (see [27] for details) and using Fourier expansion we find that the magnitude:

$$\|\alpha_{lm}\|^2 = \frac{8\pi G^2 \phi_0' \delta\phi_0'^2}{a^2} \int C(k) \frac{\mathcal{T}(k)^2}{k^3} \langle \delta\phi_k' \rangle \langle \delta\phi_k' \rangle^* j_l^2(|\vec{k}| R_D) |Y_{lm}(k)^2| dk^3 \tag{8.25}$$

with R_D the comoving radius of the surface of last scattering.

In the classical case $C_0(k) = 1$. By choosing another function for $C(k)$ quantum mechanical effects can be taken into account. Deviations from the classical case shouldn't be made to large, as the classical case fits observations well. The detailed form of $C(k)$ depends on the model for wave function collapse. In [76] two simple models for $C(k)$ are developed:

$$C_1(k) = 1 + \frac{2}{z_k^2} \sin^2(\Delta_k) + \frac{1}{z_k} \sin(2\Delta_k) \tag{8.26}$$

$$C_2(k) = 1 + \sin^2 \Delta_k \left(1 - \frac{1}{z_k^2}\right) - \frac{1}{z_k} \sin(2\Delta_k) \tag{8.27}$$

with η_c^k the time of collapse of mode k, $\Delta_k = k(\eta - \eta_k^c)$ the 'collapse to observation delay' and $z_k = \eta_k^c k$. The physical background of these models is discussed at length in [76]. Shortly, the first model assumes that the expectation values of the canonical variables p_k and q_k after collapse are uncorrelated and randomly distributed within the ranges of uncertainties in the precollapsed state. In the second scheme only the conjugate momentum changes its expectation value from zero to a value in such a range. It is interesting to note that $\lim_{z_k \to \infty} C_1(k) = C_0(k) = 1$, so at infinite redshift the classical spectrum is recovered. $C_2(k)$ doesn't have this property.

We obtain $C_0(k)$ if z_k is independent of k, hence

$$\eta_k^c = z_k / k \tag{8.28}$$

Because deviations from the classical value are small, it is logical to consider small deviations from an k-independent z_k. To do so, we parametrize

$$z_k = A + BkR_D \tag{8.29}$$

with A and B constants and we multiplied with R_D to obtain a dimensionless quantity. Classical inflation models predict $\|\alpha_{lm}\|^2 \propto [2l(l+1)]^{-1}$, thus for this model the factor $\|\alpha_{lm}\|^2 2l(l+1)$ should be a constant line at 1. Plots for $C_1(k)$ and $C_2(k)$ as function of l are shown in figure 8.5 for different choices of A and B. As one can see, different models for $C(k)$ and the different values of the parameters A and B all result in a different graphs, making the different models distinguishable in principle.

Although the deviations in figure 8.5 seem not that large, they have a huge effect on the time of the q2c transition. To see this, let's compare the scale factor of the horizon crossing of the k-th mode a_k^H, which represents the classical q2c transition, with the scale factor of collapse of the k-th mode a_k^c. The moment of horizon crossing happens when the length corresponding to mode k has the same size as the horizon radius H^{-1}, thus $a_k^H = k/H$. If we also remember from equation 8.15 that $a(\eta) = -1/(H\eta)$, we get:

$$\frac{a_k^H}{a_k^c} = k\eta_k^c = z_k = A + BkR_D \tag{8.30}$$

Figure 8.6 shows the value of $\frac{a_k^H}{a_k^c}$ for a wide range of k. As one can see, the difference between a_k^H and a_k^c can be substantial.

Result 8.3. *In literature it is generally assumed that the quantum to classical transition occurred when the size of a mode reached the size of the horizon. As can be seen from the models discussed in this section, the situation is more complicated and model dependent; in some models the quantum to classical transition occurs a thousand times faster than a mode reaching horizon size.*

Observations of the collapse

A major question is if any of the effects described above can be observed. The promising answer: maybe! Detailed power spectra show a turn down in the CMB data [95] attributed to the damping effect: the damping of inhomogeneities due to nonzero mean-free-path of photons at the time of decoupling. As one can see from figure 8.5 some values of A and B result in extra damping. If the Planck satellite will have enough resolution at large l, [27] expect that the classical damping effect and the additional quantum mechanical damping described here can be separated and used to constrain A and B. In turn this constraints quantum mechanical wave function collapse!

Result 8.4. *There are several ways to model the quantum to classical transition during inflation, the details of the model depend on the assumed cause of wave function collapse. If observations are sensitive enough, it might be possible to distinguish between different models. Since wave function collapse is directly connected to the macro-objectivation problem, the inflationary quantum to classical transition provides us with the unique opportunity to gain some experimental insight on a domain of quantum mechanics considered to be purely philosophical!*

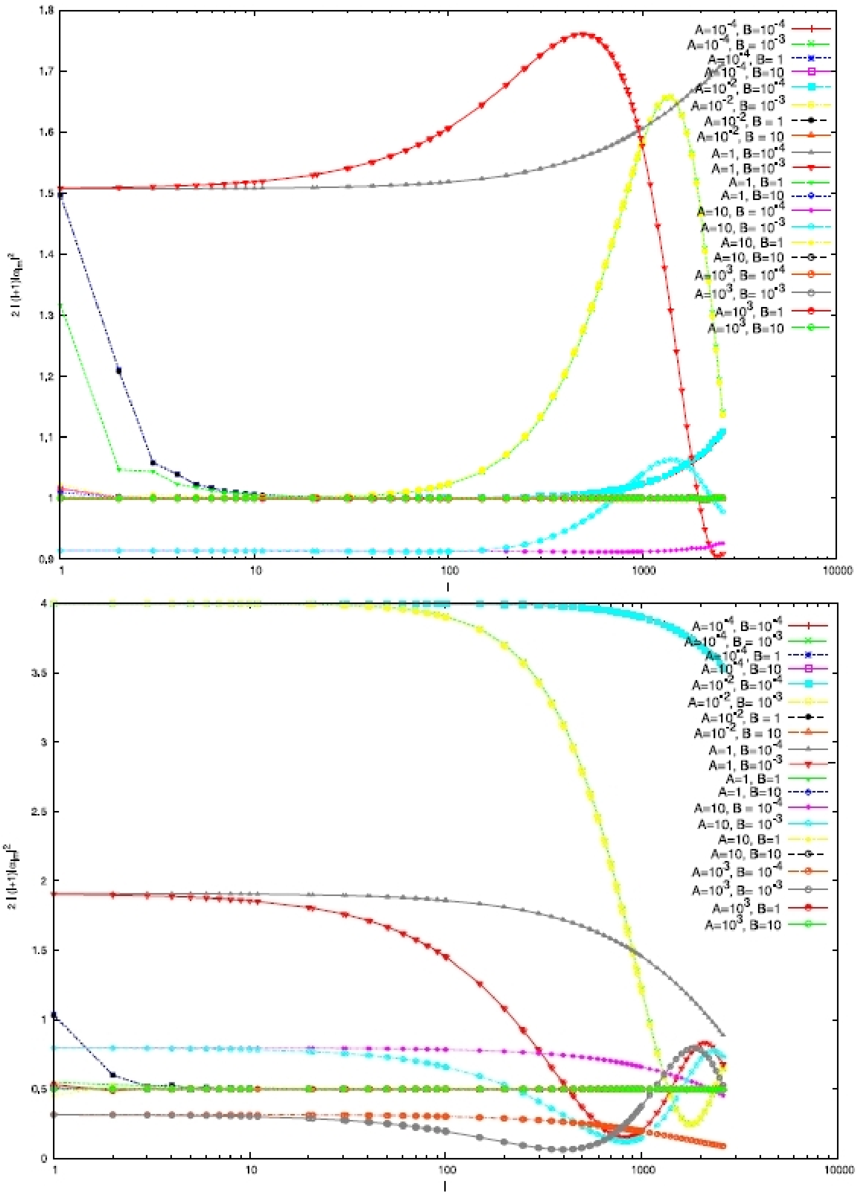


Figure 8.5: *[27] Semilog plot of* $2l(l+1)\|\alpha_{lm}\|^2(C_i(k))$ *with* $i = 1$ *(top) and* $i = 2$ *(bottom). The different orders of magnitude for* A *and* B *represent the robustness of the collapse scheme under departure from* z_k *is constant.*

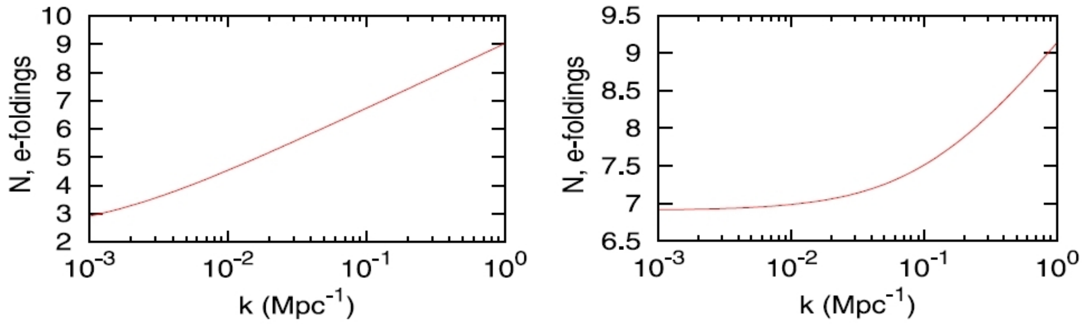


Figure 8.6: *[27] Semilogarithmic plot of the number of e-foldings between* a_k^H *and* a_k^c *for the best fit values of* A *and* B *for both models. Left:* $C_1(k)$ *with* $(A, B) = (10, 1)$*; right:* $C_2(k)$ *with* $(A, B) = (1000, 1)$.

CHAPTER 9

SUMMARY AND CONCLUSIONS

This thesis compares the maximum obtainable efficiency of several quantum communication protocols of three important quantum communication techniques without classical counterpart: teleportation, single particle distillation and collective distillation. Two essential factors in the obtainable efficiency are the entanglement fraction x and the number of channels N that two distant communication partners Alice and Bob share, with $x \in [0, 1]$ and $0 \leq N < \infty$. If $N < 5$ single particle distillation allows for the highest efficiency while for $5 \leq N < \infty$ it depends on x and N whether single particle distillation or collective distillation is most efficient. For single particle distillation, several protocols to obtain this maximum bound are available, an example is the Procrustean method. For collective distillation, the Schmidt projection method obtains the theoretical maximum bound. More precisely, figure 9 below shows the maximal success probability p as function of x for several quantum communication techniques.

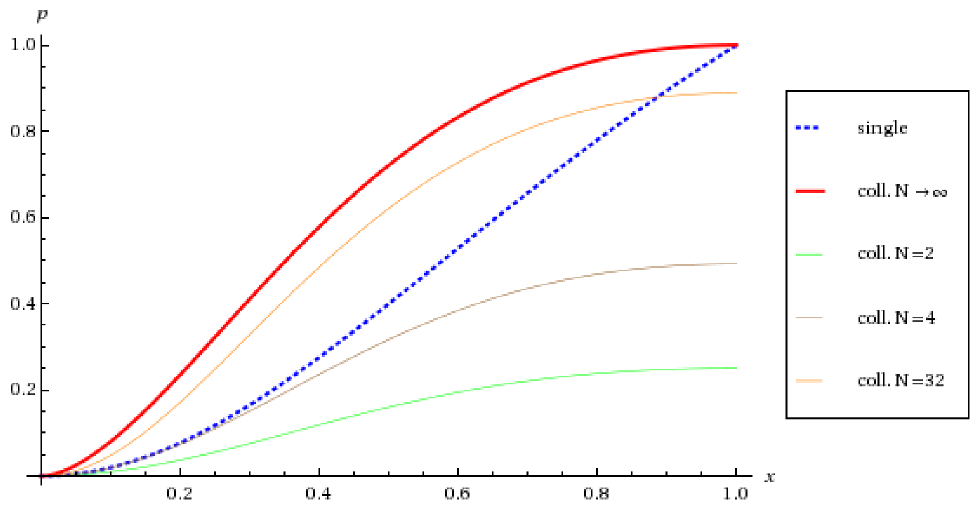


Figure 9.1: Success probability p as function of x for maximally efficient single particle distillation and for collective distillation with $N = 2$, $N = 8$, $N = 32$ and $N \to \infty$ particles.

The ultimate application of quantum communication protocols is the establishment of a global quantum communication network. Both ESA and NASA finance extensive studies to es-

tablish such an network. ESA's program, the Space-QUEST program, currently brings the first experimental hardware up to TRL3, launch of this hardware is envisioned for 2015.

The fundamental property of quantum mechanics that allows quantum communication is non-locality. *Non-local quantum states are entangled, meaning that they show stronger correlations than classicly possible. A superposition of entangled states allows quantum communication techniques.* Superposition is often observed at microscopic scales but never at macroscopic scales, although one can construct situations at which macroscopic superposition occurs. This is named the macro-objectivation problem. Today, a discussion about this problem is mainly philosophical, but *inflationary entanglement may shed experimental light upon these fundamental concepts.*

Below an overview in bulletpoints of the major aspects of this thesis is given.

1. Quantum mechanics is fundamentally non-local (section 2).

2. A contemporary problem with the interpretation of quantum mechanics is the theoretically predicted but never observed superposition of macroscopic states. The philosophical problem is named the macro-objectivation problem.

3. Entanglement is the characteristic property of quantum mechanics that overcomes the LOCC constraint (*Local quantum Operations and Classical Communications*. The simplest form of entanglement is bipartite entanglement (section 4.1). This type of entanglement can be quantified uniquely and several measures exist, among which are entanglement cost, entanglement distillation and entanglement entropy. Multipartite entanglement is more difficult to quantify than bipartite entanglement because there are several inequivalent type of states (section 4.2).

4. Continuous variable entanglement describes correlations between continuous observables and is fully described by modes. Handling general continuous variable entanglement is rather difficult and for most practical purposes the subset of Gaussian states is sufficient. These states are mathematically relatively easy and thank there name from the fact that their characteristic function is a Gaussian. For Gaussian states, a criterium to determine whether a state is physical and whether a state is entangled is developed. Two useful continuous variable entanglement measures are entanglement entropy and logarithmic negativity (section 4.3).

5. Entanglement cannot be used to make a perfect copy of a quantum state or transmit information faster than light (section 4.6).

6. Quantum teleportation is a quantum measurement procedure that allows two observers Alice and Bob to communicate one qubit with fidelity 1 if they share a maximally entangled bipartite state (section 5.1).

7. The original teleportation procedure doesn't transfer the qubit with fidelity 1 if Alice and Bob don't share a maximally entangled bipartite state. The teleportation protocol can be adapted to a probabilistic protocol that transfers the qubit with fidelity 1 but has only a success probability p (section 5.2). Some leading examples of probabilistic teleportation protocols are:

   - Conclusive teleportation uses a two step POVM measurement procedure to obtain fidelity 1 with success probability $\frac{2x^2}{1+x^2}$. The procedure requires one pure *e*bit and three *c*bits .

- Qubit assisted conclusive teleportation uses an ancilla qubit such that with some probability a teleportation scheme analogous to the original scheme can be employed, while in the other case a conclusive-like scheme has to be used. The overall success probability is $\frac{2x^2}{1+x^2}$. The procedure requires one pure *e*bit and three *c*bits .
- Probabilistic teleportation with a unitary transformation obtains fidelity 1 with success probability $\frac{2x}{1+x^2}$. The protocol requires one pure *e*bit and three *c*bits .
- The probabilistic teleportation protocol of Agrawal and Pati uses a generalized measurement with two tunable parameters to obtain fidelity 1 with success probability $\frac{2x^2}{(1+x^2)^2}$, if an appropriate value for the parameters is chosen. The procedure requires one pure *e*bit and three *c*bits .

8. Single particle distillation is a quantum measurement procedure that allows Alice and Bob to obtain a shared maximally entangled bipartite state from a shared noisy pure state with probability p (section 6.1). Some leading examples of single particle distillation protocols are:

   - The Procrustean method distills a maximally entangled state from a partially entangled state by cutting off the excess probability of the larger basis term. The procedure requires one *e*bit and two *c*bits and has success probability $\frac{2x^2}{1+x^2}$.
   - Purification via entanglement swapping uses two partially entangled states with the same degree of entanglement to swap 'a bit of entanglement' from one of the states to the other. This procedure has success probability $\frac{2x^2}{(1+x^2)^2}$. One pure *e*bit and three *c*bits are required. If the procedure fails Alice and Bob still share an entangled state (although with less entanglement) and they can try again.

9. Consider an arbitrary single particle distillation protocol which has entanglement fidelity $F_e = 1$ with success probability p, then for the bipartite case there is a probabilistic teleportation protocol which has fidelity $f_p = 1$ with probability p; and vice versa. I.e.: teleportation and single particle distillation are equivalent (section 6.2).

10. The maximum probability to obtain a perfect bipartite quantum channel between Alice and Bob using single particle distillation / teleportation is given by $\frac{2x^2}{1+x^2}$. This bound is obtained by several protocols (section 6.3).

11. Due to the superadditivity of quantum channels Alice and Bob can increase the success probability of obtaining maximally entangled states between them by using multiple channels at the same time: collective distillation (section 6.4). A leading example of such a protocol is:

    - The Schmidt projection method relies on a projective measurement to determine the number of zeros in the shared states between Alice and Bob. For N shared particles, the success probability is given by: $\frac{1}{N}\sum_{i=1}^{N-1} p_n \binom{N}{n}$.

12. The maximum fraction of EPR pairs obtained with collective distillation protocols is obtained for the limit $N \to \infty$, the limit is given by the entanglement entropy $E = (-\xi^2 \log_2(\xi^2) - \xi^2 x^2 \log_2(\xi^2 x^2))$. The Schmidt projection methods obtains this bound (section 6.5).

13. For $N \to \infty$ collective distillation is always more efficient than single particle distillation, whereas for $N < 5$ the situation is reversed. For $5 \leq N < \infty$ it depends on x and N whether single or collective distillation has the highest efficiency (section 6.6).

14. Above bipartite teleportation and distillation of qubits or qudits was considered. Generalization is possible in several ways:

    - With a tripartite state controlled teleportation is possible: Alice can teleport a quantum state to Bob if controller Charlie cooperates. With a perfect GHZ state fidelity 1 teleportation can occur with certainty, while with a perfect W state fidelity 1 teleportation can be achieved only in with a fraction of $\frac{2}{3}$. A general tripartite state can be used for probabilistic teleportation.
    - Continuous variables can be teleported using a teleportation protocol analogous to the discrete case.
    - In chain teleportation error self-correction can be used to increase the success probability of the whole teleportation process.

15. The ‘ultimate’ application of the theory considered in this thesis is the establishment of a global quantum communication network. ESA’s Space-QUEST experiment is designed as a first step in this direction by creating a space-ground quantum communication link. The experiment has been positively evaluated in two successive ESSC evaluations of ESA’s ELIPS programme. Currently the required hardware is brought to TRL3, launch is envisioned for 2015 (section 8.1).

16. On macroscopic, even universal scales entanglement plays a crucial role during inflation (section 8.2):

    - The inflaton field causes energy and metric fluctuations. Initially these have a quantum character, but the observed fluctuations are fitted excellently by a classical distribution, so somewhere during inflation a quantum to classical transition occurred.
    - In literature it is generally assumed that the quantum to classical transition occurred when the size of a mode reached the size of the cosmic horizon. As can be seen from the models discussed in this section, the situation is more complicated and model dependent; in some models the quantum to classical transition occurs a thousand times faster than the time the mode needs to grow to horizon size.
    - There are several ways to model the quantum to classical transition during inflation, the details of the model depend on the assumed cause of wave function collapse. If observations are sensitive enough, it might be possible to distinguish between different models. Since wave function collapse is directly connected to the macro-objectivation problem, the inflationary quantum to classical transition provides us with the unique opportunity to gain some experimental insight on a domain of quantum mechanics considered to be purely philosophical!

APPENDIX A
THESIS RELATED ACTIVITIES

Besides this thesis, I was involved in several thesis related activities. This appendix gives an overview of these activities: (i) a summer school, (ii) peer reviews, (iii) language courses (iv) a quantum information theory course and (v) a popular scientific publication.

USEQIP

The *Institute for Quantum Computing* of the *University of Waterloo*, Toronto, Canada, organized the *Undergraduate School on Experimental Quantum Information Processing* (USEQIP), a two week intensive summer school on the theory and experimental study of quantum information processing. The Insitute for Quantum Computing is a leading institute within the field of quantum information processing and consequently we had lectures of famous scientists within the field, like Nobel Laureate Sir Anthony Leggett, director Raymond Laflamme and MIT professor David Cory. The two weeks of the summer school were extremely interesting: the entire field was reviewed both theoretically and experimentally. A printout of the schedule of events is included below.

Peer reviews

On request of prof. dr. Gisin I peer reviewed three manuscripts for the *European Physics Journal D*. The manuscripts I reviewed are:

- *Chain teleportation via partially entangled states*. The manuscript was interesting, but had to be revised on certain relevant parts. The authors revised the manuscript thoroughly and after revision I suggested to publish the manuscript. The manuscript was published in July 2009 [102].

- *Probabilistic teleportation via a non-maximally entangled GHZ state*. I advised to publish a revised version of the article only if the authors could convincingly argue that their teleportation protocol described in their manuscript is really different from protocols which are already published. Based on my review, the manuscript was rejected.

- *W state, GHZ state, Teleportation and Bell's inequality*. The quality of the research in the manuscript was marginal and the article contained quite some errors and I advised to publish the manuscript only after major revisions. The authors revised the manuscript significantly and after a second review and subsequent corrections I considered the article ready for publication. The manuscript was published in January 2010 [25].

Language courses

Geneva is located in French speaking part of Swiss and the Université de Genève is the only French-language university in the country. Perhaps due to this, French still plays a relatively important role in the university. To improve my French I took two French language courses for Erasmus students, offered by the university: (i) *Français Élémentaire* and (ii) *Français Intermédiaire 1 - Oral*. I passed the exams for both courses successfully, their combined equivalent value is 4 ECTS. A copy of the testimony is included below.

Quantum information theory course

Prof. dr. Gisin gives a course on quantum information theory. The course started in september and went on until June. Halfway of March, the topics became interesting for my thesis so I attended the last third of the lectures and exercise classes.

Popular scientific publication

A shortened and non-technical summary of this thesis has been published in the Periodiek of April 2010 [67]. A copy of the article is included below.

BIBLIOGRAPHY

[1] Quantum computing and quantum communications. In Colin P. Williams, editor, *Lecture Notes in Computer Science*, 1998. First NASA International Conference, QCQC'98, Palm Springs, California, USA.

[2] Testing the speed of 'spooky action at a distance'. *Nature*, 454:861–864, Aug 2008.

[3] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach. Generalized schmidt decomposition and classification of three-quantum-bit states. *Phys. Rev. Lett.*, 85(7):1560–1563, Aug 2000.

[4] Pankaj Agrawal and Arun K. Pati. Probabilistic quantum teleportation. *Physics Letters A*, 305(1-2):12 – 17, 2002.

[5] David Z. Albert and Rivka Galchen. A quantum threat to special relativity. *Scientific American*, 300:32–39, Mar 2009.

[6] Josep Maria Perdigues Armengol, Bernhard Furch, Clovis Jacinto de Matos, Olivier Minster, Luigi Cacciapuoti, Martin Pfennigbauer, Markus Aspelmeyer, Thomas Jennewein, Rupert Ursin, Tobias Schmitt-Manderbach, Guy Baister, John Rarity, Walter Leeb, Cesare Barbieri, Harald Weinfurter, and Anton Zeilinger. Quantum communications at esa: Towards a space experiment on the iss. *Acta Astronautica*, 63(1-4):165 – 178, 2008. Touching Humanity - Space for Improving Quality of Life. Selected Proceedings of the 58th International Astronautical Federation Congress, Hyderabad, India, 24-28 September 2007.

[7] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49(2):91–94, Jul 1982.

[8] Somshubhro Bandyopadhyay. Teleportation and secret sharing with pure entangled states. *Phys. Rev. A*, 62(1):012308, Jun 2000.

[9] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D. J. Wineland. Deterministic quantum teleportation of atomic qubits. *Nature*, 429:737–739, 2004.

[10] Jacob D. Bekenstein. Generalized second law of thermodynamics in black-hole physics. *Phys. Rev. D*, 9(12):3292–3300, Jun 1974.

[11] J.S. Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3):195–200, 1964.

[12] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53(4):2046–2052, Apr 1996.

[13] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[14] Charles H. Bennett and David P. DiVincenzo. Quantum information and computation. *Nature*, 404:247–255, March 2000.

[15] Niels Bohr. Can quantum mechanical description of reality be considered complete? *Physical Review*, 48:696–702, Oct 1935.

[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. *Phys. Rev. Lett.*, 80(6):1121–1125, Feb 1998.

[17] S. Bose, V. Vedral, and P. L. Knight. Purification via entanglement swapping and conserved entanglement. *Phys. Rev. A*, 60(1):194–197, Jul 1999.

[18] Raphael Bousso. The holographic principle. *Rev. Mod. Phys.*, 74(3):825–874, Aug 2002.

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

[20] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Observation of three-photon greenberger-horne-zeilinger entanglement. *Phys. Rev. Lett.*, 82(7):1345–1349, Feb 1999.

[21] Warwick P. Bowen, Nicolas Treps, Roman Schnabel, and Ping Koy Lam. Experimental demonstration of continuous variable polarization entanglement. *Phys. Rev. Lett.*, 89(25):253601, Dec 2002.

[22] Gilles Brassard, Pawel Horodecki, and Tal Mor. Telepovm - a generalized quantum teleportation scheme. *IBM J. Res. & Dev.*, 48(1):87–97, Jan 2004.

[23] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77(2):513–577, Jun 2005.

[24] S.L. Braunstein and H.J. Kimble. A posteriori teleportation. *Nature*, 394:840–841, Aug 1998.

[25] I. Chakrabarty. Teleportation via a mixture of a two qubit subsystem of a n-qubit w and ghz state. *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics*, 57:265–269, 2010. 10.1140/epjd/e2010-00017-8.

[26] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, Oct 1969.

[27] Adolfo De Unánue and Daniel Sudarsky. Phenomenological analysis of quantum collapse as source of the seeds of cosmic structure. *Phys. Rev. D*, 78(4):043510, Aug 2008.

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

[29] Prof. dr. Gisin. Université de genève, May 2009. Personal communication.

[30] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, Nov 2000.

[31] P.H. Eberhard. Bell's theorem and the different concepts of locality(*).

[32] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum mechanical description of reality be considered complete? *Physical Review*, 47:777–780, May 1935.

[33] J. Eisert and D. Gross. *Lectures on Quantum Information*, chapter Multiparticle entanglement. Wiley Interscience, 2006. ISBN: 978-3-527-40527-5.

[34] Dr. Joseph Emmerson. Institute for quantum computing, Jun 2009. USEQIP lecture 'review quantum mechanics'.

[35] Richard P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21(6–7):467–488, Jun 1982.

[36] Arthur Fine. The einstein-podolsky-rosen argument in quantum theory. In *Stanford Encyclopedia for Philosophy*. 2004. http://plato.stanford.edu.

[37] European Science Foundation. Scientific perspectives for esa's future programme in life and physical sciences in space. Technical report, May 2005. ESSC-ESF recommendations.

[38] European Science Foundation. Scientific evaluation and future priorities of esa's elips programme. Technical report, Feb 2008. Report from the Sasbachwalden Workshop.

[39] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional Quantum Teleportation. *Science*, 282(5389):706–709, 1998.

[40] Ting Gao, FengLi Yan, and YouCheng Li. Optimal controlled teleportation via several kinds of three-qubit states. *Science in China Series G: Physics, Mechanics and Astronomy*, 51(10):1529 – 1556, 2008.

[41] Marco Genovese. Cosmology and entanglement. *Advanced Science Letters*, pages 303–309, 2009.

[42] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402, Nov 1999.

[43] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, Jul 1997.

[44] H Haffner, W. Hansel, C.F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Korber, U.D. Rapol, M. Riebe, P.O. Schmidt, C. Becher, W. Guhne, W Dur, and R. Blatt. Scalable multiparticle entanglement of trapped ions. *Nature*, 438:643–646, December 2005.

[45] E. Hagley, X. Maître, G. Nogues, C. Wunderlich, M. Brune, J. M. Raimond, and S. Haroche. Generation of einstein-podolsky-rosen pairs of atoms. *Phys. Rev. Lett.*, 79(1):1–5, Jul 1997.

[46] Dr. Lucien Hardy. Center for quantum computation, oxford. Lecture 3, chapter 9: concentrating entanglement.

[47] N. Herbert. Flash - a superluminal communicator based upon a new kind of quantum measurement. *Foundations of physics*, 12:1171–1179, 1982.

[48] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1–8, Nov 1996.

[49] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60(3):1888–1898, Sep 1999.

[50] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. ‘‘event-ready-detectors’’ bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71(26):4287–4290, Dec 1993.

[51] Jietai Jing, Jing Zhang, Ying Yan, Fagang Zhao, Changde Xie, and Kunchi Peng. Experimental demonstration of tripartite entanglement and controlled dense coding for continuous variables. *Phys. Rev. Lett.*, 90(16):167903, Apr 2003.

[52] Jaewoo Joo and Young-Jai Park. Comment on ‘teleportation of an unknown state byw states’: [phys. lett. a 296 (2002) 161]. *Physics Letters A*, 300(2-3):324 – 326, 2002.

[53] Rainer Kaltenbaek, Markus Aspelmeyer, Thomas Jennewein, Caslav Brukner, Anton Zeilinger, Martin Pfennigbauer, and Walter R. Leeb. Proof-of-concept experiments for quantum physics in space. volume 5161, pages 252–268. SPIE, 2004.

[54] Anders Karlsson and Mohamed Bourennane. Quantum teleportation using three-particle entanglement. *Phys. Rev. A*, 58(6):4394–4400, Dec 1998.

[55] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007. ISBN: 9780198570493.

[56] E.H. Kennard. Zur quantenmechanik einfacher bewegungstypen. *Zeitschrift fr Physik A Hadrons and Nuclei*, 44:326–352, 1927.

[57] N.P. Landsman. When champions meet: rethinking the bohr-einstein debate. *Studies in the History and Philosophy of Modern Science*, 37:212–242, 2006.

[58] Sir Anthony J. Leggett. Is quantum mechanics the whole truth?, Jun 2009. USEQIP lecture.

[59] De-Chao Li and Zhong-Ke Shi. Probabilistic teleportation via entanglement. *Int. J. Theor. Phys.*, 47:2645–2654, Jan 2008.

[60] Wan-Li Li, Chuan-Feng Li, and Guang-Can Guo. Probabilistic teleportation and entanglement matching. *Phys. Rev. A*, 61(3):034301, Feb 2000.

[61] Seth Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, Aug 1996.

[62] Hoi-Kwong Lo and Sandu Popescu. Concentrating entanglement by local actions: Beyond mean values. *Phys. Rev. A*, 63(2):022301, Jan 2001.

[63] Dr. Owen Marony. University of sydney, perimeter institute, Jun 2009. Personal communication.

[64] Tal Mor. 'telepovm' - more faces of teleportation. quant-ph/9608005v1, 1996.

[65] Tal Mor and Pawel Horodecki. Teleportation via generalized measurements, and conclusive teleportation. quant-ph/9906039v1, 1999.

[66] Yasusada Nambu. Entanglement of quantum fluctuations in the inflationary universe. *Phys. Rev. D*, 78(4):044023, Aug 2008.

[67] Keimpe Nevenzeel. Spooky action at spacy distances. *Periodiek*, 2:28–31, Apr 2010.

[68] M.A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, 1998:52–55, 1998.

[69] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2003. ISBN: 0521635039.

[70] Travis Norsen. Against realism. *Foundations of Physics*, 37:311–340, 2007. 10.1007/s10701-007-9104-1.

[71] S. Olmschenk, D.N. Matsukevich, P. Maunz, D. Hayes, L.M. Duan, and C. Monroe. Quantum teleportation between distant qubits. *Science*, 323:486–489, Jan 2009.

[72] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: Entangling photons that never interacted. *Phys. Rev. Lett.*, 80(18):3891–3894, May 1998.

[73] Asher Peres. Neumark's theorem and quantum inseparability. *Foundations of Physics*, 20:1441–1453, 1990. 10.1007/BF01883517.

[74] Asher Peres. *Quantum Theory: concepts and methods*, volume 72 of *Fundamental theories of physics*. Kluwer Academic Publishers, 1995. ISBN: 0792325494.

[75] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, Aug 1996.

[76] Alejandro Perez, Hanno Sahlmann, and Daniel Sudarsky. On the quantum origin of the seeds of cosmic structure. *Classical and Quantum Gravity*, 23(7):2317, 2006.

[77] Dr. Marco Piani. Institute for quantum computing, Jun 2009. USEQIP lecture on entanglement and entanglement measures.

[78] S. Pirandola and S. Mancini. Quantum teleportation with continuous variables: A survey. *Laser Physics*, 16(10):1418 – 1438, Oct 2006.

[79] Martin B. Plenio and Shashank Virmani. An introduction to entanglement measures. quant-ph/0504163v3, 2006.

[80] John Preskill. Quantum computation, 1998. Lecture notes for ph219/cs219.

[81] M. Riebe, H. Hffner, C. F. Roos, Benhelm J. Hänsel, W. and, G. P. T. Lancaster, T. W. Körber, Becher C., F. Schmidt-Kaler, D. F. V. James, and R. Blatt. Deterministic quantum teleportation with atoms. *Nature*, 429:734–737, Jun 2004.

[82] M.A. Rowe, D. Kielpinski, , V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland. Experimental violation of bell's inequality with efficient detection. *Nature*, 409:791–794, Feb 2001.

[83] C.A. Sackett, D. Kielpinski, B.E. King, C. Langer, V. Meyer, C.J. Myatt, M. Rowe, Q.A. Turchette, W.M. Itano, D.J. Wineland, and C. Monroe. Experimental entanglement of four particles. *Nature*, 404:256–259, Mar 2000.

[84] Tobias Schmitt-Manderbach, Henning Weier, Martin Furst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[85] Benjamin Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54(4):2614–2628, Oct 1996.

[86] Benjamin Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Phys. Rev. A*, 54(4):2629–2635, Oct 1996.

[87] Alessio Serafini, Fabrizio Illuminati, and Silvio De Siena. Symplectic invariants, entropic measures and correlations of gaussian states. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 37(2):L21, 2004.

[88] Bao-Sen Shi and Akihisa Tomita. Reply to 'comment on: Teleportation of an unknown state by wstate': [phys. lett. a 300 (2002) 324]. *Physics Letters A*, 300(4-5):538 – 539, 2002.

[89] Bao-Sen Shi and Akihisa Tomita. Teleportation of an unknown state by w state. *Physics Letters A*, 296(4-5):161 – 164, 2002.

[90] Peter W. Shor. Algorithms for quantum computation:discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, 1994.

[91] Dr. Christoph Simon. Gap optique, université de genève, May 2009. Quantum information theory lecture 'Quantum repeaters'.

[92] R. Simon. Peres-horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84(12):2726–2729, Mar 2000.

[93] R. Simon, N. Mukunda, and Biswadeb Dutta. Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. *Phys. Rev. A*, 49(3):1567–1583, Mar 1994.

[94] Marco Spaans. The role of information in gravity. *Arxiv.org*, Jul 2009. http://arxiv.org/abs/0903.4315.

[95] D. N. Spergel, R. Bean, O. Dore, M. R. Nolta, C. L. Bennet t, J. Dunkley, G. Hinshaw, N. Jarosik, E. Komatsu, L. Page, H. V. Peiris, L. Verde, M. Halpern, R. S. Hill, A. Kogut, M. Limon, S. S. Meyer, N. Odegard, G. S. Tucker, J. L. Weiland, E. Wollack, , and E. L. Wright. Three-year wilkinson microwave anisotropy probe (wmap) observations: Implications for cosmology. *The Astrophysical Journal Supplement Series*, 170(2):377–408, 2007.

[96] John D. Trimmer. The present situation in quantum mechanics: a translation of schrödinger's cat paradox paper. *Proceedings of the American Philosophical Society*, 124:323–338, Oct 1980. Translation of Schrödingers three-part 1935 paper in Naturwissenschaften 23, pp. 807–812; 823–929; 844–849.

[97] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lutkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger. Space-quest, experiments with quantum entanglement in space. *Europhysics News*, 40(3):26–29, may 2009.

[98] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature physics*, pages 481–486, Jul 2007.

[99] Erik P. Verlinde. On the origin of gravity and the laws of newton. *Arxiv.org*, Jan 2010. http://arxiv.org/abs/1001.0785/.

[100] Guifré Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83(5):1046–1049, Aug 1999.

[101] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between space and earth. *New Journal of Physics*, 10(3):033038 (12pp), 2008.

[102] M. Y. Wang and F. L. Yan. Chain teleportation via partially entangled states. *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics*, 54:111–114, 2009. 10.1140/epjd/e2009-00159-8.

[103] Meiyu Wang and Fengli Yan. Chain teleportation via partially entangled states. *European Physics Journal D*. In press.

[104] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of bell's inequality under strict einstein locality conditions. *Phys. Rev. Lett.*, 81(23):5039–5043, Dec 1998.

[105] J. Williamson. On the algebraic problem concerning the normal forms of linear dynamical systems. *Am J Math*, 58:141–163, 1936.

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

[107] Hidehiro Yonezawa, Takao Aoki, and Akira Furusawa. Demonstration of a quantum teleportation network for continuous variables. *Nature*, 431:430–433, Sep 2004.

[108] A. Zee. *Quantum field theory in a nutshell*. Princeton University Press, 2003. ISBN: 0691010196.

[109] Zhi Zhao, Yu-Ao Chen, An-Ning Zhang, Tao Yang, Hans J. Briegel, and Jian-Wei Pan. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature*, 430:54–57, 2004.

USEQIP
JUNE 1-12, 2009

USEQIP: Undergraduate School on Experimental Quantum Information Processing

June 1-12, 2009

IQC Institute for Quantum Computing

Schedule of Events

**Tentative Schedule*

Monday, June 1st

9:00	Coffee
9:30	Intro to Quantum Information Processing (QIP) (Mosca)
11:00	Break
11:30	Review Linear Algebra & Matlab (Emerson)
12:30	Lunch
1:30	Explore QD (Cory)
3:30	Coffee
4:00	Review Quantum Mechanics (Emerson)
6:00	Dinner

Tuesday, June 2nd

9:00	Coffee
9:30	Intro to Nuclear Magnetic Resonance (NMR) 1 (Baugh)
11:00	Break
11:30	NMR Experiment (Baugh)
12:30	Lunch / IQC
1:30	NMR Experiment A1-A2 / Detector Experiment B1-B2 (Majedi)
3:30	Coffee
4:00	NMR 2 Students / Detector Experiment
6:00	Dinner

Wednesday, June 3rd

9:00	Coffee
9:30	NMR / QIP (Cory)
11:00	Break
11:30	Spinor
12:30	Lunch

1:30	NMR Experiment Students B1-B2 / Detector Experiment A1-A2 (Majedi)
3:30	Coffee
4:00	NMR 2 Students / Detector Experiment
6:00	Dinner

Thursday, June 4th

9:00	Coffee
9:30	Optics (Resch)
11:00	Break
11:30	Optics (Resch)
12:30	Lunch / IQC
1:30	Optics Experiment B1-B2 / A1-A2
3:30	Coffee
4:00	Optics Experiment
6:00	Dinner

Friday, June 5th

9:00	Coffee
9:30	Bell
11:00	Break
11:30	Optics Experiments
12:30	Lunch
1:30	Optics Experiments A1-A2 / B1-B2
3:30	Coffee
4:00	Optics Experiment
6:00	TBD

Monday, June 8th

9:00	Coffee
9:30	Quantum Cryptography (Lütkenhaus/Jennewein)
11:00	Break
11:30	Quantum Cryptography (Lütkenhaus/Jennewein)
12:30	Lunch
1:30	QKD Hands-on Experiment (Lütkenhaus/Jennewein)
3:30	Coffee
4:00	QKD Hands-on Experiment (Lütkenhaus/Jennewein)
6:00	Dinner

Tuesday, June 9th

9:00	Coffee

9:30	QEC (Laflamme)
11:00	Break
11:30	QEC (Laflamme)
12:30	Lunch
1:30	Optics B1-B2 / A1-A2
3:30	Coffee
4:00	Optics
7:00	Dinner at Perimeter Institute

Wednesday, June 10th

9:00	Coffee
9:30	Quantum Algorithms (Mosca)
11:00	Break
11:30	Quantum Algorithms (Mosca)
12:30	Lunch
1:30	TBD
3:30	Coffee
4:00	Talk by Marco Piani
6:00	Dinner

Thursday, June 11th

9:00	Coffee
9:30	Intro to Superconducting Qubits (Lupascu)
11:00	Break
11:30	Undergrad Symposium
12:30	Lunch
1:30	Fabrication Facility (Logiudice)
3:30	Coffee
4:00	Lecture by Anthony J. Leggett
6:00	Dinner
	QKD Demo/Experiment (Erven)

Friday, June 12th

9:00	Coffee
9:30	Foundations (Emerson)
11:00	Break
11:30	TBD
12:30	Lunch
1:30	Lucien Hardy - Perimeter Institute

Page Top

UNIVERSITÉ
DE GENÈVE
FACULTÉ DES LETTRES
Ecole de langue
et de civilisation françaises
Ligne directe: 022 379 74 36

Genève, le 15 juin 2009

ATTESTATION

La direction de l'Ecole de langue et de civilisation françaises de l'Université de Genève certifie que

Keimpe NEVENZEEL

a participé régulièrement durant le semestre de printemps 2009 aux Cours d'appui linguistique pour étudiants non francophones, à raison de 2 cours de deux heures par semaine chacun.

Les résultats obtenus sont les suivants :

Oral, niveau intermédiaire 1

Note de semestre	4
Crédits obtenus :	2

Français élémentaire débutant

Note de semestre	5
Crédits obtenus :	2

Indication du volume de travail en crédits ECTS : 4

La présente attestation est délivrée pour servir et valoir ce que de droit.

Laurent Gajo
Directeur de l'ELCF

Système de notation de l'Université de Genève ; échelle de notation : 6 à 0 (6= excellent 4= note de passage 0 = nul)
Intermédiaire 1
Cet enseignement correspond aux **niveaux A2-B1** dans le Cadre européen commun de référence pour les langues CECR
Intermédiaire 2
Cet enseignement couvre les **niveaux B1-B2** dans le Cadre européen commun de référence pour les langues CECR
Avancé
Cet enseignement correspond aux **niveaux B2-C1+** dans le Cadre européen commun de référence pour les langues CECR
Débutant
Cet enseignement correspond au **niveau A1** dans le Cadre européen commun de référence pour les langues CECR

Uni Bastions – Case postale – CH-1211 Genève 4
Tél. 022 379 74 33 - Fax 022 379 76 81 www.unige.ch/lettres/elcf - elcf@unige.ch

Spooky action at spacy distances

DOOR **KEIMPE NEVENZEEL**

In 1935 stelde Einstein een paradox op met drie mogelijke oplossingen: (i) de kwantummechanica is een onvolledige theorie; (ii) de natuurkunde geeft geen beschrijving van de werkelijkheid, maar alleen een wiskundig formalisme om meetuitkomsten te voorspellen en (iii) bepaalde effecten kunnen sneller reizen dan het licht.

De oplossing van deze paradox leidde tot fundamenteel nieuw inzicht in de natuur en technische toepassingen van de oplossing zullen de digitale wereld revolutioneren. Toepassingen van de oplossing door ESA en NASA in satellieten zorgen er misschien zelfs een tweede keer voor dat ons beeld van de natuur grondig moet worden herzien.

Bohr versus Einstein

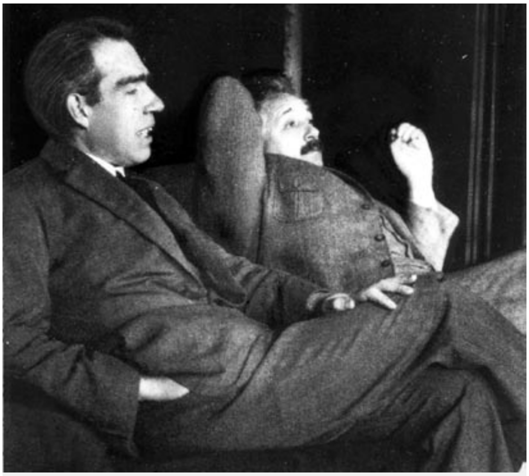
Kwantummechanica is bizar. Iedereen die een gevorderde introductie in deze richting van de natuurkunde heeft gehad zal dit beamen. Deeltjes zijn eigenlijk waarschijnlijkheidsgolven en grote groepen deeltjes vormen interferentiepatronen (ook als je de deeltjes één voor één afschiet), en zo heb je nog meer intrigerende concepten.

Wat moet je van al deze tegenintuïtieve aspecten denken? Niels Bohr, een van de vaders van de kwantummechanica, was geheel overtuigd van zijn theorie. In zijn ogen luidde de theorie een nieuw tijdperk voor de wetenschap in, niet alleen in fysisch maar ook in filosofisch opzicht. Het oude ideaal van de natuurkunde als beschrijving van een objectieve werkelijkheid was achterhaald. Fenomenologische wetten, wetten die waarnemingen wiskundig goed beschrijven maar niet op een fundamentele manier verklaren, zouden het hoogst haalbare zijn. Een van zijn voornaamste tegenstanders was niemand minder dan Albert Einstein, die tot zijn dood bleef geloven dat natuurkunde wel degelijk fundamenteel inzicht geeft over de objectieve werkelijkheid. De tegenintuïtieve en probabilistische aspecten van de kwantummechanica dichtte hij toe aan onvolledigheid. Een nog te ontdekken uitgebreidere versie van de kwantummechanica zou deze vreemde aspecten wel vanuit fundamentelere principes verklaren. De status van de kwantummechanica was een geregeld terugkerend onderwerp in lange discussies tussen Bohr en Einstein.

De EPR-paradox

Het intellectuele gevecht tussen Bohr en Einstein duurde jaren en bereikte een hoogtepunt in een beroemd artikel geschreven door Einstein, Podolsky en Rosen uit 1935 waarin ze de ‘EPR-paradox’ introduceren. In dat artikel was hun gedachtegang ongeveer als volgt: beschouw een molecuul bestaande uit twee gekoppelde atomen A en B, beiden met spin $\pm\frac{1}{2}$, zodanig dat het molecuul als geheel spin 0 heeft. Dus als de spin van deeltje A gemeten wordt, is de spin van deeltje B ook bekend (min de spin van deeltje A).

Vervolgens worden de atomen uit elkaar gehaald en naar de ver van elkaar verwijderde waarnemers Alice en Bob gebracht, dit alles zonder de spins te verande-



FIGUUR 1 Bohr en Einstein in discussie

ren. Als Alice de x-spin van haar deeltje zou meten is instantaan ook de x-spin van Bobs deeltje bekend (namelijk min de x-spin van deeltje A). Hetzelfde geldt voor de y- en z-component. Deeltje B verandert instantaan door meting van deeltje A, en omdat de deeltjes ver uit elkaar liggen lijkt het er dus op dat in de deeltjes informatie over alledrie de spin-componenten ligt opgeslagen. Immers: een signaal van deeltje A naar B met "pssst, ik ben gemeten in de x-richting met uitkomst spin-up, word snel spin-down in de x-richting" kost tijd, terwijl de verandering instantaan was.

Klassiek is dat geen probleem: alle spin-componenten kunnen tegelijkertijd bekend zijn en de deeltjes kunnen dus van te voren een spin-waarde in een bepaalde richting hebben afgesproken. Kwantummechanisch ontstaat wel een probleem: de verschillende spin-componenten commuteren niet en kunnen dus niet alle tegelijkertijd bepaald zijn! Toch laten metingen zien dat Bobs deeltje altijd de tegenoverstelde waarde van Alice' deeltje aanneemt. Ziehier de paradox: bij meting van Alice' deeltje nemen de onbepaalde spin-componenten van Bobs onverstoorde deeltje toch spontaan een bepaalde waarde aan.

De paradox kan op verschillende manieren worden opgelost:

1. Bohrs oplossing: er is geen paradox. In de klassieke natuurkunde kan een onbepaalde eigenschap inderdaad niet spontaan een bepaalde eigenschap met een specifieke waarde worden, maar blijkens de experimenten kan dat in de kwantummechanica wel. Dit zegt niets over de werkelijkheid achter de kwantummechanica, want de kwantummechanica geeft slechts een wiskundige beschrijving van metingen en niet een beschrijving van de werkelijkheid.
2. Einsteins oplossing: de kwantummechanica is incompleet, een uitgebreidere versie van de kwantummechanica kan wel een verklaring geven.
3. De 'niet-lokale' oplossing: het deeltje van Bob verandert daadwerkelijk instantaan door Alice' meting.

Bohr en Einstein zouden het gedurende hun leven nooit eens worden, maar over één ding waren ze het

Kwantummechanica

De kwantummechanica beschrijft de natuur op atomaire schaal en kleiner. Drie kenmerkende aspecten van de kwantummechanica zijn:

1. Alle eigenschappen van fysische objecten worden beschreven door waarschijnlijkheidsgolven, die golffuncties worden genoemd. De positie-golffunctie van een proton geeft bijvoorbeeld de waarschijnlijkheid dat het proton zich op een bepaalde plaats bevindt.
2. Meting van een eigenschap zorgt ervoor dat de golffunctie van die eigenschap ineen stort tot een delta-functie. Als bijvoorbeeld wordt gemeten dat de positie van het proton a is, dan verandert de positie-golffunctie in een delta-functie op a.
3. Heisenbergs onzekerheidsprincipe: twee waarneembare eigenschappen die niet commuteren kunnen niet tegelijkertijd volledig bekend zijn. Een voorbeeld hiervan zijn positie x en impuls p. Noteer de onzekerheid in beiden met Δx en Δp, dan geldt $\Delta x \cdot \Delta p \geq \frac{1}{4\pi}h$, met h de constante van Planck. Als de positie van een deeltje dus heel precies bepaald wordt, dan wordt de impuls geheel onbepaald.

De kwantummechanica heeft zware experimentele verificatie doorstaan en wordt dus als betrouwbare theorie gezien, maar op fundamenteel niveau zijn er belangrijke vragen. Eén hiervan is wat ineenstorting van de golffunctie precies betekent: is de ineenstorting slechts een wiskundige beschrijving, of is er een echte fysische interpretatie (zo ja, wat dan?). Experimenten die de kwantummechanica over grote afstanden testen kunnen hier misschien nieuwe inzichten geven.

Spin

De spin van een deeltje is min of meer de rotatie van het deeltje om zijn eigen as. Elementaire deeltjes hebben een karakteristieke spin, zo hebben elektronen spin $\pm\frac{1}{2}$ en fotonen ± 1, waarbij we plus spin-up en min spin-down noemen. De absolute waarde van de spin van een deeltje kan niet veranderen, maar het teken wel. Een deeltje heeft drie spin-componenten: de x-, y- en z-component, die elk spin-up of spin-down kunnen zijn.

Kwantummechanisch blijken de verschillende spin-componenten niet te commuteren! Effectief betekent dit dat als met een meting één van de spin-componenten wordt bepaald, de andere spincomponenten geheel onbepaald zijn.

wel eens: *spooky action at a distance*, zoals Einstein de derde oplossing noemde, diende verworpen te worden. Instantane veranderingen lijken in directe tegenspraak met de speciale relativiteitstheorie.

Nature is spooky

Pogingen Einsteins paradox op te lossen leidde in 1982 tot een revolutie in ons begrip van de natuur: er werd experimenteel aangetoond dat 'spooky action at a distance' wel mogelijk is! Kwantummechanische bewerkingen kunnen twee deeltjes zo aan elkaar koppelen dat ze verstrengeld (*entangled*) raken. De golffunctie van een van de deeltjes kan dan nog alleen volledig worden beschreven door ook de golffunctie van het andere deeltje te beschrijven. Verstrengeling betekent in feite dat de natuurkundige eigenschappen van de deeltjes (bijvoorbeeld spin) sterkere correlaties vertonen dan klassiek mogelijk is. Verstrengelde deeltjes kunnen deze sterke correlaties in eigenschappen behouden ongeacht de afstand tussen beide en daarom worden deze correlaties ook wel non-lokale correlaties genoemd.

Kun je met verstrengelde deeltjes sneller dan het licht informatie overdragen? Nee, want hoewel Bobs deeltje instantaan verandert als Alice haar deeltje meet, kan hij deze verandering alleen goed interpreteren met behulp van Alice' meetresultaten. Die meetresultaten moet Alice eerst op een klassieke manier (telefoon, internet, postduif) naar Bob sturen, wat de maximale overdrachtssnelheid van informatie dus beperkt tot de lichtsnelheid.

Van klassieke bit naar qubit?

De sterke correlaties tussen verstrengelde deeltjes bieden ongeëvenaarde mogelijkheden voor dataverwerking. Ter illustratie: de klassieke data-eenheid is de bit, een deeltje dat up (1) of down (0) kan zijn. Een geheugen bestaande uit n klassieke bits kan dus in 2^n verschillende toestanden zijn: 00…00, 00…01, 00…10, …, 11…11.

De kwantumdata-eenheid is de qubit. Noteer up met 1 en down met 0, dan is een qubit een verstrengeld paar deeltjes met golffunctie

$$|\phi\rangle_{AB} = \alpha|10\rangle_{AB} + \beta|01\rangle_{AB},$$

waarbij $\alpha, \beta \in \mathbb{C}$ en $\alpha^2 + \beta^2 = 1$. Een geheugen bestaande uit n qubits heeft als golffunctie

$$|\phi\rangle = \sum_{i=00\ldots0}^{11\ldots1} c_i|x\rangle,$$

met $c_i \in \mathbb{C}$ en $\sum_i c_i^2 = 1$.

Doordat qubits dus in een veel hogere dimensie leven dan de klassieke bits kunnen computers gebaseerd op qubits, kwantumcomputers, bepaalde taken exponentieel sneller uitvoeren: in minuten in plaats van eeuwen. Denk hierbij aan wiskundige algoritmes, zoekalgoritmes en simulaties van kwantumsystemen.

Om echter enigszins voordelen te bieden ten opzichte van een klassieke computer heeft een kwantumcomputer circa vijfitg qubits nodig, terwijl de huidige meest geavanceerde kwantumcomputers nog niet de helft van dit aantal hebben. Er is dus nog wel wat werk aan de winkel.

Scotty, beam me up!

Bij klassieke computers worden voor informatieverwerking bits heen en weer gezonden. Evenzo moeten bij kwantumcomputers voor informatieverwerking kwantumtoestanden worden uitgewisseld. Stel dat Alice en Bob ver van elkaar verwijderd zijn en Alice wil de kwantumtoestand, bijvoorbeeld de spin, van deeltje C aan Bob doorgeven. Ze kan deeltje C zelf sturen, maar er is een grote kans dat de spin door interactie met de omgeving tijdens zijn reis van Alice naar Bob verandert. Ze kan ook de spin meten en deze informatie op klassieke wijze doorgeven, maar omdat de verschillende spin-componenten niet commuteren kan ze nooit een volledige beschrijving van de spin doorgeven. Als Alice en Bob een paar verstrengelde deeltjes A en B delen kunnen ze echter ook de niet-lokale eigenschappen van verstrengeling gebruiken om de kwantumtoestand van C te teleporteren. Hierbij moet je niet meteen aan Star Trek-achtige taferelen denken zoals mensen die direct vanuit een ruimteschip op de grond van een verre planeet belanden, maar aan een wat bescheidener schaal: het overbrengen van de kwantumtoestand van C *zonder* dat de informatie door een foton of een ander deeltje wordt overgedragen.

Naast de overdracht van informatie in kwantumcomputers heeft teleportatie nog een andere belangrijke toepassing: kwantumcryptografie. Een geteleporteerde kwantumtoestand legt nooit fysiek de afstand tussen Alice en Bob af en kan dus ook nooit worden onderschept. Kwantumcryptografie is daarmee de enige vorm van cryptografie waarbij de veiligheid door de wetten van de natuur zelf wordt gegarandeerd!

In tegenstelling tot kwantumcomputers, waarvan op het moment nog alleen prototypes bestaan, is kwantumcryptografie al experimenteel gerealiseerd. Het huidige afstandsrecord in de vrije lucht is 144 kilometer!

Spacy quantum entanglement

Vanwege de grote voordelen van kwantumcryptografie wordt hard nagedacht over het opzetten van een globaal kwantumcommunicatienetwerk. Een belangrijke stap hierin is het mogelijk maken van kwantumcommunicatie via satellieten. Sinds een jaar of vijf besteden ESA en NASA daarom expliciet aandacht aan het ontwikkelen van ruimtewaardige kwantumcommunicatietechnologie. In 2007 begon ESA's Space-QUEST (*QUantum Entanglement for Space experimenTs*) programma, met als doel het installeren van een kwantumcommunicatiemodule aan boord van het ISS. Deze module moet paren verstrengelde fotonen creëren en versturen naar twee ver weg gelegen grondstations, bijvoorbeeld Groningen en Peking. Als beide grondstations één foton van een verstrengeld paar fotonen hebben ontvangen, delen de grondstations een verstrengeld paar en is kwantumcommunicatie tussen beide stations mogelijk! Als alles volgens plan gaat moet de module in 2015 op het ISS geïnstalleerd worden.

Naast gegarandeerd veilige communicatie is er vanuit wetenschappelijke hoek om heel andere redenen interesse in een kwantumcommunicatiemodule in het ISS: het creëert de unieke mogelijkheid om kwantummechanische effecten op grote afstand te testen. Dit geeft wellicht inzicht in enkele openstaande fundamentele problemen van de kwantummechanica zoals het ineenstorten van golffuncties. Einstein gaf een verkeerde oplossing voor zijn paradox, maar zijn paradox an sich heeft wellicht voor de tweede keer grote gevolgen voor ons beeld van de natuur. •

Referenties

- Nielsen, M.A. en Chuang, I.L. "Quantum Computation and Quantum Information." Cambridge University Press, 2000.
- Einstein, A., Podolsky, B. en Rosen, N. "Can quantum-mechanical description of Physical Reality be considered complete?" Phys Rev 47:777-780, 1935.
- Bennett, C.H. et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels." Phys Rev Let 70:1895-9, 1993.
- Ursin, R. et al, "Space-QUEST: Experiments with quantum entanglement in space." Proc. IAC, 2008.