Department of Physics
Faculty of Nuclear Sciences and Physical Engineering

Czech Technical University in Prague

Entanglement and its role in quantum information processing

Author: **Jaroslav Novotný**

Doctoral thesis

Supervisor: **Prof. Ing. Igor Jex, DrSc.**

Prague, 2007

Katedra fyziky
Fakulta jaderná a fyzikálně inženýrská

České vysoké učení technické v Praze

Provázání a jeho úloha v kvantových informačních procesech

Autor: **Jaroslav Novotný**

Disertační práce

Školitel: **Prof. Ing. Igor Jex, DrSc.**

Praha, 2007

Abstract

The thesis presents results of my research in two related areas of quantum information: sharing of entanglement in multi-qubit states - analysis of bipartite entanglement structures carried by quantum states, and the role of entanglement in quantum information processing - optimal copying and complementing of two entangled qubits.

The thesis is structured as follows. Chapter 1 and Chapter 2 are intended to summarize the theory and to introduce basic concepts needed in the subsequent discussions. In Chapter 1 we review the mathematical formalism describing quantum state transformations. Using the concept of quantum operations we define and discuss LOCC and covariant quantum operations. We address problems of cloning and complementing of unknown quantum states and propose a general covariant approach how to optimize this type of state transformations. In Chapter 2, the contemporary state of knowledge on quantum entanglement is presented. We give the needed notions and definitions, recapitulate accessible tools for detecting bipartite entanglement, list several bipartite entanglement measures for pure and mixed states and discuss briefly the problem of multipartite entanglement.

The first topic that will be addressed is bipartite entanglement sharing in multi-qubit states. In the first part of Chapter 3, the concept of entangled graphs for multi-qubit states is introduced and it is proved that a broad set of entangled graphs can be represented by pure quantum states. In the second part we investigate the general structure of entanglement in linear passive optical networks with one and two excitations and specify the result for Ising-type networks. We show how to design a network to prepare a prescribed pattern of entanglement for one excitation and study the maximum attainable entanglement for passive optical networks in general.

Chapter 4 concerns with the role of entanglement in quantum information processing. The first part is devoted to the general problem of copying pure two-qubit states of a given degree of entanglement in an optimal way. Two different figures of merit are considered, local and global fidelity, and for each of them covariant optimal quantum copying operations are constructed. The second part of this chapter deals with complementing two-qubit states of a given degree of entanglement in an optimal way. In the special case of maximally entangled states the general structure of perfect quantum NOT operations is found and using these perfect NOT operations a remote state protocol for two-qubit maximally entangled qubits is proposed. In order to solve the general problem of optimal NOT operations we find the structure of all completely positive

quantum operations which transform two-qubit input states into two-qubit ouptut states in a prescribed covariant way. Using these results, all covariant optimal quantum NOT operations for pure two-qubit states with a given degree entanglement are determined. We propose a physical implementation for all covariant processes, providing the ancillary quantum state and the global master unitary evolution. Moreover, we design a network of quantum gates which is capable of implementing a large variety of covariant two-qubit processes.

Finally, the summary and conclusions are given in Chapter 5.

Declaration

This thesis is the result of my own work, except where explicit reference is made to the work of others and has not been submitted for another qualification to this or any other university.

Acknowledgments

Completing a PhD is truly a marathon event, and I would not have been able to complete this journey without the aid and support of many people. First and foremost, I would like to thank my supervisor, professor Igor Jex, for guiding me during my Ph.D. studies, for his support, numerous suggestions, discussions, comments, and last but not least for numberless readings and corrections of this thesis. My thanks extend to my friends and colleagues at the Department of Physics whom I had the pleasure and privilege to collaborate and discuss my problems: Martin Štefaňák, Vojtěch Košt'ák.

Over the years, I have enjoyed the aid of several projects and collaborations. My special thanks go to professor Gernot Alber for many stimulating and illuminating discussions, for his invaluable insight, and for his invitations and arranging my stays in Germany. I would like to thank members of the research group of professor Vladimír Bužek, especially to Martin Plesch for discussions, the opportunity to collaborate with him and for arranging my visits to Slovakia. I would like to thank also people with who I had the opportunity to discuss problems of quantum information, as Mário Ziman, Stefan Probst-Schendzielorz, Bernd Mohring, Tamas Kiss, Zoltán Kurucz, Erika Anderson, during their visits to Prague.

Finally, my warmest thanks go to my wife and my son for their love and support during my studies.

Contents

Introduction

In the beginning was the Word,
and the Word was with God,
and the Word was God.

WAIT! Is not a word a piece of information? And is it possible to treat information in an abstract way without any reference to a physical object? Can we consider information to be stand-alone, being completely independent on physical reality? From the physical point of view to operate information is to operate physical systems, and vice versa. In fact, we realize that any information is encoded, processed and transmitted by physical means. *Information is physical* because it is always encoded on or carried by a physical system. The deep connection between physics and information is often demonstrated on the paradox often called Maxwell demon. Maxwell introduced a very small intelligent being to show the limitation of the second law of thermodynamics [1]. If we admit that the memory content of this being, here an information about a measurement stored in its memory, is nonphysical, we would be hypothetically able to design a machine which transforms all delivered heat to work. How to understand this paradox? The problem really lies in our idea, that information is nonphysical and do not need to be stored in any physical system. In 1961 Rolf Landauer suggested the idea, that the erasure of one bit of information always increases the thermodynamical entropy of the world by $k \ln 2$ [2]. Applying Landauer's principle, Charles Bennett successfully settled the illusive Maxwell paradox [3].

Hence, natural limits for encoding, manipulating and distributing information are given by the very laws of physics. As a natural consequence it appears, that different laws, which dominate in the classical world and the quantum world, result in different properties of information carried by classical and by quantum systems. It uncovers the reasons for so huge interest in the general field of quantum information. Quantum mechanics gives rise to new and often not yet completely understood advantages and restrictions on information sharing, processing and distribution compared to classical. Quantum information theory is devoted to the investigation

of these theoretical privileges and limits, which quantum mechanics establishes when dealing with information encoded in quantum systems. We have to be careful in thinking what is in quantum information possible and what is not. Great effort was invested into understanding the nature of information carried by quantum objects. The development in this area revealed us, that the laws of quantum mechanics impose severe conditions on what types of operations can be realized on unknown quantum states. In other words some common information tasks cannot be realized perfectly in quantum mechanics. This is very often illustrated on the case of copying information. Perfect copies of classical bits are our everyday experience. It took considerable time to find out that this simple operation is impossible in the quantum domain. The so-called "No-cloning theorem" first-time mentioned by W. K. Wootters and W. H. Zurek [4] says that perfect cloning of an unknown single quantum state is forbidden. Similarly, it was shown that there is no linear trace preserving operation that takes two copies of unknown qubit and delete one acting jointly on both two copies. It is also well accepted that a quantum NOT operation, which transform an arbitrary (unknown) pure quantum states into its orthogonal complement, cannot be performed perfectly due to its anti-linear character [5]. Suchlike *no-go* theorems are also known for other elementary tasks of quantum information processing [6]. An impossibility to perform quantum-mechanically some common operation does not mean automatically a disadvantage. For instance, the No-cloning theorem makes secure quantum communication possible. Moreover from a theoretical point of view, the No-cloning theorem precludes superluminal communication in the presence of entanglement.

One of the most striking features of quantum formalism is quantum entanglement. This "main suspect in the cause Quantum information" is a simple consequence of linearity applied to quantum systems consisting of two and more parts. For example if we let interact two separate quantum systems, we will not be able after a certain time, in general, to assign a single state vector to either of the two subsystems. The well-known example of such states is the so called singlet state of two qubits

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle|1\rangle - |1\rangle|0\rangle \right). \tag{1}$$

This state cannot be written as a tensor product of two individual states describing each of the two qubits.

For the first time the strange properties of entanglement were recognized by Einstein, Podolsky and Rosen [7] and Schrödinger [8] in 1935. Let us focus firstly on the contribution of Einstein, Podolsky and Rosen (further we use the abbreviation EPR). In their famous and in physics most cited paper they proposed a thought experiment with the aim to prove that the newborn quan-

tum mechanics is not a complete theory of Nature. The essential idea of the EPR reasoning was the concept of "local realism". It supposes the validity of two natural principles. The first is locality, which claims that if we measure two non-interacting subsystems, the measurement on one subsystem cannot affect the result of measurement on the second system. Hence the manipulation of one subsystem cannot influence distant subsystem instantly. The second principle is reality, which is based on the belief that every measurable observable corresponds to what they termed "elements of reality". Simply expressed, the result of a measurement of any observable is given in advance. The important message for us is that these elements of reality exist independently, whether a measurement was performed or not. Applying the test of local realism on entangled state, EPR demonstrated that quantum mechanics is not, in this sense, a complete theory.

The biggest contribution in the resolution of this enigma belongs to Bell [9]. He also proposed a thought experiment, in which each of two participants (usually called as Alice and Bob) receives a spin particle. Bell showed, that if we apply the requirement of local realism on predictions of spin correlations between Alice's and Bob's particle, we arrive at constraints now well-known as Bell inequalities. This result is independent on whether the particle is a classical object, quantum or something else. The only assumptions are that the value of spin corresponds to some element of reality (result of measurement is given in advance) and that Alice's measurements cannot affects Bob's measurements. The latter assumption can be satisfied by arranging measurements in a causally disconnected manner.

Also in the year 1935, Schrödinger proposed a different approach to the EPR problem based on information capacity of quantum states [8]. He showed that entangled states exhibit a strange information property, namely subsystems of an entangled composite system carry a smaller piece of information than the whole entangled system. For example, in spite of our small or even no knowledge about the subsystems we can still have considerable or even complete knowledge about the whole entangled system.

It was clear that quantum entangled states violate this type of Bell inequalities. The good news was, that using Bell inequalities we are able to decide experimentally, whether quantum mechanics is a local realistic theory or not. Indeed, starting from the year 1972, violations of Bell inequalities were observed in many experimental tests with entangled states [10, 11, 12]. These experiments testified against the general validity of local realism and by contrast brought to light new striking features of information carried by quantum objects (further in our text we use a familiar term quantum information).

From a technological point of view, the primary interest of quantum information theory is to

improve algorithms and find more efficient and secure information protocols based on intrinsic (non-classical) features of quantum mechanics. For a long time it appeared, that entanglement has been only an interesting mathematical vagary and would have no practical consequences and applications. But the development of quantum information in current years have infilled us trust that entanglement can have important practical applications.

One of the first steps on this road and certainly one of the most famous one's was done by Bennett et al. [13]. They discovered a remarkable information protocol called quantum teleportation. In this protocol a sender (usually called as Alice) transmits in general an unknown quantum state to a spatially separated receiver (usually refer to Bob) using only a shared pair of particles in a singlet state (1) and two bits of classical communication. The teleportation protocol did not remain in this development alone. Entanglement plays a pivotal role in various types of quantum information processings like quantum data compression and quantum cryptography. As was already mentioned, most of these theoretical scenarios require the use of entangled subsystems, which are spatially separated. However, only global operations can increase entanglement among subsystems, if the subsystems interact directly with one another or each interacts directly with an intercessory additional party. In either case, to establish entanglement between spatially separated parties, quantum systems have to physically traverse the distance between them.

Unfortunately, it is impossible to prevent some interaction with the environment, which is out of experimenter's control, during this transmission. The uncontrolled intervention leads to a change of the quantum system, which is becoming typically more mixed due entanglement creation with the environment. The state of the system can be viewed as an ensemble of pure states with definite random probabilities. In consequence, this makes a transmitted entangled state useless.

Is there any possibility, how to protect against this unpleasant feature of quantum mechanics? Fortunately, the answer is "yes". The solution to this problem was presented by Bennett et al. [14, 15], Deutsch et al. [16] and Gisin [17], who have proposed a procedure to "distill" maximally entangled states of two qubits out of a set of qubit pairs in certain mixed entangled states by using local operations and classical communication (LOCC). A natural question have arisen, from which types of states are we capable to distill or purify entanglement using only LOCC.

To settle this issue, two kinds of effort have to be made. First, we have to obtain a good insight into the structure of entangled mixed states to be able to decide which state is entangled and which is not. In other words we have to be able to detect entanglement in a given state. The reason is simple, local operations and classical communication cannot turn a non-entangled

state (called separable state) into entangled (inseparable) ones and therefore these states are useless. To find the answer is very difficult. Quantum information theory exposes a fruitful list of methods or criteria. For instance, the Horodecki family proved, that the positive partial transposition (PPT) of density operator is a necessary and sufficient condition for separability of $2 \otimes 2$ and $2 \otimes 3$ systems (so called Peres criterion). However, so far many problems remain open. Second, we have to solve still whether all states can be distilled. Using the PPT criterion, the Horodecki family showed that any entangled state of two qubits or a qubit and qutrit can be distilled into a singlet. Therefore it was supposed and conjectured that all inseparable states are distillable and the proof would be only question of time. Unexpectedly, it was found out, that it has been not true. There are entangled states of two qutrits, for instance, which have positive partial transposition. We call this type of entanglement bound, because in was shown all PPT states cannot be distilled. With respect to this we can naturally ask, whether all states with negative partial transposition are distillable. The completely comprehensive answer to this question is at present unknown.

In spite of these theoretical difficulties, quantum mechanics has offered a new perspective on efficient and secure communication, storage of information and exploration of new kinds of algorithms. Entanglement underlies most of these remarkable applications of newborn quantum information and in itself it has every right to be regard as a physical resource, like for instance energy. In our effort to understand this resource we have to face many problems like detection of entanglement, quantification entanglement, general structure of entanglement, sharing entanglement among different parties, its role in information processes, tradeoff between the other information resources.

Notation

To each quantum system, let say A, a complex separable Hilbert space $\mathscr{H}_A$ is associated, equipped with the inner product $\langle\psi|\phi\rangle$, linear in ϕ and antilinear in ψ. From now on, if not otherwise specified, we will deal with finite complex Hilbert spaces, for which all linear operators are everywhere defined, bounded and trace-class, and the self-adjointness coincides with hermiticity. Moreover, spectral operator resolutions are all discrete, i. e. $X = \sum_j x_j \Pi_j^X$.

The set of linear operators on $\mathscr{H}$ will be denoted as $\mathsf{L}(\mathscr{H})$. Positive semi-definite trace-one operator ρ is called a *state*. We will denote the set of states of a system $\mathscr{H}$ as $\mathsf{S}(\mathscr{H})$. Composite systems carry a tensor-product Hilbert space, $\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \cdots \otimes \mathscr{H}_N$ and we will sometimes use the notation $|\phi_1\rangle|\phi_2\rangle...|\phi_N\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes ... \otimes |\phi_N\rangle$, where $|\phi_i\rangle \in \mathscr{H}_i$. Linear operators $\mathsf{L}(\mathscr{H})$ form themselves a Hilbert space isomorphic to $\mathscr{H}^{\otimes 2} \equiv \mathscr{H} \otimes \mathscr{H}$. If we fix a basis $\mathbf{b} = \{|i\rangle\}$ for $\mathscr{H}$, we define the following isomorphism between operators in $\mathsf{L}(\mathscr{H})$ and vectors in $\mathscr{H}^{\otimes 2}$:

$$X = \sum_{ij} X_{ij}|i\rangle\langle j| \longleftrightarrow |X\rangle\!\rangle \equiv \sum_{ij} X_{ij}|i\rangle \otimes |j\rangle, \tag{2}$$

satisfying

1. $\langle\!\langle X|Y\rangle\!\rangle = \mathrm{Tr}[X^\dagger Y]$, i. e. the Hilbert-Schmidt product;
2. $(X \otimes Y)|Z\rangle\!\rangle = |XZY^T\rangle\!\rangle$, where Y^T denotes the transposition with respect to the fixed basis $\mathbf{b}$;
3. $\mathrm{Tr}_1[|X\rangle\!\rangle\langle\!\langle Y|] = X^T Y^*$, where Y^* denotes the complex conjugation with respect to $\mathbf{b}$;
4. $\mathrm{Tr}_2[|X\rangle\!\rangle\langle\!\langle Y|] = XY^\dagger$.

In this notation the state $|I/\sqrt{d}\rangle\!\rangle$ is the maximally entangled state on $\mathscr{H}^{\otimes 2}$:

$$\frac{1}{\sqrt{d}}|I\rangle\!\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle. \tag{3}$$

In the thesis we will use the following notation:

$\mathbb{C}^d$	= complex vector space with dimension d
$\mathscr{H}$	= Hilbert space $\mathscr{H}$
$\mathscr{H}^d$	= Hilbert space $\mathscr{H}$ with dimension d
$\mathsf{L}(\mathscr{H}_1, \mathscr{H}_2)$	= space of all linear operators mapping the Hilbert space $\mathscr{H}_1$ into the Hilbert space $\mathscr{H}_2$
$\mathsf{L}(\mathscr{H})$	= space of all linear operators mapping the Hilbert space $\mathscr{H}$ into $\mathscr{H}$
$\mathsf{S}(\mathscr{H})$	= convex set of all density operators acting on Hilbert space $\mathscr{H}$
$\mathbb{C}^{n,m}$	= complex space of all complex matrices $n \times m$
$\mathbb{R}^{n,m}$	= real space of all real matrices $n \times m$
A	= operator A
A^T	= transposition of operator A with respect to a given basis
$A^\dagger$	= conjugation of operator A
A^*	= complex conjugation of operator A with respect to a given basis
$\mathrm{Tr}_a\, Q$	= trace of operator Q over the system **a**
$\langle \ldots, \ldots \rangle$	= inner product
$\|\psi\rangle$	= bra vector
$\langle\psi\|$	= ket vector

Chapter 1

Quantum processes

This chapter has several goals. First, it summarizes the theory of quantum operations, secondly, it establishes two particular families of quantum operations: LOCC operations and covariant quantum channels, thirdly, it introduces two classes of maps, which cannot be realized perfectly: quantum copying and quantum NOT operation, and finally, we explain the covariant approach of the optimal approximation of these "non-physical maps".

1.1 Quantum evolution of closed systems

Quantum information is encoded into quantum states. Hence arbitrary manipulations with information are ruled by laws of quantum mechanics. Some counterintuitive features of quantum mechanics can make it difficult to decide what types of information processing may be performed and what is impossible. In order to understand and solve this type of problems we have to clarify which types of state evolution or state changes in time are possible in quantum mechanics. Standard textbooks on quantum mechanics deal mostly with unitary evolution of states combined eventually with measurements performed on these states in closed systems. It supposes, that we know the Hamiltonian operator $H(t)$ of the whole system, which implies complete knowledge of all interactions acting in or on our system. Provided this assumption is fulfilled, this should be the end of the story. The time evolution of a state $|\psi(t)\rangle$ is given by the Schrödinger equation

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

or in the case of mixed state $\rho(t)$ by the Liouville equation

$$i\hbar\frac{\partial\rho(t)}{\partial t} = [H(t), \rho(t)]\,, \tag{1.2}$$

where $[.,.]$ denotes a commutator of two operators A, B defined as $[A,B] = AB - BA$. The only nontrivial problem remains to solve these equations for a given initial state.

Unfortunately, any real system suffers from unwanted interactions with the outside world. Every quantum system is open due to noise. We need to understand and control such noise processes in order to design efficient quantum information systems. The mathematical concept of quantum operations is a suitable tool for describing dynamics in open quantum systems. Further in the text we consider finite dimensional Hilbert spaces, even in cases, in which we could consider more general Hilbert spaces.

1.2 Quantum operations

Quantum operations have wide use in various branches of quantum physics. This is simply due to the fact, that this tool can be used to describe systems both weakly and strongly coupled. In particular, quantum operations are a well adapted tool to describe discrete state changes, i.e. transformations between an input (initial) state ρ_{in} and output (final) state ρ_{out}, without specific reference to the passage of time

$$\rho_{out} = \mathcal{E}\left(\rho_{in}\right), \tag{1.3}$$

where $\mathcal{E}$ denotes a quantum operation. Thus quantum operations serve as a tool to capture the dynamics of state changes.

There are three different, but mutually complement approaches how to view quantum operations. The first approach starts from physically motivated axioms which we expect quantum operations should obey. In this approach, a quantum operation is defined as a map from the set of density operators of the input Hilbert space $\mathscr{H}_1$ to the set of density operators of the output Hilbert space $\mathscr{H}_2$

$$\mathcal{E} : \mathsf{S}\left(\mathscr{H}_1\right) \longrightarrow \mathsf{S}\left(\mathscr{H}_2\right), \tag{1.4}$$

with the following three properties:

a1. The term $\mathrm{Tr}\left[\mathcal{E}(\rho)\right]$ determines the probability that the process represented by the map $\mathcal{E}$ occurs (ρ_{in} is the initial state). Hence the condition $0 \leq \mathrm{Tr}\left[\mathcal{E}(\rho_{in})\right] \leq 1$ has to be fulfilled.

a2. The map $\mathcal{E}$ should be convex-linear on the set of density operators $\mathsf{S}\left(\mathscr{H}_1\right)$

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i \mathcal{E}\left(\rho_i\right), \tag{1.5}$$

where p_i are probabilities summing up to one.

a3. The map $\mathcal{E}$ is completely positive. Each physically allowed transformation has to map density operators, acting on Hilbert space $\mathscr{H}_1$, to density operators, acting on Hilbert space $\mathscr{H}_2$, i.e. the map is positive. Moreover, we require the map $\mathcal{E}$ to be positive with respect to an arbitrary enlargement of our system. In other words, if we introduce an additional system with Hilbert space $\mathscr{H}_{extra}$ of arbitrary dimension, the map $\mathcal{E} \otimes \mathcal{I}$ has to be positive on the convex set of density operators $\mathsf{S}(\mathscr{H} \otimes \mathscr{H}_{extra})$, where $\mathcal{I}$ denotes the identity map acting on $\mathsf{L}(\mathscr{H}_{extra})$ (space of all linear operators mapping the Hilbert space $\mathscr{H}_{extra}$ into Hilbert space $\mathscr{H}_{extra}$).

If $\mathrm{Tr}\left[\mathcal{E}(\rho)\right] = 1$ for all density operators ρ, we call the quantum operation $\mathcal{E}$ trace-preserving (deterministic or channel, depending upon context). Conversely, if this condition is not satisfied, we call the quantum operation non-trace-preserving (probabilistic, stochastic, selective or measuring, also depending upon context). In this case the quantum operation $\mathcal{E}$ does not provide a complete description of the physical process that may occur. It happens if a measurement with different results is part of the physical process. Then a quantum operation corresponds to one output which will occur with certain probability.

A better insight into this problem is given by the second approach, the formalism of Kraus operators. This approach considers a general setting where our principal system, described again by the Hilbert space $\mathscr{H}_1$, evolves through interactions with other quantum ancillary systems (described by Hilbert space $\mathscr{H}_{ancilla}$) in a sequence of three steps:

a) We first add ancillary systems to our system - this ancilla can be environment particles interacting with our system, or additional particles to design some special quantum protocol, etc. (depending on the physical situation which we model).

b) Then we perform joint unitary transformations and measurements on the composite system.

c) Finally, we discard all or some ancillary particles based on the physical situation and the measurement outcomes. We finish with a system described by Hilbert space $\mathscr{H}_2$.

If the ancillary system used in this process is originally uncorrelated with our system then we can described the physical process by so-called Kraus operators [18]. Suppose that we keep complete knowledge of outcomes obtained during measurements. Then the state ρ_i corresponding to measurement outcomes i occurs with probability $p_i = \mathrm{Tr}\left\{E_i \rho_{in} E_i^\dagger\right\}$ and reads

$$\rho_i = \frac{E_i \rho_{in} E_i^\dagger}{\mathrm{Tr}\left\{E_i \rho_{in} E_i^\dagger\right\}}, \tag{1.6}$$

where ρ_{in} is the initial state, i.e. $\rho_{in} \in \mathsf{S}(\mathscr{H}_1)$, and E_i are Kraus operators mapping Hilbert space $\mathscr{H}_1$ into Hilbert space $\mathscr{H}_2$. The probabilities have to sum up to one, therefore the Kraus operators have to fulfil the condition $\sum E_i^\dagger E_i = I$, where I denotes the identity operator on the input Hilbert space $\mathscr{H}_1$. However there is also the possibility that a part or all of the measurement outputs are not accessible. In the most extreme case, which corresponds to physical situation, where all ancillary particles are traced out, the quantum operation is given by

$$\rho_{out} = \sum_i E_i \rho_{in} E_i^\dagger. \tag{1.7}$$

We have formulated two different approaches, how to describe state changes. The following important Choi's theorem [19] shows that both approaches are equivalent.

Theorem 1.2.1 *The map $\mathcal{E} \in \mathsf{L}(\mathscr{H}_1, \mathscr{H}_2)$ satisfies axioms* **a1**,**a2** *and* **a3** *if and only if there is some set of Kraus operators E_i from the input space $\mathscr{H}_1$ to the output space $\mathscr{H}_2$ such that*

$$\mathcal{E}(\rho_{in}) = \sum_i E_i \rho_{in} E_i^\dagger \quad \text{and} \quad \sum_i E_i^\dagger E_i \leq I. \tag{1.8}$$

The I again denotes the identity operator on the input Hilbert space $\mathscr{H}_1$. Hence, this theorem gives us a very useful correspondence between a quantum operation (defined through physically motivated axioms **a1**,**a2**, **a3**) and its Kraus representation. One can easily check, that Kraus operators of the quantum operation, which occurs with certainty, obey the equation $\sum E_i^\dagger E_i = I$. On the contrary if the quantum operation $\mathcal{E}$ occurs with probability $0 \leq \mathrm{Tr}[\mathcal{E}(\rho)] < 1$ (the quantum operation does not provide full description of the physical process and only corresponds to some measurement outputs), its Kraus representation fulfils the relation $\sum_i E_i^\dagger E_i < I$. Here we should emphasize, that Kraus representation of a given quantum operation is not unique. The complete answer to the freedom of Kraus representations gives us the following theorem

Theorem 1.2.2 *Let $\{E_1, ..., E_m\}$ and $\{F_1, ...F_n\}$ are Kraus operators giving rise to quantum operations $\mathcal{E}$ and $\mathcal{F}$, respectively. By appending zero operators to the shorter list of Kraus operators we achieve that $m = n$. Then $\mathcal{E} = \mathcal{F}$ if and only if there exists unitary $m \times m$ such that*

$$E_i = \sum_{j=1}^{m} u_{ij} F_j. \tag{1.9}$$

As we have already mentioned, Kraus operators describe the combined action of unitary evolutions and measurements on composite systems. But the converse is also true and it brings us to the third approach, which reflects our natural requirement, that every state change arises

from unitary evolutions and measurements of our principal system and additional ancillary systems, which together form a closed system. The following theorem [20] proves that our physical intuition is correct.

Theorem 1.2.3 *Let $\mathscr{H}_1$ be the input Hilbert space and $\mathscr{H}_2$ the output Hilbert space with in general different dimensions. Let $\mathcal{E}$ be any quantum operation, mapping an arbitrary input density operator $\rho_{in} \in \mathsf{S}(\mathscr{H}_1)$ to the output density operator $\rho_{out} \in \mathsf{S}(\mathscr{H}_2)$. Then there exists a model preparation ancillary system* $\mathbf{R}$ *(with Hilbert space $\mathscr{H}_R$, starting in a pure state $|\phi_R\rangle$), a model measurement ancillary system* $\mathbf{L}$ *(with Hilbert space $\mathscr{H}_L$, fulfilling equation $\mathsf{dim}(\mathscr{H}_1) \times \mathsf{dim}(\mathscr{H}_R) = \mathsf{dim}(\mathscr{H}_2) \times \mathsf{dim}(\mathscr{H}_L)$) and dynamics specified by a unitary operator U (acting on the composite system with Hilbert space $\mathscr{H}_1 \otimes \mathscr{H}_R$) and a non-vanishing projector P on the Hilbert subspace of a measurement ancillary system $\mathscr{H}_L$ such that*

$$\mathcal{E}(\rho_{in}) = \mathrm{Tr}_L \left[(I_{\mathscr{H}_1} \otimes P) U (\rho_{in} \otimes |\phi_R\rangle\langle\phi_R|) U^\dagger \right]. \tag{1.10}$$

In other words, an arbitrary quantum operation can be implemented in three steps. First, we add a preparation ancillary system. Then the composite system undergoes an unitary evolution with a projective measurement on measurement ancillary system at the end. Finally, the measurement ancillary system is traced out to leave the system in the desired output state. This last approach gives us a physical realization of a given quantum operation. In particular, if the operation is a channel (trace-preserving operation), no measurement is needed after a unitary evolution and we call this realization an unitary delation of this quantum operation.

We have summarized the theoretical framework of quantum operations, which describes the most general state changes subjected to the laws of quantum mechanics. All other state transformations, which are not in accordance with these laws, we call non-physical maps.

1.3 LOCC operations

An important family of quantum operations are those, which satisfy the so-called LOCC constraint - a term which we will briefly explain. There are theoretical and also technological motivations for this constrain. The latter arises from various quantum communication schemes over a distance. These communication scenarios typically involve several parties (represented by quantum subsystems) at disposal of different distant members of quantum communication. A necessary preparation step in all quantum communications is the distribution of these subsystems in desired quantum states (for instance in quantum teleportation [13] the perfect distribution of maximally entangled states is necessary). However, an inevitable environment noise

decreases our ability to perform this task. Is there any chance how to overcome this problem? One possibility is to employ noisy channel and distribute imperfect quantum states so many times as we need and then use quantum operations in distant local parties. Under this restriction each member can act only locally on his part - perform only local operations (LO). A very simple example of such LO operation is provided by

$$\rho_{out} = U_A \otimes U_A \rho_{in} U_B^\dagger \otimes U_B^\dagger, \tag{1.11}$$

where $\rho_{in} \in \mathsf{L}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is an input density operator of a bipartite system described by Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$ and $U_A(U_B)$ represents a local action (unitary transformation) acting on the subsystem A (B).

During these local quantum operations classical communication can be exploited (use a phone to send results of their measurements, etc) performed using standard classical technology. It gives us the possibility to coordinate the quantum actions of distant parties. We call such operations LOCC (Local Operations and Classical Communication).

Apart of these technical reasons there is also a fundamental reason why we are interested in LOCC operations. The LOCC constraint allows us to establish a concept of quantum entanglement (see section 2.1).

What is the general structure of all LOCC operations? Actually, we do not know their complete general structure because classical communication makes a complete characterization of LOCC operations very hard. We know that LOCC operations belong to the bigger set of separable quantum operations. In the case of two parties, these are the operations, which have a product Kraus decomposition, i.e.

$$\rho_{out} = \frac{\sum_k E_k \otimes F_k \rho_{in} E_k^\dagger \otimes F_k^\dagger}{\mathrm{Tr}\left[\sum_k E_k \otimes F_k \rho_{in} E_k^\dagger \otimes F_k^\dagger\right]}, \tag{1.12}$$

where Kraus operators have to satisfy $\sum_i E_i^\dagger E_i \otimes F_i^\dagger F_i = I$. Any LOCC operation can be written in the form (1.12), but surprisingly there are separable operations which cannot be implemented as LOCC operations [24].

1.4 Choi-Jamiołkowski isomorphism

There are two frequent problems which we face in quantum information processing. First, being given a transformation of states, we have to decide whether this transformation is a quantum operation and which are the physical devices that realize it. Provided that the answer to the

first problem is "no" we face the other problem, namely best approximation for a given quantum information task. In order to solve both these tasks we need to obtain a list of possible quantum operations. A solution of this very hard problem usually depends on our ability to decide which map is completely positive and which is not.

A useful tool to characterize quantum trace-preserving operations in finite dimensional systems is the Choi-Jamiołkowski [19, 21, 22] isomorphism. It is a one-to-one correspondence—between CP maps $\mathcal{E} : \mathsf{S}(\mathscr{H}) \to \mathsf{S}(\mathscr{K})$ and positive operators $R_{\mathcal{E}}$ on $\mathscr{K} \otimes \mathscr{H}$. The definition reads

$$R_{\mathcal{E}} = (\mathcal{E} \otimes \mathcal{I})|I\rangle\!\rangle\langle\!\langle I| \longleftrightarrow \mathcal{E} = \mathrm{Tr}_{\mathscr{H}}\left[\left(I \otimes \rho^T\right) R_{\mathcal{E}}\right], \tag{1.13}$$

where $\mathcal{I}$ is the identity map on $\mathsf{S}(\mathscr{H})$, $|I\rangle\!\rangle = \sum_i |i\rangle \otimes |i\rangle$ is the maximally entangled (non normalized) vector in $\mathscr{H} \otimes \mathscr{H}$, and O^T denotes the transposition with respect to the fixed basis used to write $|I\rangle\!\rangle$. This isomorphism allows us to translate some problems of complete positivity into the language of positive operators. One can easily checks, that trace-preservation constraint $\sum_i E_i^\dagger E_i = I_{\mathscr{H}}$ translates as $\mathrm{Tr}_{\mathscr{K}}[R_{\mathcal{E}}] = I_{\mathscr{H}}$, where $I_{\mathscr{H}}$ denotes the identity operator on Hilbert space $\mathscr{H}$.

A simple consequence of this isomorphism which can help us to answer the question whether a given linear operation is completely positive or not, is a theorem due to Jamiołkowski and Choi [19, 21, 23]. This theorem states the following:

Theorem 1.4.1 (Choi, Jamiolkovski) *Let $\{|u_i\rangle\}$ be an orthonormal basis in the Hilbert space $\mathscr{H}_1$ and $P_{ij} = |u_i\rangle\langle u_j|$ be the corresponding standard orthonormal basis in the Hilbert space $\mathsf{L}(\mathscr{H}_1)$. Then a linear map $\mathcal{E} : \mathsf{L}(\mathscr{H}_1) \to \mathsf{L}(\mathscr{H}_1)$ is completely positive if and only if the linear operator $\mathcal{J}(\mathcal{E}) = \sum_{ij} \mathcal{E}(P_{ij}) \otimes P_{ij}$ is positive.*

To prove this theorem it is sufficient to check the validity of the following equation

$$R_{\mathcal{E}} = \mathcal{E} \otimes \mathcal{I}\left(\sum_{i,j} |u_i\rangle\langle u_j| \otimes |u_i\rangle\langle u_j|\right) = \sum_{i,j} \mathcal{E}(|u_i\rangle\langle u_j|) \otimes |u_i\rangle\langle u_j|. \tag{1.14}$$

The other interesting feature of this tool is, that different Kraus representations of a quantum operation $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ correspond to different ensemble representations for $R_{\mathcal{E}} = \sum_i |E_i\rangle\!\rangle\langle\!\langle E_i|$. Again, if we want to be sure about the correctness of this statement it is sufficient to realize, that

$$\mathcal{E}(\rho) = \sum_i \mathrm{Tr}_{\mathscr{H}}\left[I \otimes \rho^T |E_i\rangle\!\rangle\langle\!\langle E_i|\right] = \sum_i E_i \rho E_i^\dagger. \tag{1.15}$$

It is a one-to-one correspondence between ensemble representations of operator $R_{\mathcal{E}}$ and Kraus decompositions of the map $\mathcal{E}$. Hence to obtain Kraus representation of a quantum operation $\mathcal{E}$, it is enough to construct the operator $R_{\mathcal{E}}$ and then take one of its ensemble decompositions.

As we will see in the next section, the Choi-Jamiołkowski isomorphism (1.13) can be also a useful tool for describing covariant channels.

1.5 Covariant trace-preserving operations

Current literature on quantum maps describes a variety of processes. Among them quite a privileged role is played by so called *covariant processes*. In this part we introduce this family of quantum operations. In literature covariance means that the process is required to work equally well on a set of states which is invariant under a group of transformations.

Let $\mathbf{G}$ be a group, U_g and V_g be its unitary representations. Consider a class of states $\Omega \in \mathsf{S}(\mathscr{H})$, which is invariant under the action of a group $\mathbf{G}$, namely $U_g \rho U_g^\dagger \in \Omega$ for all $g \in \mathbf{G}$ and for all states $\rho \in \Omega$. We say that a trace preserving quantum operation $\mathcal{E} : \mathsf{S}(\mathscr{H}) \to \mathsf{S}(\mathscr{K})$ is covariant under the action of the group $\mathbf{G}$, if it satisfies the covariance condition

$$\mathcal{E}(V_g \rho V_g^\dagger) = U_g \mathcal{E}(\rho) U_g^\dagger, \tag{1.16}$$

for all states $\rho \in \Omega$ and all $g \in \mathbf{G}$. The requirement "equally well" is ensured in that the output state of a group-transformed input state is given as the transformed output (see figure (1.1)). For instance, if one wants to design quantum operation which should work equally well on all

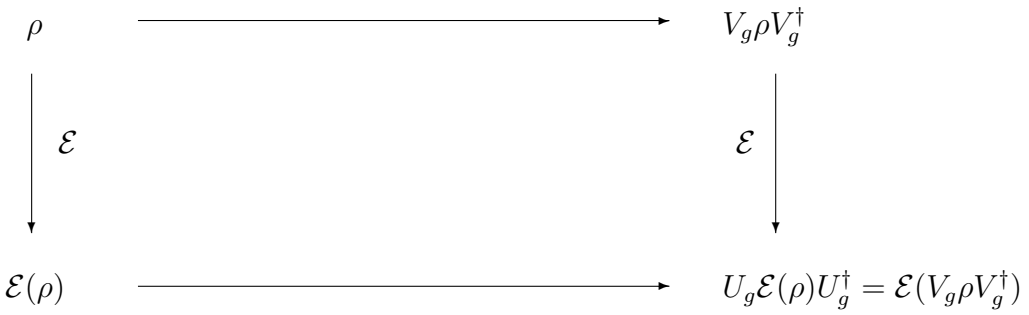

Figure 1.1: Graphic representation of covariant condition

pure states of a d-dimensional Hilbert space, then the channel has to be covariant with respect

to the action of the full $\mathsf{SU}(d)$ group. These processes are usually called *universal*. Conversely, non-universal processes are called *state-dependent*.

In some cases it can be helpful to know that in the Choi-Jamiołkowski isomorphism, the covariant condition (1.16) reads [22]

$$[R_{\mathcal{E}}, V_g \otimes U_g^*] = 0, \qquad \forall g \in \mathbf{G}. \tag{1.17}$$

The complex conjugate is with respect to the basis in which the operator $R_{\mathcal{E}}$ is defined.

Suppose that the group $\mathbf{G}$ is compact. Then the group $\mathbf{G}$ is equipped with a Haar measure (see section B.3). It allows us to define for an arbitrary quantum operation $\mathcal{E} : \mathsf{S}(\mathscr{H}) \to \mathsf{S}(\mathscr{K})$ the linear map $\hat{\mathcal{E}} : \mathsf{L}(\mathscr{H}) \to \mathsf{L}(\mathscr{K})$ as follows

$$\hat{\mathcal{E}}(\rho) \equiv \int_G dg \;\; U_g^\dagger \mathcal{E}(V_g \rho V_g^\dagger) U_g. \tag{1.18}$$

As we will show, this map is also a quantum operation (a completely positive trace-preserving map) and moreover fulfils the condition of covariance (1.5). We do the proof in a few steps. Firstly using the theorem (1.4) we can prove that the map $\hat{\mathcal{E}}$ is completely positive. We have to check only whether the operator $\mathcal{J}(\hat{\mathcal{E}}) = \sum_{ij} \hat{\mathcal{E}}(P_{ij}) \otimes P_{ij}$ is positive, where P_{ij} is given as $P_{ij} = |u_i\rangle\langle u_j|$ with respect to some orthonormal basis $\{|u_i\rangle\}$ of the Hilbert space $\mathscr{H}$. A simple calculation reveals us

$$\begin{aligned} \mathcal{J}(\hat{\mathcal{E}}) &= \sum_{ij} \left(\int_G dg \;\; U_g^\dagger \mathcal{E}(V_g P_{ij} V_g^\dagger) U_g \right) \otimes P_{ij} = \\ &= \int_G dg \;\; U_g^\dagger \otimes V_g^\dagger \left(\sum_{ij} \mathcal{E}(P'_{ij}) \otimes P'_{ij} \right) U_g \otimes V_g \end{aligned} \tag{1.19}$$

with $P'_{ij} = |u'_i\rangle\langle u'_j|$, where the basis $\{|u'_i\rangle\}$ is defined as a unitary change of our original basis $|u'_i\rangle = V_g|u_i\rangle$. Let us now take an arbitrary state $|\psi\rangle \in \mathsf{S}(\mathscr{K} \otimes \mathscr{H})$ and figure out the fidelity

$$\begin{aligned} \langle\psi|\mathcal{J}(\hat{\mathcal{E}}|\psi\rangle &= \langle\psi| \int_G dg \;\; U_g^\dagger \otimes V_g^\dagger \left(\sum_{ij} \mathcal{E}(P'_{ij}) \otimes P'_{ij} \right) U_g \otimes V_g |\psi\rangle \\ &= \int_G dg \;\; \langle\psi_g| \sum_{ij} \mathcal{E}(P'_{ij}) \otimes P'_{ij} |\psi_g\rangle, \end{aligned} \tag{1.20}$$

where we have used the notation $|\psi_g\rangle = U_g \otimes V_g|\psi\rangle$. Because the original quantum operation $\mathcal{E}$ is completely positive, the argument in the integral (1.20) is a nonnegative function for all elements of the group $\mathbf{G}$. Hence the integral is nonnegative and the map $\hat{\mathcal{E}}$ is completely positive.

In the same way we show that the map $\hat{\mathcal{E}}$ is also a trace-preserving operation, i.e. $\mathrm{Tr}[\hat{\mathcal{E}}(\rho)] = 1$ for all density operators $\rho \in \mathsf{S}(\mathscr{H})$

$$\begin{aligned} \mathrm{Tr}\{\hat{\mathcal{E}}(\rho)\} &= \sum_i \langle u_i| \int_G dg \;\; U_g^\dagger \mathcal{E}(V_g \rho V_g^\dagger) U_g |u_i\rangle \\ &= \int_G dg \;\; \sum_i \langle u_i| U_g^\dagger \mathcal{E}(V_g \rho V_g^\dagger) U_g |u_i\rangle = \int_G dg \;\; 1 = 1. \end{aligned} \tag{1.21}$$

Finally, using a left-invariant property of the Haar measure we demonstrate that the map $\hat{\mathcal{E}}$ is covariant (1.16). Let us consider an arbitrary element of the group $h \in \mathbf{G}$, then the term $\hat{\mathcal{E}}(V_h \rho V_h^\dagger)$ can be rewritten as

$$\begin{aligned} \hat{\mathcal{E}}(V_h \rho V_h^\dagger) &= \int_G dg \;\; U_g^\dagger \mathcal{E}(V_g V_h \rho V_h^\dagger V_g^\dagger) U_g = \\ &= U_h \left[\int_G dg \;\; U_{gh}^\dagger \mathcal{E}(V_{gh} \rho V_{gh}^\dagger) U_{gh} \right] U_h^\dagger = U_h \hat{\mathcal{E}}(\rho) U_h^\dagger \end{aligned} \tag{1.22}$$

We showed how to construct a covariant quantum operation from an arbitrary one. In the section 1.8 we will explain, why covariant quantum operations turn out to be very useful in optimization of non-physical maps by quantum operations.

1.6 No-cloning theorem

We have summarized the theory of quantum operations. In certain cases it helps to decide which classical operations can be performed ideally also quantum mechanically. One of the most common classical information tasks forbidden by quantum mechanics is *copying*. The impossibility of perfect quantum copying is the content of the famous *No-cloning Theorem* due to W. K. Wooters and W. H. Zurek [4]. Suppose a quantum system associated with a Hilbert space $\mathscr{H}$ and a deterministic quantum operation $\mathcal{T} : \mathscr{H} \longrightarrow \mathscr{H} \otimes \mathscr{H}$ which copies pure states perfectly, i.e.

$$\mathcal{T}(|\psi\rangle\langle\psi|) = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \tag{1.23}$$

for all pure states $|\psi\rangle\langle\psi| \in \mathsf{S}(\mathscr{H})$. This is our only requirement on the deterministic copying quantum operation $\mathcal{T}$. Let us consider another pure state $|\phi\rangle$ and calculate the fidelity F (for its definition and its properties see appendix A) between these states before and after the copying. Owing to the theorem (A.0.3) we know that any trace-preserving operation cannot decrease fidelity between two input states, we get

$$|\langle\psi|\phi\rangle|^2 = F(|\psi\rangle|\psi\rangle, |\phi\rangle|\phi\rangle) = F(\mathcal{T}(|\psi\rangle\langle\psi|), \mathcal{T}(|\phi\rangle\langle\phi|)) \geq \tag{1.24}$$

$$\geq F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|. \tag{1.25}$$

The inequality $|\langle\psi|\phi\rangle|^2 \geq |\langle\psi|\phi\rangle|$ is fulfilled if and only if $|\langle\psi|\phi\rangle|$ is 0 or 1. We thus have arrived at a contradiction, in whose heart lies the linearity of quantum mechanics, and we can formulate the no-cloning theorem as follows

Theorem 1.6.1 *Let Ω be a set of states from $\mathsf{S}(\mathscr{H})$, which contains at least two non-orthogonal states. It is impossible to make a perfect copy of an unknown state from the set Ω with certainty.*

We can think also about cloning mixed states. This generalization of cloning is usually referred to as the *broadcasting of quantum states*. For an arbitrary mixed state $\rho \in \mathsf{S}(\mathscr{H})$, the broadcasting machine should return a general entangled state $\rho_{out} \in \mathsf{S}(\mathscr{H}^{\otimes 2})$, such that $\mathrm{Tr}_1\, \rho_{out} = \mathrm{Tr}_2\, \rho_{out} = \rho$. It was shown [25] that it is impossible to broadcast two unknown non-commuting density operators perfectly.

Thus, perfect copying is impossible: either the copies are not perfect, or they are perfect but sometimes the copying process gives no outcome (probabilistic cloning [26]). Does the impossibility of perfect quantum state copying invalidate the entire concept of quantum information? Surprisingly, the drawback can be turned into an advantage. If information encoded into non-orthogonal states arrives perturbed at a receiver, there is a chance, that information was copied by any adversary. This makes it possible to establish the idea of quantum cryptography (see [27], [28], [29]). There is also a deep connection with fundamental laws of theoretical physics. For instance the impossibility to make perfect copies in connection with the entangled EPR pair (1) prohibits us to design a process permitting a communication faster then light communication [30].

1.7 NOT operation

Another non-physical map is the *NOT-transformation*. Consider a d-dimensional Hilbert space $\mathscr{H}$. The NOT transformation is defined as the operation, which maps an arbitrary pure input state $|\phi\rangle \in \mathsf{S}(\mathscr{H})$ onto a pure state which is orthogonal to state $|\phi\rangle$, i.e. $|\phi\rangle^{\perp} \in \mathsf{S}(\mathscr{H})$ that $\langle\phi|\phi^{\perp}\rangle = 0$. Suppose that such a quantum operation $\mathcal{N}$ exists. Let E_i be its Kraus operators (see theorem (1.4.1)), i.e. $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^{\dagger}$ for any density operator $\rho \in \mathsf{S}(\mathscr{H})$. When $\mathcal{N}$ is indeed a perfect quantum NOT-transformation, all pure states have to be turned into the form

$$\mathcal{N}(|\psi\rangle\langle\psi|) = \sum_i E_i|\psi\rangle\langle\psi|E_i^{\dagger} = |\psi^{\perp}\rangle\langle\psi^{\perp}|. \tag{1.26}$$

Using this assumpton it is simple to check that

$$0 = \langle\psi|\mathcal{N}(|\psi\rangle\langle\psi|)|\psi\rangle = \langle\psi|\left(\sum_i E_i(|\psi\rangle\langle\psi|)E_i^\dagger\right)|\psi\rangle = \sum_i |\langle\psi|E_i|\psi\rangle|^2. \tag{1.27}$$

The relation (1.27) is fulfilled if and only if all the Kraus operators satisfy $E_i = 0$. Hence the only map which suits our requirement is the nonphysical null operator.

The key issue of this problem is again linearity of quantum mechanics. Indeed, it is easy to check that an arbitrary anti-symmetric conjugate anti-linear operator Θ satisfies the requirement $\langle\psi|\Theta|\psi\rangle = 0$ for every state $|\psi\rangle \in \mathsf{S}(\mathscr{H})$. Therefore we conclude that it is possible to construct a NOT-gate for an arbitrary real subspace of $\mathscr{H}$. This result has some consequences for quantum information processing. For instance, there are so-called remote state preparation protocols, in which the NOT-gate plays important role and the existence of perfect NOT-gate allows to perform perfect remote state preparation. For details see part 4.2.3.

1.8 Covariant optimization of non-physical maps

We have presented two well-known cases of forbidden (non-physical) operations. However the fact, that certain operations are forbidden by laws of quantum mechanics, is not the end of the story. On the contrary, "forbidden" goads our interest. A natural question arises. *How well can we approximate these non-physical transformations by quantum operations and how do these limits influence quantum information processing?* Much work has been devoted to the copying of pure quantum states [31, 32, 33, 34, 35, 36, 37, 38, 39] and also to the NOT-gate [5, 40, 41, 42].

Most of these works make a basic assumption, which allows to solve the optimization explicitly: the apparatus should work equally well on all states of interest. A natural framework, usually used for work within this assumption, are covariant quantum operations. In this approach we suppose that the set of input states $\Omega_{in} = \{\rho\} \subset \mathsf{S}(\mathscr{H})$, for which the process should work equally well, is invariant under the action of a unitary representation V_g on $\mathscr{H}$ of a group $\mathbf{G}$

$$V_g\rho V_g^\dagger \in \Omega_{in}, \qquad \forall g \in \mathbf{G} \qquad \forall \rho \in \Omega_{in}. \tag{1.28}$$

Moreover, we suppose that transitive action of the group $\mathbf{G}$ connects all elements of Ω_{in} with some reference state $\rho_{ref} \in \Omega_{in}$

$$(\forall \rho \in \Omega_{in})(\exists g \in \mathbf{G})(V_g\rho_{ref}V_g^\dagger = \rho). \tag{1.29}$$

1.8 **Covariant optimization of non-physical maps**

Consider a transformation which ascribes to each input state the output ideal state (our desired state). But we can assume more general situation, namely that there are more possible ideal output states. Taking account with this general setting, let us consider a map $\mathcal{K}$, which ascribes to each state ρ from the set of input states Ω_{in} the set of output states $\mathcal{K}(\rho) \subset \mathsf{S}(\mathscr{K})$. Actually, this set of output states $\mathcal{K}(\rho)$ represents all possible ideal state transformations. We suppose that these ideal transformations cannot be performed ideally, i.e. they can be even nonphysical. Our aim is to find a good approximation of these ideal maps. Let the set $\Omega_{out} = \{\mathcal{K}(\rho)|\rho \in \Omega_{in}\}$ be invariant under the action of another unitary representation U_g of the group $\mathbf{G}$, i.e.

$$U_g \mathcal{K}(\rho) U_g^\dagger \in \Omega_{out}, \qquad \forall g \in \mathbf{G} \qquad \forall \rho \in \Omega_{in}. \tag{1.30}$$

Suppose also the map $\mathcal{K}$ is covariant, i.e. $\mathcal{K}(U_g \rho U_g^\dagger) = V_g \mathcal{K}(\rho) V_g^\dagger$ for all elements $g \in \mathbf{G}$ and all states $\rho \in \Omega_{in}$. To be able to decide how well a given quantum operation approximates the set of ideal maps given by the map $\mathcal{K}$, we introduce a merit function. This function, let say $\delta(\sigma, \mathcal{K}(\rho)) \in \mathbb{R}_+$, defines a distance between a state $\sigma \in \mathsf{S}(\mathscr{K})$ and the set of ideal outputs $\mathcal{K}(\rho) \in \Omega_{out}$ of an input state $\rho \in \Omega_{in}$. We impose two natural requirements

- the merit function δ is convex (resp. concave) in the first argument and achieves its minimum (resp. maximum) when $\sigma \in \mathcal{K}(\rho)$
- the merit function δ fulfills the invariance property

$$\delta(\sigma, U_g \mathcal{K}(\rho) U_g^\dagger) = \delta(U_g^\dagger \sigma U_g, \mathcal{K}(\rho)), \quad \forall \rho \in \Omega_{in}, \forall \sigma \in \mathsf{S}(\mathscr{K}), \forall g \in \mathbf{G}. \tag{1.31}$$

In the following, we will consider the case of a convex function δ (our considerations can be easily reformulated for the case of a concave function δ). Let us consider a quantum operation $\mathcal{E} : \mathsf{S}(\mathscr{H}) \to \mathsf{S}(\mathscr{K})$. The largest achievable distance $\Delta_{\mathcal{K}}(\mathcal{E})$

$$\Delta_{\mathcal{K}}(\mathcal{E}) \equiv \sup_{\rho \in \Omega_{in}} \delta(\mathcal{E}(\rho), \mathcal{K}(\rho)) = \sup_{g \in \mathbf{G}} \delta\left(\mathcal{E}(V_g \rho_{ref} V_g^\dagger), \mathcal{K}(V_g \rho_{ref} V_g^\dagger)\right) \tag{1.32}$$

is called an error measure characterizing the quality with which the channel $\mathcal{E}$ approximates the set of ideal outputs given by the $\mathcal{K}$. To find the best performing channel we have to look for those operations, which minimizes the error measure (1.32). In many cases covariant channels allow this maximization problem to be solved analytically. Covariant quantum operations give the same error measure for all input states $\rho \in \Omega_{in}$. Indeed, consider an arbitrary state $\rho \in \Omega_{in}$ connected with a reference state $\rho_{ref} \in \Omega_{in}$ by an element of the unitary representation V_g.

From the invariance property (4.8) it follows

$$\begin{aligned}\delta(\mathcal{E}(\rho),\mathcal{K}(\rho)) &= \delta(\mathcal{E}(V_g\rho_{ref}V_g^\dagger),\mathcal{K}(V_g\rho_{ref}V_g^\dagger)) = \delta(\mathcal{E}(V_g\rho_{ref}V_g^\dagger),U_g\mathcal{K}(\rho_{ref})U_g^\dagger) \\ &= \delta(U_g^\dagger\mathcal{E}(V_g\rho_{ref}V_g^\dagger)U_g,\mathcal{K}(\rho_{ref})) = \delta(\mathcal{E}(\rho_{ref}),\mathcal{K}(\rho_{ref})). \qquad (1.33)\end{aligned}$$

Hence in the case of covariant channels we can omit sup in the definition (1.32) and calculate the error measure only for an arbitrary chosen state.

Now, the optimization in a covariant setting is based on the fact, that if the optimum error measure is reached by some channel $\mathcal{E}$, it is always possible to achieve the optimum by a covariant channel $\hat{\mathcal{E}}$ (1.18). We can show it in the following way. Consider an arbitrary state $\rho \in \Omega_{in}$. We get

$$\begin{aligned}&\delta(\hat{\mathcal{E}}(\rho),\mathcal{K}(\rho)) = \delta\left(\int_G dg\ U_g^\dagger\mathcal{E}(V_g\rho V_g^\dagger)U_g,\mathcal{K}(\rho)\right) \\ &\leq \int_G dg\ \delta\left(U_g^\dagger\mathcal{E}(V_g\rho V_g^\dagger)U_g,\mathcal{K}(\rho)\right) = \int_G dg\ \delta\left(\mathcal{E}(V_g\rho V_g^\dagger),\mathcal{K}(V_g\rho V_g^\dagger)\right) \\ &\leq \int_G dg \sup_{\rho\in\Omega_{in}} \delta(\mathcal{E}(\rho),\mathcal{K}(\rho)) = \Delta_{\mathcal{K}}(\mathcal{E}). \qquad (1.34)\end{aligned}$$

The first inequality is a special form of the so-called Jensen's operator inequality [43]. Therefore, we can restrict the optimization procedure to covariant channels, which form a convex set. Moreover, we can search for the optimal quantum operation within the boundary of the convex set of covariant processes, since a convex function defined on a convex set achieves its extremal values on the boundary.

Chapter 2

Quantum entanglement

In this chapter we take a tour across contemporary state-of-the-art of entanglement. We discuss differences between classical and quantum correlations and using the notion of separability we define entangled states. We summarize mathematical tools how to detect and quantify bipartite entanglement. Finally, we give a brief description of multi-partite correlations.

2.1 Separability versus Entanglement

To give a comprehensive answer to the fundamental question, what is the physical meaning of entanglement itself, is a very hard task. Entanglement is loosely characterized as the quantum correlation that can occur in many-party quantum states. But how can we define quantum correlations, and what separates them from classical correlations? Here we give the most convenient definition using the concept of separable states. This approach is motivated by the idea that classical correlations among quantum states are those which can be prepared in a classical way using only local operations acting on individual subsystems and classical communication among these parties (see section 1.3). Such states can embody only classical correlations. Allowing classical communication in the set of LOCC operations means that they are not just local anymore and therefore the structure of quantum states embodying classical correlation (separable states) can be quite complicated.

Suppose we have a quantum system formed by N subsystems (parties), each with Hilbert space $\mathscr{H}_i$, $i \in \mathbb{N}$. Hence the Hilbert state of the whole system is given as $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes ... \otimes \mathscr{H}_N$. We say, that a state is *separable* if it can be represented as a convex linear combination (a statistical mixture) of product states. In other words, the density matrix ρ acting on the whole

Hilbert space $\mathcal{H}$ represents a separable state if it can be expressed as

$$\rho = \sum_k p_k \rho_1^{(k)} \otimes \rho_2^{(k)} \otimes ... \otimes \rho_N^{(k)}, \tag{2.1}$$

with $\rho_d^{(k)}$ density operator acting only on the Hilbert space $\mathscr{H}_d$, and positive p_k fulfilling the normalization $\sum_k p_k = 1$. These states can be prepared by LOCC operations and all their correlations can be described classically. Hence we conclude that separable states contain no entanglement.

All states which cannot be written as a convex decomposition (2.1) are called *entangled*. In this way entanglement is defined as quantum correlation which cannot be prepared by LOCC. To implement quantum entanglement nonlocal quantum operations, acting on two or more parties, are required. Here it is necessary to emphasize that separability (or conversely entanglement) strongly depends on the chosen structure of parties. In other words: a separable state with respect to a given structure of parties may not be separable with respect to different one.

Separable states form a convex set, but entangled states do not. If we consider, for example, maximally entangled states $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$, then the state $\frac{1}{\sqrt{2}}(|\psi_-\rangle\langle\psi_-| + |\psi_+\rangle\langle\psi_+|)$ is separable. The basic question is whether a given state is entangled or separable. In practice it is often an impossible task to decide it due to infinitely many ways of decomposing a state ρ. Of course, the task is the harder the bigger a number of subsystems is. Therefore most of work dealing with entanglement detection focuses on entanglement between two parties. This is the reason why we often characterize a multipartite entanglement structure using only bipartite entanglement. Of course, it is not a full-featured description of multipartite entanglement but we do not have yet anything better. Although some results can be extended to analyze certain features of multipartite entanglement, there are still many problems under investigation or remain open often because they were not solved even in the bipartite case yet. This was also one of the reasons, which led us to characterized entanglement in our work purely with the help of bipartite entanglement. Let us briefly review the tools which are on display to characterize bipartite entanglement.

2.1.1 Pure states, Schmidt coefficients

If a density operator ρ describes a pure state, i. e. $\rho = |\phi\rangle\langle\phi|$, it is easy to check whether the state is separable or not. The state is separable (within this context we say also factorizable), if and only if both subsystems are also in a pure state, i. e. $|\phi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$. In this connection we introduce the so-called Schmidt decomposition of the state [44, 45]. For any pure state

$|\phi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ there are orthonormal basis $\{|e_i^A\rangle\}$ and $\{|e_i^B\rangle\}$ in the Hilbert spaces $\mathscr{H}_A$ and $\mathscr{H}_B$, that the state can be written as a sum of products of orthogonal states

$$|\phi\rangle = \sum_{i=1}^{k} q_i |e_i^A\rangle \otimes |e_i^B\rangle, \tag{2.2}$$

with $k \leq \min\{\mathsf{dim}(\mathscr{H}_A), \mathsf{dim}(\mathscr{H}_B)\}$. The state is entangled iff at least two coefficients in the Schmidt decomposition (2.2) do not vanish. Among the consequences of the Schmidt decomposition is, if the whole system is in a pure state, eigenvalues of density operators of both subsystems are the same. Many important properties of quantum systems are completely determined by the eigenvalues of density matrices. Hence for a pure states of a composite system such properties will be the same for both subsystems.

A technique related to Schmidt decomposition is *purification*. Consider a state ρ^A of a quantum system A. It is possible to introduce another *reference* system, which we denote R, and define a pure state $|AR\rangle$ for the joint system AR such that $\rho^A = \mathrm{Tr}_R(|AR\rangle\langle AR|)$. Let us explain how to construct a system R and purification $|AR\rangle$ for a given state ρ^A. Suppose ρ^A has orthonormal decomposition $\rho^A = \sum_i p_i |i^A\rangle\langle i^A|$. To purify ρ^A we introduce a system R which has the same state space as system A, with orthonormal basis states $|i^R\rangle$, and define a pure state for the combined system $|AR\rangle = \sum_i \sqrt{p_i}|i^A\rangle|i^R\rangle$. Now it is simple to verify, that this state is the purification of the state ρ^A.

2.1.2 Entanglement witness

As we have already mentioned, separable states form a convex set. Thus we can apply the Hahn-Banach theorem [46], which says that two convex and compact sets can be separated by a hyperplane. Using this fact, the Horodecki family proved the following theorem [47]:

Theorem 2.1.1 *For any entangled state represented by density operator ρ acting on Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$ there exists Hermitian operator V such that*

$$\mathrm{Tr}\{V\rho\} < 0 \qquad \textit{and} \qquad \mathrm{Tr}\{V\sigma\} \geq 0 \tag{2.3}$$

for all separable states σ.

The operator V is called *entanglement witness*. The expression $\mathrm{Tr}\{V\rho\}$ represents an inner product for operators on $\mathscr{H}$ and therefore can be regarded as a scalar product of two vectors, where the orientation of the hyperplane is determined in such a way, that separable states lie

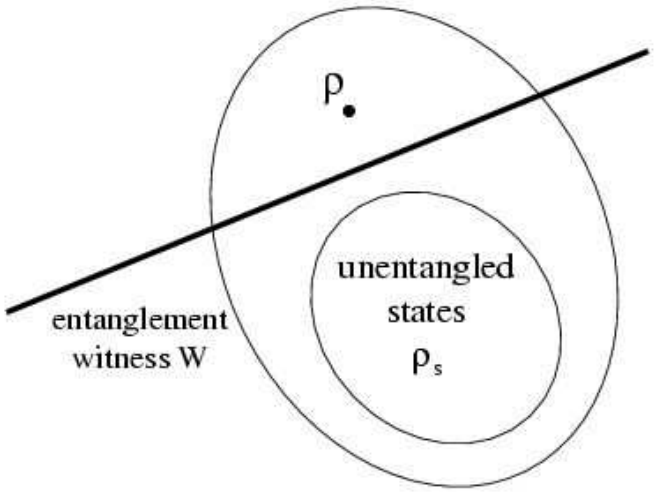

Figure 2.1: Hyperplane described by the entanglement witness operator W separates the entangled state ρ from the set of separable states

always on the positive side, whereas on negative side remain only entangled states. This fact is illustrated in the picture (2.1).

This rather abstract theorem gives us the possibility to construct criteria for detecting entanglement. Every such entanglement witness generates a sufficient condition for states to be entangled. Contrary, if we have such entanglement witness W then an arbitrary separable state has necessary to fulfil the condition $Tr\{V\sigma\} \geq 0$. The natural task arises: design a set of entanglement witness operators which is optimal, i.e. a minimal number of entanglement witnesses, which completely specify the convex set of separable states.

Using the Jamiołkowski isomorphism [21] between the positive maps and operators which are positive on the product projectors we can reformulate the theorem (2.1.1) as follows:

Theorem 2.1.2 *Let ρ act on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$. Then ρ is separable if and only if for any positive map $\Lambda : \mathsf{L}(\mathscr{H}_A) \longrightarrow \mathsf{L}(\mathscr{H}_B)$ the operator $(I \otimes \Lambda)\,\rho$ is positive.*

One good example of entanglement witness is the flip operator V [48]. The flip operator is defined on $\mathscr{H}^d \otimes \mathscr{H}^d$ by $V\left(|\psi\rangle \otimes |\phi\rangle\right) = |\phi\rangle \otimes |\psi\rangle$. It is easy to verify $\mathrm{Tr}\left\{V(P \otimes Q)\right\} = \mathrm{Tr}\left(PQ\right)$ for all operators P,Q acting on $\mathscr{H}^d$. The flip operator corresponds to the operation of partial transposition in the Jamiołkowski isomorphism.

2.1.3 PPT

The criterium of positive partial transposition was found by Peres [49]. So far it appears to be the strongest available criterium. It is convenient to define the partial transposition in matrix elements. Let ρ be a state of a bipartite Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$ with matrix elements in some product basis

$$\rho_{m\mu,n\vartheta} = \langle m| \otimes \langle \mu|\rho|n\rangle \otimes |\vartheta\rangle, \tag{2.4}$$

where the kets with Latin (resp. Greek) letters form an orthonormal basis in the Hilbert space describing the first (resp. second) subsystem. Hence the partial transposition of ρ with respect to the subsystem B is defined as

$$\rho^{T_B}_{m\mu,n\vartheta} = \rho_{m\vartheta,n\mu}. \tag{2.5}$$

We say that a state ρ is PPT if $\rho^{T_B} \geq 0$, otherwise we say that a state is NPT. The partial transposition has a simple operational form

$$PT = I_A \otimes \mathcal{T}, \tag{2.6}$$

where I_A is identity operator on the subsystem A and $\mathcal{T}$ is the transposition on the subsystem B. Consider a general separable state on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$

$$\rho_{sep} = \sum_k p_k \rho^{(k)}_A \otimes \rho^{(k)}_B. \tag{2.7}$$

Applying the partial transposition on (2.7) we obtain from (2.6)

$$\rho^{T_B}_{sep} = \sum_k p_k \rho^{(k)}_A \otimes (\rho^{(k)}_B)^{T_B}. \tag{2.8}$$

The outcome is again a density operator and therefore all separable states are PPT states. We conclude that a positive partial transposition is a necessary condition for separability. It was shown by the Horodecki family [47] using positive maps, that in bipartite systems of dimensions 2×2 and 2×3 the PPT is not only necessary but also sufficient condition. Unfortunately, we cannot generalize this theorem to cases of Hilbert spaces with higher dimensions.

2.1.4 Reduction criterion

Suppose Λ is a positive map on $\mathsf{L}(\mathscr{H}_B)$ (space of linear operators acting on $\mathscr{H}_B$). Then for any separable state (2.7) we have

$$(I \otimes \Lambda)\, \rho_{sep} \geq 0. \tag{2.9}$$

However in general, for all mixed states, it is not true. Provided the map Λ is not completely positive, there are entangled states which do not satisfy the inequality (2.9). If we define the map Λ as $\Lambda(A) = \mathrm{Tr}(A)I - A$, we can easily check that the eigenvalues of this map are given by $\lambda_i = \mathrm{Tr}(A) - a_i$, where a_i are eigenvalues of the operator A and $\mathrm{Tr}(A) = \sum_i a_i$. Thus the map Λ is positive.

Now let find out, into what form the formula (2.9) and the dual formula $(\Lambda \otimes I)\,\rho_{sep} \geq 0$ will convert. A simple calculation gives us the so-called reduction criterium [50]

$$I \otimes \rho_A - \rho \geq 0, \qquad \rho_A \otimes I - \rho \geq 0, \tag{2.10}$$

where ρ_A (resp. ρ_B) is the reduced density operator with respect to subsystem A (resp. subsystem B). What relation is between PPT criterium and the reduction criterium? The reduction criterium is weaker then PPT, but for 2×2 and 2×3 systems they are equivalent.

In context of the reduction criterium we introduce also the fully entangled fraction $\mathcal{F}(\rho)$ of a state ρ (acting on $\mathscr{H}^d \otimes \mathscr{H}^d$) defined as

$$\mathcal{F}(\rho) = \max_{|\psi\rangle} \langle\psi|\rho|\psi\rangle. \tag{2.11}$$

The maximum is taken over all maximally entangled states of the Hilbert space $\mathscr{H}^d \otimes \mathscr{H}^d$. From the reduction criterium we can derive simply, that an arbitrary state ρ satisfying $\mathcal{F}(\rho) > 1/d$ has to be entangled.

2.1.5 Majorization criterion

Consider a d-dimensional vector space $\mathbf{V}$. A vector with decreasing coefficients we will denote $x^{\downarrow}$, i.e. $x_i \geq x_{i+1}$ for $i \in \{1, 2, ..., d-1\}$. A vector $x^{\downarrow}$ is *majorized* by a vector $y^{\downarrow}$, denoted as $x^{\downarrow} \prec y^{\downarrow}$, when $\sum_{j=1}^{k} x_j \leq \sum_{j=1}^{k} y_j$ holds for $k = 1, ..., d-1$ and the equality holds for $k = d$.

The majorization criterion [54] says that if a state $\rho \in \mathsf{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is separable, then

$$\lambda_\rho^{\downarrow} \prec \lambda_{\rho_A}^{\downarrow} \qquad \text{and} \qquad \lambda_\rho^{\downarrow} \prec \lambda_{\rho_B}^{\downarrow} \tag{2.12}$$

have to be fulfilled. Here $\lambda_\rho^{\downarrow}$ denotes the vector consisting of the eigenvalues of ρ, in decreasing order. Zeros are appended to the vectors $\lambda_{\rho_A}^{\downarrow}$ (resp. $\lambda_{\rho_A}^{\downarrow}$) in order to make their dimension equal to the one of $\lambda_\rho^{\downarrow}$. Hence for separable states the ordered vector of eigenvalues for the whole density operator is mojorized by the ones of the reduced density operator. The majorization criterion is only a necessary, not a sufficient condition for separability.

2.2 Entanglement measures

The detection of entanglement is only the first step in our aim to understand this phenomenon. We have already mentioned that separable states contain no entanglement. The natural question raises, whether there is a maximally entangled state, i.e. one that is more entangled then all others. Indeed, at least in bipartite systems consisting of two fixed d-dimensional sub-systems (usually referred as qudits), such states exist. We say a state $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ to be *maximally entangled*, whenever both of its restrictions (reduced density operators) are maximally mixed. The Schmidt decomposition for an arbitrary maximally entangled vector $|\psi_{ME}\rangle$ reads

$$|\psi_{ME}\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |e_i\rangle \otimes |f_i\rangle, \tag{2.13}$$

where $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ are suitable orthonormal basis in the Hilbert space $\mathscr{H}_A$ and $\mathscr{H}_B$. For bipartite systems we have defined a concept of maximally entangled states, which is independent of the specific quantification of entanglement. This independent definition is based on the fact that using only LOCC operations any bipartite mixed state can be created from an arbitrary maximally entangled state. Examples of maximally entangled states are the *Bell states* of 2-dimensional subsystems

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right) \tag{2.14}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right). \tag{2.15}$$

The next question is, how can we quantify the amount of entanglement in a given state? It is not surprising that there is no simple answer to this. There are in principle two ways how to quantify the entanglement in a quantum state. First, *operational measures* are based on how well a certain task can be performed with the aid of an entangled state. Given a state and a task that consumes entanglement, how much can we achieve? In this sense, different tasks can generate different types of measures and hence different orderings of quantum states. The other way, which gives rise to *abstract measures*, is to work from a set of natural axioms we believe an entanglement measure should satisfy, and look for functionals that satisfy these axioms.

In general, an entanglement measure $E(.)$ is a real-valued positive functional defined on the set of all quantum states. We focus our attention on bipartite systems, hence

$$E : \mathsf{S}(\mathscr{H}_A \otimes \mathscr{H}_B) \to \mathbb{R}^+. \tag{2.16}$$

We will summarize the requirements for a well defined bipartite entanglement measure, and introduce the reader to some important entanglement measures. We do not make any attempt

to discuss all existing measures and related quantities. At the end of the chapter we give some remarks on the case of multipartite measures.

2.2.1 Requirements for entanglement measures

A good entanglement measure should satisfy several requirements. However, it is still an open question whether all of these conditions are indeed necessary. In fact, some of the entanglement measures we introduce below do not fulfill the complete list of properties

(P0a) $E(\rho) = 0$ if and only if ρ is separable. This is a useful property, but it is too strict in general.

(P0b) If $\rho \in \mathsf{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is separable then $E(\rho) = 0$.

(P1) *Normalization:* the entanglement of a maximally entangled state of two d-dimensional systems is given by

$$E(|\psi_{ME}\rangle\langle\psi_{ME}|) = \log d. \tag{2.17}$$

(P2a) *No increase under LOCC:* local operations and classical communication cannot increase the entanglement of a given state ρ, i.e.

$$E(\Omega_{LOCC}(\rho)) \leq E(\rho). \tag{2.18}$$

(P2b) *Invariance under local unitary operators:* local unitary operations do not change the degree of entanglement of a given state

$$E(U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger = E(\rho), \tag{2.19}$$

where U_1 (resp. U_2) is an arbitrary unitary operator on $\mathscr{H}_A$ (resp. $\mathscr{H}_A$).

(P3) *Continuity:* Let $\{\rho_n\}$ and $\{\sigma_n\}$ be sequence of bipartite states living on the Hilbert space $\mathscr{H}$. For all sequences $||\rho_n - \sigma_n||_1 \to 0$, where $||.||_1$ is the trace norm $||A||_1 = \mathrm{Tr}(\sqrt{A^\dagger A})$, the limit

$$E(\rho_n) - E(\sigma_n) \to 0 \tag{2.20}$$

should be valid.

(P4a) *Aditivity:* n identical copies of the state ρ should contain n times the entanglement of one copy, i.e.

$$E(\rho^{\otimes n}) = nE(\rho) \tag{2.21}$$

for all states ρ and $n \geq 1$.

(P4b) *Existence of a regularization:* For all bipartite states ρ, the limit

$$E^{\infty}(\rho) \equiv \lim_{n\to\infty} \frac{E(\rho^{\otimes n})}{n} \tag{2.22}$$

exists. E^{∞} is a measure which automatically satisfies aditivity.

(P5) *Subadditivity:* The entanglement of the tensor product of two states ρ and σ should not be larger than the sum of the entanglement of each of the states

$$E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma). \tag{2.23}$$

(P6) *Convexity:* The entanglement measure should be a convex function, i.e.

$$E(\lambda\rho + (1-\lambda)\sigma) \leq \lambda E(\rho) + (1-\lambda)E(\sigma) \tag{2.24}$$

for $0 \leq \lambda \leq 1$.

We have already mentioned that it is an open question, whether all these conditions are necessary for a good measure. However, the first three properties are accepted to be the denominator in the axiomatic approach and any function E satisfying the first three properties is called an entanglement monotone.

2.2.2 Pure states

Before treating the general case of mixed states we consider the simpler case of entanglement measures of pure states. The treatment is facilitated by the fact that a pure state contains no classical correlations between the subsystems. Hence, any correlation contained in a pure state must be of quantum origin. If an entangled state is pure, the states of the subsystems - described locally by the reduced density operator - are mixed. The amount of "mixing" of a pure state turns out to be the only source of quantum correlations and therefore a good measure of entanglement. How mixed is a quantum state ρ is given by the well-known *von Neumann entropy*, defined as

$$S(\rho) \equiv -\operatorname{Tr}(\rho \log \rho), \tag{2.25}$$

where we take the logarithm with the base 2 as is the custom in information theory. Its value is easily calculated from eigenvalues λ_i of ρ as

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i. \tag{2.26}$$

The von Neumann entropy describes the uncertainty in a quantum state. It is minimal (zero) for pure states and maximal (equal with $\log_2 d$, where d is $\min\{\mathsf{dim}\mathscr{H}_A, \mathsf{dim}\mathscr{H}_B\}$).

A good measure of entanglement of bipartite pure states, the so called *entropy of entanglement* E_E [15], is defined by the von Neumann entropy

$$E_E(|\psi\rangle) = S(\rho_A) \tag{2.27}$$

of the reduced density matrix ρ_A of the subsystem A, i.e. $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. In general, the von Neumann entropy depends only on the eigenvalues of the density matrix. Eigenvalues of both reduced density operators of a pure bipartite state are the same, as was mentioned in section (2.1.1). Thus the reduced von Neumann entropy is equal for both density matrices. The entropy of entanglement has some properties we find natural. (i) It is zero for any product states, (ii) it is maximal when the reduced density matrix is completely mixed, e.g. when the subsystems have no individual properties and (iii) it is invariant under local unitary transformations.

The entropy of entanglement was first introduced as a measure of entanglement in [55]. It is an abstract measure in the sense that it satisfies some requirements, and it does not have an immediate operational interpretation. Moreover if an arbitrary bipartite entanglement measure E satisfies properties (P0), (P1b), (P2a), (P3) and (P4a) for all pure states, then E coincides with the entropy of entanglement $E = E_E$. This is the content of the so-called uniqueness theorem for entanglement measures [56, 57].

In the following section we will discuss several bipartite entanglement measures that have been proposed in the literature. All the following quantities are entanglement monotones.

2.2.3 Mixed states

For mixed states the situation is much more involved, because there are both classical and quantum correlations that have to be discriminated by the entanglement measure. Therefore the definition of an entanglement measure for mixed states is more complicated and there is no unique entanglement measure.

First of all we have to mention that there is one special generalization that applies to any entanglement measure for pure states [58], and therefore is the most commonly used. Any mixed state can be expressed as a convex sum of pure states:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.28}$$

where p_i are positive and sum to one. The generalization of an entanglement measure E for pure states uses the infimum over all decompositions into pure states - the so called *convex roof*:

$$E(\rho) = \inf_{\{p_i, |\phi_i\rangle\}} \sum_i p_i E(|\psi_i\rangle), \quad \text{with} \quad p_i > 0 \quad \text{and} \quad \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.29}$$

However, an explicit evaluation of this quantity for a specific state implies a high dimensional optimization problem and therefore is in general a very hard computational task.

Let us start a short review of entanglement measures by two operational measures: *entanglement cost* and *distillable entanglement*.

Entanglement cost and distillable entanglement

The entanglement cost quantifies, how expensive it is to create an entangled state ρ, i.e. the minimal rate r at which one converts (using only LOCC operations) blocks of $r \times n$ 2-qubit maximally entangled states (2.13) into output states that approximate n copies $\rho^{\otimes n}$, such that the approximations become vanishingly small in the limit of large block sizes n. To be precise we denote a general LOCC operation by Λ. Then the entanglement cost can be defined as

$$E_C(\rho) = \inf \left\{ r : \lim_{n\to\infty} \left[\inf_{\Lambda} ||\rho^{\otimes n} - \Lambda((\Phi^+)^{\otimes rn})||_1 \right] = 0 \right\}. \tag{2.30}$$

Hence the entanglement of cost compares all quantum states with the "golded standard currency" - the maximally entangled Bell states.

Just as $E_C(\rho)$ measures how many maximally entangled states are required to create copies of ρ by LOCC alone, we can ask about the reverse process: at what rate may we extract maximally entangled two-qubit states from an input supply of states of the form ρ. This process is usually called *entanglement distillation*. The maximum yield which we can achieve in this process defines another asymptotic entanglement measure which is the distillable entanglement, $E_D(\rho)$. In analogy to the definition of $E_C(\rho)$ we give the precise mathematical definition of $E_D(\rho)$ as

$$E_D(\rho) = \sup \left\{ r : \lim_{n\to\infty} \left[\inf_{\Lambda} ||\Lambda(\rho^{\otimes n}) - (\Phi^+)^{\otimes rn}||_1 \right] = 0 \right\}. \tag{2.31}$$

In two party quantum information protocols entanglement is usually required in the form of maximally entangled states. So $E_D(\rho)$ tells us the rate at which noisy mixed states may be converted back into the "golden standard" Bell state by LOCC.

Obviously, the computation of either, the entanglement cost and the distillable entanglement are extraordinarily difficult tasks. However, it was shown in [59] that both the distillable

entanglement and entanglement cost are equal to the entropy of entanglement for pure states,

$$E_D(|\psi\rangle\langle\psi|) = E_C(|\psi\rangle\langle\psi|) = E_E(|\psi\rangle). \tag{2.32}$$

Indeed, if two states $|\psi_1\rangle$ and $|\psi_2\rangle$ have the same entropy of entanglement, then one can be converted into the other with efficiency approaching unity as $n \to \infty$. If they do not have the same entropy of entanglement, $|\psi_1\rangle$ can be converted into $|\psi_2\rangle$ with an asymptotic yield of $E_E(|\psi_1\rangle)/E_E(|\psi_2\rangle)$.

The other remarkable feature is, that E_D and E_C can be viewed as extreme measures in the sense that under certain conditions E_D is a lower bound and E_C is an upper bound for other entanglement measures. In fact, in [56] it was proved that if an entanglement measure satisfies requirements (P1a), (P2a), (P3) and (P4b) then the *regularized* version E^∞ fulfills the relation

$$E_D(\rho) \leq E^\infty(\rho) \leq E_C(\rho) \tag{2.33}$$

for all states ρ. These conditions are satisfied by the well-known measure: *Entanglement of formation*.

Entanglement of formation, Concurrence

The entanglement of formation is a straightforward generalization of the entropy of entanglement to mixed states. Any state $\rho \in \mathsf{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$ can be decomposed as a convex combination of projectors onto pure states, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with $\sum_i p_i = 1$ and $|\psi_i\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$. The entanglement of formation is defined as the averaged von Neumann entropy of the reduced density matrices of the pure states $|\psi_i\rangle$, minimized over all possible decompositions

$$E_F(\rho) = \inf_{dec} \sum_i p_i E_E(|\psi_i\rangle\langle\psi_i|). \tag{2.34}$$

From the definition of E_F, it is easy to see that it satisfies (P0a), normalization (P1a), LOCC monotonicity (P2a) and continuity (P3). It is not known whether the entanglement of formation is additive, but in all surveyed cases it was confirmed. We can be sure that subadditivity (P5) is fulfilled and convexity (P6) is a direct consequence of the definition (2.34).

A serious drawback of this measure is that we do not know in general, how to minimize analytically over all decompositions. It makes the calculation and hence the use of this measure very problematic. One must either resort to numerical techniques for general states [60], or restrict attention to cases with high symmetry (e.g. [61, 62, 63]), or consider only cases of low dimensionality. A closed form solution is known for bipartite qubit states [64, 65]. This exact

formula is based on the often used two-qubit entanglement measure: *concurrence*. To introduce this measure we have to define for every bipartite qubit state ρ a conjugate density matrix

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y), \tag{2.35}$$

where σ_y is the Pauli spin operator and the star-symbol (*) denotes complex conjugation. Let λ_1, λ_2, λ_3, λ_4 are eigenvalues of the matrix

$$R = R(\rho) = \rho\tilde{\rho} \tag{2.36}$$

sequenced in decreasing order. In terms of these eigenvalues the concurrence of the quantum state ρ is defined by the relation

$$C(\rho) = \max\left\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\right\}. \tag{2.37}$$

In particular, for pure state $\rho = |\psi\rangle\langle\psi|$ the concurrence can be written as

$$C(|\psi\rangle) = 2\sqrt{\det(\rho_A)}, \tag{2.38}$$

where ρ_A is the density matrix of the first subsystem, i.e. $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. According to this definition the values of the concurrence are confined to the interval $[0, 1]$ with $C(\rho) = 0$ and $C(\rho) = 1$ corresponding to a separable and a maximally entangled two-qubit state. The concurrence is monotonous under LOCC, and can thus be used as an entanglement measure for two qubits. The great advantage is that it is easily computable. However more important is that it is directly related to the entanglement of formation. For general bipartite qubit state it has been shown [66] that

$$E_F(\rho) = h\left(\frac{1 - \sqrt{1 - C^2(\rho)}}{2}\right) \tag{2.39}$$

with

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x). \tag{2.40}$$

With respect to the equation (2.39) the two-qubit $E_F(\rho)$ and the two-qubit concurrence are equivalent because these measures are monotonically related. This explains why most of authors use the concurrence to characterize entanglement of a two-qubit state rather then the E_F. Here we have to emphasize that the concurrence obtains its meaning via its connection to the entanglement of formation and not vice versa. For higher dimensional systems we do not have any such similar connection. There have been various attempts to generalize the concept of concurrence (see e.g. [40, 58, 60, 67, 68]).

Negativity

The entanglement measures, which we have discussed so far, have a serious drawback. In their definition some kind of optimization is included, which make their evaluation very difficult. The only exception is the concurrence, but it works well only for two entangled qubits. With the aim of introducing a computable measure of entanglement Vidal and Werner proposed a quantity called *negativity* [69]. This entanglement measure is defined as

$$N(\rho) \equiv \frac{||\rho^{T_B}||_1 - 1}{2}, \tag{2.41}$$

where $||\rho^{T_B}||_1 = \mathrm{Tr}(\sqrt{(\rho^{T_B})^\dagger \rho^{T_B}})$ is the trace norm of the partial transpose of a state ρ (*see* sction (2.1.3)). The trace norm of any hermitian operator A is equal to the sum of the absolute values of the eigenvalues of A. Density matrices have all their eigenvalues positive and thus $||\rho_1||_1 = \mathrm{Tr}(\rho) = 1$. The partial transpose ρ^{T_B} has also its trace equal one, but since it may have negative eigenvalues $\mu < 0$, its trace norm reads in general

$$||\rho^{T_A}||_1 = 1 + 2|\sum_i \mu_i| \equiv 1 + 2N(\rho). \tag{2.42}$$

Therefore the negativity $N(\rho)$, the sum $|\sum_i \mu_i|$ of the negative eigenvalues μ_i of ρ^{T_B}, measures by how much ρ^{T_B} fails to be positive definite. In other words, the negativity quantifies how much the state ρ violates the PPT criterion.

As we have already discussed in section (2.1.3), for any separable state ρ_s, its partial transposition is also a separable state and therefore $||\rho_S^{T_B}||_1 = 1$ and $N(\rho) = 0$. The opposite is not true because the negativity is zero also for PPT entangled states. It is equal to $\frac{1}{2}$ for Bell states, thus the negativity does not satisfy the normalization (P1). It is monotonic under LOCC (P2a), convex (P6), and subadditive (P5), satisfying $N(\rho \otimes \sigma) = N(\rho) + N(\sigma) + 2N(\rho)N(\sigma)$.

There are many other proposed measures like *relative entropy of entanglement*[70], *logarithmic negativity*[69], *robustness of entanglement* [71], *squashed entanglement* [72] and so on. All of them have the same serious drawback, namely we do not know how to evaluate them for general mixed states.

2.2.4 Multipartite entanglement

We have dealt so far with the bipartite entanglement and its quantification. In this section we would like to give some remarks on multipartite entanglement.

If we consider a system with more then two parties we face states which involve various types of entanglement. Let us exemplify this complex situation considering only three particles,

let say Alice, Bob, and Carol, in a state ρ. We say that a state describing particles Alice and Bob is bipartite (or two-way) entangled if their reduced density matrix is not separable, i.e. if

$$\rho_{AB} = \mathrm{Tr}_C\, \rho \tag{2.43}$$

is not separable. In this way we could describe the entanglement in a given three-particle state using three bipartite entanglements. Unfortunately it is not a complete description, because there are states which exhibit only entanglement of higher order than bipartite. Indeed, suppose that our three particles are in the $|GHZ\rangle$ state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle\right), \tag{2.44}$$

where individual qubits subsequently belong to Alice, Bob and Carol. This state is called the Greenberger-Horne-Zeileinger state (GHZ state). One can check that all two-particle density matrix are the same and equal to $\rho_{AB} = \rho_{BC} = \rho_{AC} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$. This state is mixed, classically correlated but also separable. All pairs are unentangled. The GHZ state can be rewritten as the following superposition

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left[|\Phi^+\rangle_{AB} \otimes \frac{1}{\sqrt{2}}(|0\rangle_C + |1\rangle_C) + |\Phi^-\rangle_{AB} \otimes \frac{1}{\sqrt{2}}(|0\rangle_C - |1\rangle_C)\right], \tag{2.45}$$

where $|\Phi^\pm\rangle_{AB}$ represent particles Alice and Bob in the Bell states. Now we can ask Carol to perform the measurement on her particle in the base $\frac{1}{\sqrt{2}}(|0\rangle_C + |1\rangle_C)$, $\frac{1}{\sqrt{2}}(|0\rangle_C - |1\rangle_C)$. Independently of how Carol is far away from Alice and Bob, particles Alice and Bob will collapse into one of maximally entangled Bell states $|\Phi^+\rangle_{AB}$ or $|\Phi^-\rangle_{AB}$, which is separated from the particle of Carol. Hence using only LOCC operation we are able to prepare an entangled pair. But we have already mentioned that LOCC operations cannot increase entanglement between parties. A solution of this disagreement comes from the fact, that the $|GHZ\rangle$ state contains *three-way* (or three-partite) entanglement.

In a straightforward way we can extend these considerations to multi-partite systems. We define a multi-partite GHZ state

$$|\Phi^+\rangle_N = \frac{1}{\sqrt{N}}\left(|0\rangle^{\otimes N} + |0\rangle^{\otimes N}\right). \tag{2.46}$$

This state contains only N-*way* (or N-partite) entanglement. So N-partite entanglement is a type of entanglement which critically involves all N particles. A general state of N particles can contain various types of entanglement as 2-way, 3-way, 4-way entanglement and so on. The complex structure of entanglement makes the investigation of this phenomenon difficult.

So far we do not have neither any reasonable and reputable criterion for separability of N particles nor computable multipartite entanglement measure for general mixed states. There have been several proposal made for entanglement measures of multipartite states (see e.g. [68, 73, 74, 75, 76, 77]). However each of them is very hard to evaluate for mixed states.

Despite of this drawback, searching for multipartite entanglement measures shed new light and boots our understanding of the structure of multipartite entanglement. The story was started in the year 2000, when Valerie Coffman, Joydip Kundu and William K. Wootters discovered an interesting quantity for a tripartite two-level (qubit) system, referred to as the *residual entanglement*.

Consider three qubits, let say A, B and C, in a state ρ_{ABC} [73]. The residual entanglement is defined by

$$\tau_{ABC} = C^2_{A(BC)} - C^2_{AB} - C^2_{AC}, \tag{2.47}$$

where C_{AB} and C_{AC} are the bipartite concurrences of the original state ρ_{ABC} with traces taken over qubits C and B, respectively. $C_{A(BC)}$ is the concurrence of the bipartite state $\rho_{A(BC)}$ with qubits B and C regarded as a single object. The latter subsystem (BC) consists of two qubits and therefore one could be surprised, because the concurrence was originally defined for bipartite system of two qubits. Let us explain it. For subsystems of one and two qubits the bipartite concurrence is defined as follows. Let first consider that the original three-qubit state is pure. Then the reduced density matrices $\rho_A = \mathrm{Tr}_{BC}\,\rho_{ABC}$ and $\rho_{BC} = \mathrm{Tr}_A\,\rho_{ABC}$ have the same nonzero eigenvalues (see section 2.1.1). The first reduced density matrix ρ_A has only two eigenvalues and therefore also the second two-qubit density matrix ρ_{BC} has at the most two nonzero eigenvalues. Hence we can regard the second two-qubit subsystem as one qubit and define the concurrence $C_{A(BC)}$ for the pure state ρ_{ABC} as (2.38)

$$C_{A(BC)}(\rho_{ABC}) = 2\sqrt{\det(\rho_A)}. \tag{2.48}$$

The generalization of the concurrence $C_{A(BC)}$ for a mixed state ρ is given by the convex roof (2.29)

$$C_{A(BC)}(\rho) = \inf_{\{p_i,|\phi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle), \quad \text{with} \quad p_i > 0 \quad \text{and} \quad \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.49}$$

The residual entanglement (2.47) is a well defined measure for three-way entanglement of three qubits, unfortunately very bad computable for mixed states. The values of the residual entanglement τ are confined to the interval $[0, 1]$. Therefore for three qubits the CKW (Coffman-Kundu-Wootters) inequality is fulfilled

$$C^2_{AB} + C^2_{AC} \leq C^2_{A(BC)}. \tag{2.50}$$

The right side of the inequality (2.50) is bound by 1, whilst the left side can achieve at the first sight even number 2. The important message extracted from CKW inequality is that *bipartite entanglement in a three-qubit system cannot be shared freely.*

The question, whether the generalized CKW inequality

$$C_{12}^2 + C_{13}^2 + ... + C_{1n}^2 \leq C_{1(2...n)}^2 \leq 1 \tag{2.51}$$

is also valid for a system of n qubits, was remaining long time unanswered. This longstanding inequality was testified by all examined cases but proved only recently by Tobias J. Osborne and Frank Verstraete in 2006 [78]. Again, this CKW inequality tells us that the sum of squares of bipartite concurrencies between first qubit and the others is bounded above by one.

Here we have to emphasize that we have spoken first about sharing of bipartite quantum correlations in multi-qubit systems and thus this limitation is related just to bipartite entanglement. One can expect that similar restrictions of sharing entanglement will be found for various type of entanglement structures. A hopeful progress in this direction was done by Chang-shui Yu and He-shan Song [75, 77].

Chapter 3

Sharing of bipartite entanglement in multi-qubit systems

As we have already discussed in the previous part, bi-partite entanglement in multi-qubit systems cannot be shared freely. The rules of quantum mechanics impose severe restrictions on how multi-qubit systems can be entangled. This observation induces a new question, namely, which types of entanglement structures are carried by quantum states. First works, which focused on this problem, have studied special states of multi-qubit systems that maximize bi-partite entanglement between selected pairs of qubits in the system [79, 80, 81, 82].

The entanglement properties of a multi-qubit system may be represented mathematically in several ways. Dür [82], for instance, has introduced *entanglement molecules*: mathematical objects representing distributions of bi-partite entanglement in a multi-qubit system. He has shown that given an entanglement molecule, relevant *mixed* states with the corresponding entanglement properties can be found.

An alternative possibility for representing the entanglement relations of a multi-qubit system is the application of *entangled graphs*. The entanglement properties of a system of N qubits are represented by a graph of N vertexes. The vertexes refer to qubits, while the edges of the graph represent the presence of entanglement between the corresponding pair of qubits. It was shown that for every possible graph one can find a pure state, which would be represented by that graph [83]. The amount of pairwise entanglement was however not taken into account.

3.1 Sharing of entanglement in entangled graphs

In the present chapter we extend the concept of entangled graphs to describe the amount of pairwise entanglement in the system as well. We present a complete analysis of existence of quantum states of multi-qubit systems with entanglement properties represented by a given particular graph. We prove in the following, that if an additional criterion is fulfilled, namely that the weight of each edge is bounded from above by a certain value, a pure state corresponding to the given graph can be found. This bound on the weights depends only on the number of qubits in the system. We also propose a constructive method, how to find these states.

3.1.1 Entangled graphs

Let us consider a system of N qubits, labeled 1,2, ...n, in a state ρ. As we have already mentioned, we represent the entanglement properties of the system with a weighted graph with N vertexes. Every qubit is identified with one of the vertexes, whereas the entanglement (quantified by the concurrence) between a pair of qubits is identified with a weighted edge, connecting relevant vertexes. If a pair of qubits is not entangled at all, there is no edge present in the graph between the relevant vertexes (thus, the edge with a zero weight is equivalent to no edge). Thus the graph itself is defined by the number of qubits N and a set of real numbers C_{ij}, giving the concurrencies between relevant pairs of qubits.

Having a pure or mixed state, it is always possible to determine the graph, corresponding to the state. To find the graph one has to calculate concurrencies of all pairs of qubits. In contrast, the opposite question, turns out to be much more difficult. For a given graph, many quantum states may be appropriate. The graph itself is not, for instance, sensitive to local unitary operations on the qubits. On the other hand, there exist graphs for which no suitable state can be found. The reason behind this is that bi-partite entanglement cannot be shared freely: e.g. the CKW inequalities (2.51) form an obstacle. So, for instance, we cannot have an entangled graph of three qubits such that each pair is maximally entangled with the value of concurrence equal to unity.

Thus the question of interest is: Given a graph, does there exist a state of the whole system having the desired graph as its bipartite entanglement representation?

The question of existence of states with specific distribution of bi-partite entanglement have been studied by several authors. In particular, Dür [82] studied a distribution of bipartite entanglement between every pair of qubits that are prepared in a *mixed state*. He showed that it is possible to construct a corresponding mixed state for every entangled graph with the total

concurrence (given as a simple sum of concurrencies over all pairs in the graph) equal with one.

In the work of Koashi et. all. [81], the authors have studied fully symmetric states (with respect to all permutation of qubits) of N qubits such that all $N(N-1)/2$ pairs of qubits in the system are entangled with the same degree of entanglement, i.e. all edges have the same weight. They have shown that under these conditions the maximal concurrence takes the value

$$C_{\max} = \frac{2}{N}. \tag{3.1}$$

A state satisfying this condition is the well known W-state defined as

$$|W\rangle = |N;1\rangle, \tag{3.2}$$

where $|N;k\rangle$ is a totally symmetric state of N qubits, with k qubits in the state $|1\rangle$ and all the others in the state $|0\rangle$.

As we have mentioned earlier, it has been proved, that all N-qubit states have to fulfil the CKW inequalities (2.51). Any violation of this inequality means that the corresponding entangled graph cannot be represented by a physical state. Under the assumption that all concurrencies C_{kj} in (2.51) are mutually equal, i.e. $C \equiv C_{kj}$, we obtain from the CKW inequality the bound

$$C \leq \frac{1}{\sqrt{N}}.$$

which is not achievable. To see this we remind ourselves, that in the case of the entangled web (all qubits are mutually entangled) the maximal value of the concurrence is given by equation (3.1), which is much lower than the bound that following from the CKW inequality.

One may proceed by deriving tighter CKW-type inequalities that can be saturated by physical states (graphs). Alternatively, one can consider only entangled graphs with specifically bounded weights on their edges. The following two parts deal with results obtained by following the second approach. For better lucidity, the first part is intended for the formulation of our main results and the second part contains all necessary proofs.

3.1.2 Theorem for graphs with bounded edges

We restrict our following considerations to those graphs in which the concurrence is smaller than a certain value. Then it is possible to show that there exists a nonzero bound on the concurrence such that all graphs with weighted edges that satisfy this additional condition can be realized by pure states. These states are of the form

$$|\Psi\rangle = \alpha|A\rangle + \sum_{\{i,j\}} \gamma_{ij}|B_{ij}\rangle, \tag{3.3}$$

where

$$|B_{ij}\rangle \equiv (|11..0_i..0_j..1\rangle + |00..1_i..1_j..0\rangle) \; ; \tag{3.4}$$

$$|A\rangle \equiv (|00...0\rangle + |11...1\rangle) \; . \tag{3.5}$$

α and γ_{ij} are real positive coefficients that satisfy the normalization condition

$$2\alpha^2 + 2\sum_{\{i,j\}} \gamma_{ij}^2 = 1. \tag{3.6}$$

The sums in equations (3.3) and (3.6) go through all pairs $i < j$, $i, j \in N$ (or, equivalently, the sums can be extended for all pairs $i, j \in N$ with the restriction $\gamma_{ij} = 0$ for $j \leq i$). Due to the high (permutational) symmetry of the state one can calculate directly the concurrence (see section 3.1.3)

$$C_{ij} = \max\left\{2\left(2\alpha\gamma_{ij} - \sum_k \gamma_{ki}^2 - \sum_k \gamma_{kj}^2\right), 0\right\}, \tag{3.7}$$

which is valid under the condition

$$\alpha \geq 2\gamma_{\max}\sqrt{N-2}\,, \tag{3.8}$$

where $\gamma_{\max} = \max_{i,j}(\gamma_{ij})$.

Notice, that the concurrence between every pair of qubits of this rather complicated system is expressed as an analytic function of input parameters, utilizing just a single condition (3.8).

The set of $\frac{N(N-1)}{2}$ non-linear equations (3.7) connects parameters of the state γ_{ij} (the parameter α is specified by gammas via the normalization condition) with the concurrencies of different pairs of qubits. This set of equations is strongly coupled in a sense that in order to calculate one concurrence one needs to use approximately $2N$ gammas. The task now is to invert this set of equations, i.e. to find the set of equation defining the gammas via the set of concurrencies that are given (these concurrencies do specify the character of the entangled graph). Not for every possible choice of concurrencies there exist parameters γ_{ij} satisfying the normalization condition $\Sigma_{i,j}\,|\gamma_{ij}|^2 < 1$ and (3.8), as concurrencies have to fulfil the CKW inequalities and one also knows, that this condition is not sufficient. Hence, it is also an interesting question, for which set of concurrencies one can find solutions of the reversed equations (3.7).

We have found the solution for the parameters γ_{ij} as functions of the concurrencies C_{ij} (weights on the edges of the entangled graph) that specify the state (3.3), providing all concurrencies are smaller than a certain maximal value

$$C_{ij} \leq C_{\max}, \tag{3.9}$$

where $C_{\max}$ is a given constant. The upper bound for $C_{\max}$ is obtained from conditions for the iteration procedure as defined in section 3.1.3. There is also a precise formula for $C_{\max}$ (3.20), for which $C_{\max} > 0.45N^{-1}$ holds.

Now we can formulate a theorem dealing with entangled graphs with weighted edges:

Theorem 3.1.1 *Every entangled graph with weighted edges specified by the set of concurrencies* $\{C_{ij}\}$*, that fulfil the condition (3.9), can be represented by a pure state given by equation (3.3).*

The complete proof of this Theorem is given in section 3.1.3. Here we just sketch how the relevant parameters γ_{ij} can be obtained via an iteration algorithm, where one starts from a specific state (3.3) corresponding to the situation when

$$C_{ij} = C_{\max}$$

for all i, j and then adjusts iteratively the parameters γ_{ij} to fit the concurrencies. We can summarize the iteration process in the followings main points:

- After each step, all the concurrencies that are evaluated for the state (3.3) are greater than or equal to the desired set of concurrencies C_{ij}.
- After each step, all gammas are smaller than or equal to their values at the previous step; they do not change only if (for a specific i, j the relevant concurrence is reached.
- The iteration limit, when all gammas are zero, leads to zero concurrencies, too. Therefore, one has to cross the searched state during the iteration procedure (for a finite precision this stage can be achieved after a finite number of iteration steps)

The existence of the state itself is proved by showing, that the iteration process has a proper limit. Also, to ensure the validity of the proposed process, we made numerical tests, with varying number of qubits and the strength of entanglement. In all tested examples that satisfied the condition (3.9), a fast convergence was observed. A precision of about 10^{-6} of the maximal permitted concurrence was achieved after nine to twelve steps (changing all gammas at once).

3.1.3 Proofs of theorems

First of all we prove the validity of the formula for the concurrence (3.7).

Formula for concurrence

In what follows we will evaluate the concurrence for an arbitrary pair of qubits given by the state (3.3), i.e.

$$|\Psi\rangle = \alpha\left(|00...00\rangle + |11...11\rangle\right) + \sum_{\{i,j\}} \gamma_{ij}\left(|11\rangle_{ij}|00...00\rangle_{\overline{ij}} + |00\rangle_{ij}|11...11\rangle_{\overline{ij}}\right) , \tag{3.10}$$

where the real positive amplitudes α and γ_{ij} satisfy the normalization condition

$$2\alpha^2 + 2\sum_{\{i,j\}} \gamma_{ij}^2 = 1. \tag{3.11}$$

The sums in equations (3.10) and (3.11) go through all pairs $i \neq j$, $i, j \in \hat{N}$, so $\{i, j\} = \{j, i\}$ and thus $\gamma_{ij} = 0$ for $i < j$. The special form of the state (3.10) leads to a rather compact form of the density matrix for an arbitrary two-qubit operator that is obtained by tracing over the rest of the graph qubits:

$$\rho_{ij} = \begin{pmatrix} A & 0 & 0 & F \\ 0 & B & E & 0 \\ 0 & E & B & 0 \\ F & 0 & 0 & A \end{pmatrix} , \tag{3.12}$$

where we have used the notation

$$\begin{aligned} A &= \gamma_{ij}^2 + \alpha^2 + \sum_{\{k,l\}} \gamma_{kl}^2 , \\ B &= \sum_k \left(\gamma_{kj}^2 + \gamma_{ki}^2\right) , \\ E &= 2\sum_k \gamma_{ki}\gamma_{jk} , \\ F &= 2\alpha\gamma_{ij} . \end{aligned} \tag{3.13}$$

All sums in equations (3.13) are running through free parameters k and l, whereas i and j do denote a specific pair of qubits in the graph. In addition, the condition $i \neq k \neq l \neq j$ has to be fulfilled.

The convenient form of the matrix (3.12) allows us to calculate square roots of the eigenvalues of the matrix R given by equation (2.36):

$$\begin{aligned} \lambda_1 &= A + F , \\ \lambda_2 &= A - F , \\ \lambda_3 &= B + E , \\ \lambda_4 &= B - E . \end{aligned} \tag{3.14}$$

Because the coefficients A, B, E, F are positive, the only candidates for the largest eigenvalue are λ_1 and λ_3. Let us further define

$$\gamma_{\max} = \max_{i,j}(\gamma_{ij})\,. \tag{3.15}$$

Using the condition

$$\alpha \geq 2\gamma_{\max}\sqrt{N-2} \tag{3.16}$$

we find $\lambda_1 \geq \lambda_3$ and the general expression for the concurrence associated with edges of the entangled graph prepared in the state (3.10) reads

$$C_{ij} = \max\left\{2\left(2\alpha\gamma_{ij} - \sum_{\{k,i\}}\gamma_{ki}^2 - \sum_{\{k,j\}}\gamma_{kj}^2\right), 0\right\}. \tag{3.17}$$

In the next part we give the proof of the theorem (3.1.1).

Proof of theorem

Let us first label the set of concurrencies that determine a given entangled graph by $\mathbf{C}_{ij}$. We will use a bold $\mathbf{C}$ in order to distinguish these concurrencies from any intermediate concurrencies, obtained by the iteration process.

We will start the iteration procedure which allows us to find a pure state that corresponds to a given entangled graph with weighted edges that is specified by a set of concurrencies $\{C_{ij}\}$ with an initial state of the entangled graph given by equation (3.3). The amplitudes γ_{ij} are specified by the relation

$$\gamma_{ij}^{(0)} \equiv \frac{\lambda}{\sqrt{2+N(N-1)\lambda^2}}\,, \tag{3.18}$$

that is, the initial state is completely permutation symmetric. The parameter λ is defined as

$$\lambda = \frac{\sqrt{4(N-2)^2+2N(N-1)}-2(N-2))}{N(N-1)}. \tag{3.19}$$

The corresponding bi-partite concurrencies can be evaluated straightforwardly

$$\begin{aligned} C_{ij}^{(0)} &= C_{\max} = 2\left(\alpha^{(0)}\gamma_{ij}^{(0)} - 2(N-2)(\gamma_{ij}^{(0)})^2\right) \\ &= \frac{\sqrt{6N^2-18N+16}-2N+4}{N(N-1)}. \end{aligned} \tag{3.20}$$

The parameters $\alpha^{(0)}$ and $\gamma_{ij}^{(0)}$ are mutually connected via the normalization condition (3.6). Therefore α is always implicitly defined by γ_{ij}. It is also clear that for the state under consideration the condition (3.8) is fulfilled as well.

Before we describe the iteration procedure itself we introduce the following notation: we enumerate all pairs of qubits in the entangled graph. All pairs of qubits (i.e. the edges of the graph) are listed in the set of pairs just once. At each iteration step one parameter γ_{kl} for a selected pair of indices $\{k,l\}$ is changed, whereas all others gammas will stay unchanged. Let us now suppose, that the n-th step of the iteration is done and both conditions (3.8) and (3.9) are still fulfilled. Moreover $\alpha^{(n)}$,$\gamma_{ij}^{(n)}$ are positive. Hence we find

$$C_{ij}^{(n)} \geq \mathbf{C}_{ij}\,, \tag{3.21}$$

$$\alpha^{(n)} \geq 2\sqrt{N-2}\gamma_{\max}^{(n)}\,, \tag{3.22}$$

$$0 < \alpha^{(n)} \leq 1 \qquad 0 \leq \gamma_{ij}^{(n)} < 1\,, \tag{3.23}$$

for all pairs of indices i,j. The parameter $\gamma_{\max}^{(n)}$ is defined in the same way as in equation (3.15), i.e.

$$\gamma_{\max}^{(n)} = \max_{i,j}(\gamma_{ij}^{(n)}). \tag{3.24}$$

In the following iteration step we take a next pair of qubits (the edge) in the list. Let us denote this pair with indices $\{i,j\}$. Then, in the $(n+1)-st$ iteration step, we will change the parameters of the state in the following way:

$$\gamma_{ij}^{(n+1)} = \frac{U^{(n)} - V^{(n)}}{2}\,, \tag{3.25}$$

$$\alpha^{(n+1)} = \frac{U^{(n)} + V^{(n)}}{2}\,, \tag{3.26}$$

where

$$U^{(n)} = \left[(\alpha^{(n)} + \gamma_{ij}^{(n)})^2 + \frac{1}{2}(\mathbf{C}_{ij} - C_{ij}^{(n)})\right]^{1/2}\,,$$

$$V^{(n)} = \left[(\alpha^{(n)} - \gamma_{ij}^{(n)})^2 - \frac{1}{2}(\mathbf{C}_{ij} - C_{ij}^{(n)})\right]^{1/2}\,.$$

All other gammas remain unchanged at this step. The conditions (3.21) and (3.22) guarantee that this iteration step is well defined. Now we will discuss several important properties of the iteration process:

(1) $\alpha^{(n+1)}$ and $\gamma_{ij}^{(n+1)}$ are solutions of the equation

$$\alpha^{(n+1)}\gamma_{ij}^{(n+1)} = \alpha^{(n)}\gamma_{ij}^{(n)} + \frac{1}{4}\left(\mathbf{C}_{ij} - C_{ij}^{(n)}\right) \tag{3.27}$$

and thus according to equation (3.7)

$$\begin{aligned} C_{ij}^{(n+1)} &= \max\left\{2\left(2\alpha^{(n+1)}\gamma_{ij}^{(n+1)} - \sum_{\{k,i\}}(\gamma_{ki}^{(n+1)})^2 - \sum_{\{k,j\}}(\gamma_{kj}^{(n+1)})^2\right), 0\right\} \\ &= \max\{\mathbf{C}_{ij}, 0\} = \mathbf{C}_{ij}. \end{aligned} \tag{3.28}$$

(2) $\alpha^{(n+1)}$ and $\gamma_{ij}^{(n+1)}$ fulfil the normalization condition (3.6).

(3) $\gamma_{ij}^{(n+1)}$ and $\alpha^{(n+1)}$ are positive and satisfy the relations

$$0 \leq \gamma_{ij}^{(n+1)} < \gamma_{ij}^{(n)} \tag{3.29}$$

$$\alpha^{(n)} < \alpha^{(n+1)} \leq 1. \tag{3.30}$$

(4) From equations (3.29) and (3.30) it follows that

$$\alpha^{(n+1)} > \alpha^{(n)} \geq 2\sqrt{N-2}\gamma_{\max}^{(n)} \geq 2\sqrt{N-2}\gamma_{\max}^{(n+1)}. \tag{3.31}$$

Therefore the condition (3.22) is valid also for the $(n+1) - st$ iteration step.

(5) Let us now show, how concurrencies change in the iteration step. For $k, l \neq i, j$ we find

$$\begin{aligned} C_{kl}^{(n+1)} &= 2\left(2\alpha^{(n+1)}\gamma_{kl}^{(n+1)} - \sum_{\{k,m\}}\left(\gamma_{km}^{(n+1)}\right)^2 - \sum_{\{l,m\}}\left(\gamma_{lm}^{(n+1)}\right)^2\right) \\ &= 2\left(2\alpha^{(n+1)}\gamma_{kl}^{(n)} - \sum_{\{k,m\}}\left(\gamma_{km}^{(n)}\right)^2 - \sum_{\{l,m\}}\left(\gamma_{lm}^{(n)}\right)^2\right) \\ &> 2\left(2\alpha^{(n)}\gamma_{kl}^{(n)} - \sum_{\{k,m\}}\left(\gamma_{km}^{(n)}\right)^2 - \sum_{\{l,m\}}\left(\gamma_{lm}^{(n)}\right)^2\right) \\ &= C_{kl}^{(n)} \end{aligned} \tag{3.32}$$

and for $k = i$

$$\begin{aligned} C_{il}^{(n+1)} &= 2\left(2\alpha^{(n+1)}\gamma_{il}^{(n+1)} - \sum_{\{i,m\}}\left(\gamma_{im}^{(n+1)}\right)^2 - \sum_{\{l,m\}}\left(\gamma_{lm}^{(n+1)}\right)^2\right) \\ &= 2\left(2\alpha^{(n+1)}\gamma_{il}^{(n)} - \sum_{\{i,m\}}\left(\gamma_{im}^{(n+1)}\right)^2 - \sum_{\{l,m\}}\left(\gamma_{lm}^{(n)}\right)^2\right) \\ &> 2\left(2\alpha^{(n)}\gamma_{kl}^{(n)} - \sum_{\{i,m\}}\left(\gamma_{im}^{(n)}\right)^2 - \sum_{\{l,m\}}\left(\gamma_{lm}^{(n)}\right)^2\right) \\ &= C_{il}^{(n)}. \end{aligned} \tag{3.33}$$

The same is valid also for $k = j$.

We have shown, that after this iteration step the concurrence for fixed i, j (i.e. for the given edge) will be $C_{ij}^{(n+1)} = \mathbf{C}_{ij}$ and all other concurrencies of the entangled graph will become larger. Thus, the condition for all i, j $C_{ij}^{(n+1)} \geq \mathbf{C}_{ij}$ will be fulfilled. Therefore, the state defined by equation (3.3) with the parameters $\gamma_{ij}^{(n+1)}$ can be used for the next $(n+2)$-nd iteration step. Hence, the whole iteration is well defined and we obtain an infinite sequence of parameters $\left\{\alpha^{(n)}\right\}_{n=0}^{\infty}$ and $\left\{\gamma_{ij}^{(n)}\right\}_{n=0}^{\infty}$ for each pair of indices i,j (i.e. for each edge of the entangled graph). All sequences are monotonous and bounded, and therefore they have proper limits. Let us denote these limits as α and γ_{ij}

$$\alpha = \lim_{n\to\infty} \alpha^{(n)} \qquad \Rightarrow \qquad \alpha \in (0, 1\rangle \tag{3.34}$$

$$\gamma_{ij} = \lim_{n\to\infty} \gamma_{ij}^{(n)} \qquad \Rightarrow \qquad \gamma_{ij} \in \langle 0, 1). \tag{3.35}$$

Now we choose and fix one pair of indices i,j and we show, that

$$\lim_{n\to\infty} C_{ij}^{(n)} = \mathbf{C}_{ij}. \tag{3.36}$$

First we define a sequence $\{k(n)\}_{n=0}^{\infty}$ in the following way: $k(1) = p$, where p is the rank of $\{i, j\}$ in the order of pairs of indices, and $k(n) = p + \frac{nN(N-1)}{2}$. Then

$$C_{ij}^{(k(n))} = \mathbf{C}_{ij}. \tag{3.37}$$

The equation (3.36) is equivalent to the definition

$$(\forall\, \varepsilon \in \mathbb{R}_+, \varepsilon > 0)\, (\exists n_0 \in \mathbf{N})\, (\forall\, n \in \mathbf{N}, n > n_0) \left(|C_{ij}^{(n)} - \mathbf{C}_{ij}| < \varepsilon\right). \tag{3.38}$$

Let us choose and fix the small parameter ε. Our task is to find n_0, that satisfies the property (3.38). Because all sequences $\left\{\alpha^{(n)}\right\}_{n=0}^{\infty}$ and $\left\{\gamma_{kl}^{(n)}\right\}_{n=0}^{\infty}$ have a proper limit, they are Cauchy sequences and therefore

$$(\forall\, \tau \in \mathbb{R}_+, \tau > 0)\, (\exists m_0 \in \mathbf{N})\, (\forall\, n, m \in \mathbf{N}, n, m > m_0)\, (\forall\{k, l\}) \begin{pmatrix} |\alpha^{(n)} - \alpha^{(m)}| < \tau \\ |\gamma_{kl}^{(n)} - \gamma_{kl}^{(m)}| < \tau \end{pmatrix}, \tag{3.39}$$

where

$$\tau = \frac{\varepsilon}{4N(N-1)}\,. \tag{3.40}$$

For this τ there exists such m_0, that the property (3.39) is fulfilled and we can define n_0 as

$$n_0 \equiv k(m_0) > m_0 \tag{3.41}$$

Further we will calculate the difference $|C_{ij}^{(n+1)} - C_{ij}^{(n)}|$ for $n+1 > n_0$ and $n+1 \notin \{k(n)\}_{n=0}^{\infty}$. The last condition means, that the $(n+1) - st$ iteration step did not change $\gamma_{ij}^{(n)}$. From equations (3.89) and (3.92) we obtain two options for the difference under consideration, either

$$\left|C_{ij}^{(n+1)} - C_{ij}^{(n)}\right| = 4\left|\alpha^{(n+1)} - \alpha^{(n)}\right|\left|\gamma_{ij}^{(n)}\right| < 4\tau < 8\tau\,, \tag{3.42}$$

or

$$\begin{aligned} |C_{ij}^{(n+1)} - C_{ij}^{(n)}| &= \left|4(\alpha^{(n+1)} - \alpha^{(n)})\gamma_{ij}^{(n)} - 2(\gamma_{il}^{(n+1)})^2 + 2(\gamma_{il}^{(n)})^2\right| \\ &< 4\left|\alpha^{(n+1)} - \alpha^{(n)}\right|\left|\gamma_{ij}^{(n)}\right| + 2\left|\gamma_{il}^{(n+1)} - \gamma_{il}^{(n)}\right|\left|\gamma_{il}^{(n+1)} + \gamma_{il}^{(n)}\right| \\ &< 8\tau, \end{aligned}$$

where $\gamma_{il}^{(n)}$ is the parameter, which was changed in the $(n+1) - st$ iteration step.

Finally, we can say for $n > n_0$, if $n \in \{k(n)\}_{n=0}^{\infty}$, then $|C_{ij}^{(n)} - \mathbf{C}_{ij}| = 0$. In the opposite case there exists such $u \in \mathbf{N}_0$, that

$$n \in \langle k(m_0+u), k(m_0+u+1)\rangle. \tag{3.43}$$

Thus

$$\begin{aligned} \left|C_{ij}^{(n)} - \mathbf{C}_{ij}\right| &= \left|(C_{ij}^{(n)} - C_{ij}^{(n-1)}) + (C_{ij}^{(n-1)} - C_{ij}^{(n-2)}) + \cdots + \underbrace{(C_{ij}^{(k(m_0+u))} - \mathbf{C}_{ij})}_{=0}\right| \\ &< \frac{8N(N-1)\tau}{2} = \varepsilon. \end{aligned}$$

But then it must hold

$$\begin{aligned} \mathbf{C}_{ij} = \lim_{n\to\infty} C_{ij}^{(n)} &= \lim_{n\to\infty} 2\left(2\alpha^{(n)}\gamma_{ij}^{(n)} - \sum_{\{k,i\}}(\gamma_{ki}^{(n)})^2 - \sum_{\{k,j\}}(\gamma_{kj}^{(n)})^2\right) \\ &= 2\left(2\alpha\gamma_{ij} - \sum_{\{k,i\}}\gamma_{ki}^2 - \sum_{\{k,j\}}\gamma_{kj}^2\right). \end{aligned}$$

All other conditions remain fulfilled in the limit form as well. Because this is valid for all pairs of indices, we have found the parameters γ_{ij}, that define the state (3.3) which corresponds to a given entangled graph.

3.1.4 Conclusion

We have introduced a concept of entangled graphs with weighted edges. We have proved, that a whole class of entangled graphs with the concurrence between an arbitrary pair of qubits (vertexes) weaker than a certain value does exist in a sense that corresponding pure states of N qubits can be found that satisfy the constraints imposed by weights on the edges of the graph.

Here we would like to recall that the proof of theorem (3.1.1) involves an iteration procedure and is in a certain sense constructive. Based on this iteration procedure included in the proof, in the paper [84] a quantum network for preparation of states of entangled graphs was proposed. This network is composed of a number of elementary quantum gates that is quadratic in the number of vertexes (qubits) in the graph. Here we do not go into details as the network construction was not the primarily task of the author.

3.2 Sharing of entanglement in linear passive networks with one and two excitations

The previous section dealt with the general problem of sharing bipartite entanglement in qubit systems. In this part we focus on the study of quantum interference effects in passive optical networks for single and two photon inputs. We focus primarily on the analysis of the behavior of entanglement between the output modes of the network. We also study the inverse problem, i. e. to determine what type of bipartite entanglement structure (entangled graphs) can be prepared by a passive network. We specify the general results for the particular case of Ising-type networks with balanced beam-splitters.

3.2.1 Single photon entanglement distribution in linear passive networks

The propagation of the probability distribution of a single-particle state (probability that we find the state in a given mode) in linear passive networks (including as a special case Ising-type networks) is closely linked to the distribution of entanglement in these networks [85, 86]. Entanglement refers to the quantum correlations between the particular output modes. We demonstrate this fact for a general one particle state and a general passive network. We consider a general linear passive network characterized by the unitary transformation matrix U between

the input and the output modes creation operators

$$\begin{pmatrix} b_1^\dagger \\ b_2^\dagger \\ \vdots \\ b_N^\dagger \end{pmatrix} = U \begin{pmatrix} a_1^\dagger \\ a_2^\dagger \\ \vdots \\ a_N^\dagger \end{pmatrix}; \qquad U = \begin{pmatrix} U_{11} & U_{12} & \dots & U_{1N} \\ U_{21} & U_{22} & \dots & U_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ U_{N1} & U_{N2} & \dots & U_{NN} \end{pmatrix}. \tag{3.44}$$

Let us choose an arbitrary one-particle input state

$$|\psi_{in}\rangle = \sum_{i=1}^{N} \alpha_i |1_i\rangle = \sum_{i=1}^{N} \alpha_i a_i^\dagger |0\rangle, \qquad \sum_{i=1}^{N} |\alpha_i|^2 = 1, \tag{3.45}$$

where the state $|1_i\rangle$ denotes the state with zeros in all modes, except the i-th mode with a single photon (excitation). Then the output state has the form

$$|\psi_{out}\rangle = \mathcal{U}|\psi_{in}\rangle = \sum_{i=1}^{N} \alpha_i \mathcal{U} a_i^\dagger |0\rangle = \sum_{i=1}^{N} \alpha_i \mathcal{U} a_i^\dagger \mathcal{U}^\dagger \mathcal{U}|0\rangle = \sum_{k=1}^{N} \left(\sum_{i=1}^{N} U_{ki}\alpha_i \right) |1_k\rangle, \tag{3.46}$$

where $\mathcal{U}$ denotes the propagator of the network. The probability to find a photon in the n-th output mode is

$$P(n) = |\langle 1_n|\psi_{out}\rangle|^2 = \left| \sum_{i=1}^{N} U_{ni}\alpha_i \right|^2. \tag{3.47}$$

In the following we will investigate the evolution of bipartite quantum correlations (entanglement between two modes) using the concurrence (2.37) as the entanglement measure.

To proceed we need to calculate the entanglement between two chosen arbitrary modes i, j of the output state $|\psi_{out}\rangle$. At first we have to determine the density operator of the two particular modes

$$\begin{aligned} \rho_{ij} &= Tr_{rest \neq i,j}(|\psi_{out}\rangle\langle\psi_{out}|) = \\ &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & |\sum_k U_{ik}\alpha_k|^2 & (\sum_k U_{ik}\alpha_k)(\sum_k U_{jk}\alpha_k)^* & 0 \\ 0 & (\sum_k U_{ik}\alpha_k)^*(\sum_k U_{jk}\alpha_k) & |\sum_k U_{jk}\alpha_k|^2 & 0 \\ 0 & 0 & 0 & \sum_{l\neq i,j} |\sum_k U_{lk}\alpha_k|^2 \end{pmatrix} \end{aligned} \tag{3.48}$$

The simple form of the matrix (3.48) gives us the possibility to express the eigenvalues of the

matrix $R(\rho_{ij})$ analytically (see (2.36)). We obtain the following expressions for the eigenvalues

$$\begin{aligned}\lambda_1 &= 4\left|\sum_k U_{ik}\alpha_k\right|^2\left|\sum_k U_{jk}\alpha_k\right|^2,\\ \lambda_2 &= 0,\\ \lambda_3 &= 0,\\ \lambda_4 &= 0.\end{aligned} \tag{3.49}$$

From (2.37) follows that the concurrence reads

$$C(\rho_{ij}) = 2\left|\sum_k U_{ik}\alpha_k\right|\left|\sum_k U_{jk}\alpha_k\right|. \tag{3.50}$$

Due to the equation for the photon number distribution (3.47) we get

$$C(\rho_{ij}) = 2\sqrt{P(i)P(j)}. \tag{3.51}$$

Let us emphasize that the obtained result is completely independent on the chosen type of the passive network and is valid for all one-particle input states. The structure of bipartite entanglement of the output state has taken a simple form., i.e. it is completely determined by the mode population probabilities. All modes with non-zero probability $P(n)$ are mutually entangled. The remaining unpopulated modes stay unentangled. The degree of entanglement is independent of the relative phases between the populated modes.

3.2.2 Controlling entanglement in passive networks with one excitation

In the previous section we have settled the question how entanglement depends on the prescribed form of the passive network. Next we will reverse the task. We will determine what type of bipartite entanglement structure can be prepared by passive network and how to obtain the prescribed entanglement structure. We formulate this problem in terms of concurrence.

From the previous section we know that only such entanglement structures can be realized in which populated modes are entangled with each other. Without loss of generality, suppose we have the first n (where $n \leq N$) modes populated with a prescribed set of concurrences C_{ij} ($C_{ij} \neq 0$) for each pair of modes i and j. Using C_{ij} we will always assume that $i \neq j$ (note that $C_{ij} = C_{ji}$). Generally, all states with one excitation generated by a passive network have the form

$$|\psi\rangle = \sum_{i=1}^{n} \lambda_i |1_i\rangle, \qquad \sum_{i=1}^{n} |\lambda_i|^2 = 1. \tag{3.52}$$

In the same way as in the previous section we obtain the relation for concurrence between modes i and j

$$C_{ij} = 2|\lambda_i||\lambda_j|. \tag{3.53}$$

From the set of equations (3.53) we can express the probabilities

$$|\lambda_j|^2 = \frac{C_{ij}C_{kj}}{2C_{ik}} \quad i \neq k \neq j. \tag{3.54}$$

Therefore the concurrencies C_{ij} have to fulfill the equation

$$\frac{C_{ij}C_{kj}}{C_{ik}} = \frac{C_{aj}C_{bj}}{C_{ab}}, \tag{3.55}$$

which has to be valid for all $i, j, k, a, b \in \hat{n}$. Now we fix three indices (modes) i, j and k (naturally $i \neq j \neq k$). Therefore all the concurrencies C_{ab} (where a,$b \neq i$) can be expressed as a function of concurrencies C_{ia} and the concurrence C_{jk}

$$C_{ab} = \frac{C_{ia}C_{ib}}{C_{ij}C_{ik}}C_{jk}, \tag{3.56}$$

and for $b = j$ we have

$$C_{aj} = C_{ia}\frac{C_{ik}}{C_{jk}}. \tag{3.57}$$

Moreover, the coefficients λ_i defined by (3.54) have to fulfill the normalization condition (3.52). If we use the set of equations (3.54) the normalization condition takes the form

$$2 = \frac{C_{ij}C_{ik}}{C_{jk}} + \frac{C_{ij}C_{jk}}{C_{ik}} + \sum_{a=1,a\neq i,j}^{n} \frac{C_{ia}C_{ja}}{C_{ij}}, \tag{3.58}$$

which, with the help of equation (3.57), results in

$$2 = \frac{C_{ij}C_{ik}}{C_{jk}} + \frac{C_{jk}}{C_{ij}C_{ik}} \sum_{a=1,a\neq i}^{n} C_{ia}^2. \tag{3.59}$$

Now, it is useful to rewrite the equation (3.59) in the form

$$2 = x + \frac{K}{x}, \qquad \text{where} \quad x = \frac{C_{ij}C_{ik}}{C_{jk}} \quad \text{and} \quad K = \sum_{a=1,a\neq i}^{n} C_{ia}^2. \tag{3.60}$$

The direct consequence of the equation (3.60) is the inequality

$$0 < K = \sum_{a=1,a\neq i}^{n} C_{ia}^2 \leq 1 \tag{3.61}$$

with two possible solutions of x

$$x = 1 \pm \sqrt{1-K}. \tag{3.62}$$

The two possible solutions of C_{jk} follow from the equations (3.62) and (3.60)

$$C_{jk} = \frac{C_{ij}C_{ik}}{1+\sqrt{1-K}} \tag{3.63}$$

or

$$C_{jk} = \frac{C_{ij}C_{ik}}{1-\sqrt{1-K}}. \tag{3.64}$$

Both solutions are physical because they fulfill the condition $0 < C_{jk} < 1$. With the help of (3.63) (resp. (3.64)) the equation (3.56) reads

$$C_{ab} = \frac{C_{ia}C_{ib}}{1+\sqrt{1-K}}, \tag{3.65}$$

$$(\text{resp.} \quad C_{ab} = \frac{C_{ia}C_{ib}}{1-\sqrt{1-K}}). \tag{3.66}$$

and $a, b \neq i$. Finally we can express the absolute values of the coefficients λ_i in terms of concurrencies C_{ia}. From equations (3.54), (3.57) and (3.63) (resp. (3.64)) we get

$$\begin{aligned} |\lambda_j|^2 &= \frac{C_{1j}^2}{2(1 \pm \sqrt{1-K})}, \qquad \text{for} \quad j \neq i; \\ |\lambda_i|^2 &= \frac{1}{2}(1 \pm \sqrt{1-K}). \end{aligned} \tag{3.67}$$

Let us now summarize the obtained results into the following theorem.

Theorem 3.2.1 *Every bipartite entanglement structure $\{C_{ij}\}$, where $C_{ij} \neq 0$ for all pair of indices (i,j), can be represented by a pure state (3.52) if and only if for an arbitrary chosen and fixed index (mode) i the condition (3.61) is fulfilled and for all indices a and b (where $a, b \neq i$) the condition (3.65) (resp. (3.66)) is fulfilled. If both conditions are fulfilled we can represent this bipartite entanglement structure by a pure state (3.52), where $|\lambda_j|^2 = \frac{C_{ij}^2}{2(1+\sqrt{1-K})}$, for all $j \neq i$ and $|\lambda_i|^2 = \frac{1}{2}(1+\sqrt{1-K})$, (resp. $|\lambda_j|^2 = \frac{C_{ij}^2}{2(1-\sqrt{1-K})}$, for all $j \neq i$ and $|\lambda_i|^2 = \frac{1}{2}(1-\sqrt{1-K})$).*

Let us point out two important features. First, it is clear that this bipartite entanglement structure is generated by the set of concurrencies $\{C_{ij}\}$ between the one chosen mode i and the rest of the populated modes. Second, these concurrencies must be chosen in accordance with the restriction rule (3.61). But these restrictions are actually the well known conjectured generalized CKW inequalities (see section 2.2.4).

It should be emphasized that the form of the entangled state is not unique due to the fact that only the absolute values of the expansion coefficients λ_i are determined. Also the optical network generating such a state is not unique. For example, if we want to construct a network which generates the desired state when we send a single photon into one particular mode, then we have defined just one row of the transfer matrix of the optical network, while the others remain unspecified. The only additional restriction we impose on the form of the transfer matrix is that it should form a unitary matrix. This freedom of choice of the rest of the transfer matrix can be used to simplify the construction (using additional constrains) of the optical network with beam-splitters and phase-shifters using for instance the Zeilinger method [87].

3.2.3 Optimization of entanglement distribution in passive networks with one excitation

In the following we will denote $C_{ij} = C(\rho_{ij})$ for $i \neq j$ and $C_{ii} = 0$. For the purpose of optimization we define a function of the total value of the bipartite entanglement for a system described by its density matrix ρ

$$\tau(\rho) = \sum_{(ij)} C_{ij}^2, \tag{3.68}$$

where we sum over all pairs of indices. In the following we will understand under the problem of optimizing the entanglement distribution the maximization of the function (3.68).

From (3.51) follows, after the summation over the index j, the relation (using the normalization condition)

$$\sum_j C_{ij}^2 = 4P(i)[1 - P(i)]. \tag{3.69}$$

After the second summation over the index i we get

$$\sum_{i,j} C_{ij}^2 = 4(1 - \sum_i P(i)^2), \tag{3.70}$$

and all pairs of indices (i, j) appeared in the sum twice. Therefore we take only one half to arrive finally at

$$\sum_{(i,j)} C_{ij}^2 = 2(1 - \sum_i P(i)^2). \tag{3.71}$$

We have to maximize (3.71) with the additional condition $\sum_i P(i) = 1$. It is not difficult to show that

$$0 \leq \sum_{(i,j)} C_{ij}^2 \leq 2(1 - \frac{1}{N}) = \frac{N(N-1)}{2} \left(\frac{2}{N}\right)^2. \tag{3.72}$$

Thus the maximum attainable value of $\tau(\rho)$ is

$$\tau_{max}(N) = 2\left(1 - \frac{1}{N}\right), \tag{3.73}$$

and is achieved for $P(i) = \frac{1}{N}$. In this case all pairs of qubits are entangled alike and the single pair entanglement has the value

$$C_{ij} = \frac{2}{N}. \tag{3.74}$$

Hence the optimization of the function τ (3.68) for one-photon states leads us to the same value achieved by Koashi et al. [81] (see section 3.1).

It is important to realize that the identification of an optimal network is closely related to the given input state. For example, we wish to construct a network which distributes in the optimal way entanglement for the case, when we send a single excitation into one mode (no superposition between the input modes). In this case the condition $P(i) = \frac{1}{N}$ for all $i \in \hat{N}$ is equivalent to the condition $|U_{mn}|^2 = \frac{1}{N}$ for all $m, n \in \hat{N}$. This condition fulfils for example the discrete Fourier transform in all its possible forms [88, 89].

3.2.4 Entanglement distribution in passive networks with two photon input

The quantification of entanglement in the case of two excitations in the network is a bit more involved than in the case of a single excitation. A closed expression for the concurrence quantifying the amount of entanglement can be derived for the particular case when the total probability of detecting two photons at any of the outputs goes to zero for large network (large number of output parts). In this case we can limit ourselves to the description of quantum state propagation for states having the form $|0_i\rangle|1_j\rangle...|1_k\rangle...|0_l\rangle$, $(j \neq k)$, i.e. in each of the modes at most one excitation is present. In this case the application of the concurrence concept is completely legitime and reflects properly the entanglement distribution within the network.

The requirement on the extinction of the two photon probabilities is for instance satisfied for the nearest neighbour Ising model (or the Fourier transform acting on all the inputs) for two photon inputs via one input mode. When all the single photon output probabilities scale typically as $1/N$ the individual two photon probabilities at one output will scale as $1/N^2$. From this follows that the total probability that two photons emerge from the network via any of the outputs scales as $1/N$ and hence tends to zero for large enough networks. In the following, we will neglect the probability of the double excitations in one mode.

Let us choose an arbitrary two-particle input state

$$|\psi_{in}\rangle = \sum_{(ij)} \alpha_{ij} a_i^\dagger a_j^\dagger |0\rangle + \frac{1}{\sqrt{2}} \sum_{i=1}^{N} \alpha_i a_i^{\dagger 2} |0\rangle = \sum_{(ij)} \alpha_{ij} |1_i 1_j\rangle + \sum_{i=1}^{N} \alpha_i |2_i\rangle, \tag{3.75}$$

where in the first term the summation is done over all $\binom{n}{2}$ pairs of different indexes i, j. Then the output state has the form

$$|\psi_{out}\rangle = \sum_{k,l=1}^{N} \left\{ \sum_{(ij)} U_{ki} U_{lj} \alpha_{ij} + \sum_{i=1}^{N} \frac{1}{\sqrt{2}} U_{ki} U_{li} \alpha_i \right\} b_k^\dagger b_l^\dagger |0\rangle. \tag{3.76}$$

To simplify the lengthy notation we denote

$$\begin{aligned} \beta_{kl} &= \sum_{(ij)} 2 U_{ki} U_{lj} \alpha_{ij} + \sum_{i=1}^{N} \sqrt{2} U_{ki} U_{li} \alpha_i \\ \beta_k &= \sum_{(ij)} \sqrt{2} U_{ki} U_{kj} \alpha_{ij} + \sum_{i=1}^{N} U_{ki} U_{ki} \alpha_i, \end{aligned} \tag{3.77}$$

using these coefficients we can rewrite the output state in the form

$$|\psi_{out}\rangle = \sum_{(kl)} \beta_{kl} |1_k 1_l\rangle + \sum_{k=1}^{N} \beta_k |2_k\rangle. \tag{3.78}$$

To fulfill the condition that the two-photon excitations must vanish we have to put $\beta_k = 0$ for all modes k. The renormalized output state then has the form

$$|\psi_{out}\rangle = \frac{1}{K} \sum_{(kl)} \beta_{kl} |1_k 1_l\rangle, \tag{3.79}$$

where K is determined by

$$K^2 = \sum_{(kl)} |\beta_{kl}|^2. \tag{3.80}$$

The reduced density operator of two fixed modes a and b is easily evaluated, the result is given by

$$\rho_{ab} = \begin{pmatrix} |\beta_{ab}|^2 & 0 & 0 & 0 \\ 0 & \sum_{k \neq a,b} |\beta_{ak}|^2 & \sum_{k \neq a,b} \beta_{ak} \beta_{bk}^* & 0 \\ 0 & \sum_{k \neq a,b} \beta_{ak}^* \beta_{bk} & \sum_{k \neq a,b} |\beta_{bk}|^2 & 0 \\ 0 & 0 & 0 & \sum_{(kl) \neq (ab)} |\beta_{kl}|^2 \end{pmatrix}. \tag{3.81}$$

and the normalization constant was absorbed into the definition of β_{kl}.

To evaluate the degree of entanglement between two chosen modes we have to determine the eigenvalues of the matrix (2.36) associated with the reduced density matrix (3.81). For the eigenvalues we obtain the following expressions

$$\lambda_{1,2} = \left(\sqrt{\sum_{k\neq a,b} |\beta_{ak}|^2 \sum_{k\neq a,b} |\beta_{bk}|^2} \pm |\sum_{k\neq m,n} \beta_{ak}\beta^*_{bk}| \right)^2 \tag{3.82}$$

$$\lambda_{3,4} = \left(|\beta_{ab}| \sqrt{\sum_{(k,l)\neq a,b} |\beta_{kl}|^2} \right)^2 \tag{3.83}$$

A necessary condition for the existence of entanglement between the modes a, b is that the eigenvalue λ_1 is larger than the eigenvalues $\lambda_{3,4}$. Using these eigenvalues and the expression for the concurrence (2.37) we obtain

$$C_{ab} = 2max(|\sum_{k\neq a,b} \beta_{ak}\beta^*_{bk}| - |\beta_{ab}| \sqrt{\sum_{(k,l)\neq a,b} |\beta_{kl}|^2}, 0). \tag{3.84}$$

Let us emphasize that the obtained result holds generally for any two particle state superpositions of the form (4.20). The expressions for the concurrence differs in their characters from the simpler type valid for single photon concurrence. First of all the concurrence depends not only on the absolute value of the expansion coefficients but also on their relative phases. The single photon concurrence was dependent only on the absolute value of the amplitudes.

The expression for the concurrence can be written for the special type of state with two photons in the same input mode

$$|\psi_{in}\rangle = \frac{1}{\sqrt{2}} \hat{a}_i^{\dagger 2} |0\rangle \tag{3.85}$$

in a simplified way. With the help of the definition (3.77) and the fact that $\beta_i = 0$ for all modes i we obtain the following form of the eigenvalues

$$\begin{aligned} \lambda_1 &= 2\sqrt{(\sum_{k\neq a,b} |\beta_{ak}|^2)(\sum_{l\neq a,b} |\beta_{bl}|^2)}, \\ \lambda_{2,3} &= |\beta_{ab}| \sqrt{\sum_{(kl)\neq(ab)} |\beta_{kl}|^2}, \\ \lambda_4 &= 0. \end{aligned} \tag{3.86}$$

We now define the following probabilities of detecting the photons:

- $P\binom{ij}{}$ - the probability of detecting a photon in each of the modes i and j,
- $P\binom{}{ij}$ - the probability that no photons will be detected in modes i and j,

- $P\binom{i}{j}$ - the probability of detecting one photon in mode i and no photon in mode j,

$$\begin{aligned} P\binom{ij}{} &= |\langle 1_i 1_j|\psi_{out}\rangle|^2 = \langle 11|\rho_{ij}|11\rangle = |\beta_{ij}|^2 \\ P\binom{}{ij} &= \sum_{(kl)\neq(ij)} |\langle 1_k 1_l|\psi_{out}\rangle|^2 = \langle 00|\rho_{ij}|00\rangle = \sum_{(kl)\neq(ij)} |\beta_{kl}|^2 \\ P\binom{i}{j} &= \sum_{k\neq i,j} |\langle 1_i 1_k|\psi_{out}\rangle|^2 = \langle 10|\rho_{ij}|10\rangle = \sum_{k\neq i,j} |\beta_{ik}|^2 \end{aligned} \tag{3.87}$$

With the help of these probabilities we can rewrite the eigenvalues (3.86) and express the concurrence of modes a and b in a simple form

$$C_{ab} = 2\left[\sqrt{P\binom{a}{b}P\binom{b}{a}} - \sqrt{P\binom{}{ab}P\binom{ab}{}}\right]. \tag{3.88}$$

3.2.5 Balanced Ising-type network

In the previous sections we have derived results on entanglement which are valid for all passive networks. In the following we use these results to describe the spreading of entanglement in the balanced Ising network with one photon. Let us first of all give a small introduction to Ising-type networks.

Ising-type networks

One of the advantages of optical networks is the simplicity of its mathematical description. The basic element of the whole network is the beam splitter [90] described by the transfer matrix A having the form (we do not consider the most general form)

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{3.89}$$

The angle θ determines the transmittivity and reflectivity of the beam splitter. The network with nearest neighbour coupling is now formed by repeating a sequence of beam splitters with two different transmittivities specified by angles θ, ϕ as illustrated in Fig. 3.1. The transfer

matrix U is determined as a product of two block diagonal matrices

$$U = \begin{bmatrix} B_{22} & 0 & 0 & \cdots & & B_{21} \\ 0 & & & & & \\ & & B & & & \\ 0 & & & & & \\ \vdots & & & B & & \\ & & & & \ddots & \\ B_{12} & & & & & B_{11} \end{bmatrix} \begin{bmatrix} \boxed{\text{A}} & & 0 & 0 & \cdots & \\ & & 0 & 0 & \cdots & \\ 0 & 0 & & & & \\ & & & A & & \\ 0 & 0 & & & & \\ \vdots & \vdots & & & \ddots & \\ & & & & & A \end{bmatrix}. \tag{3.90}$$

The matrix B is defined as

$$B = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}. \tag{3.91}$$

Defining the network transform we used periodic boundary condition (elements B_{12}, B_{21}). This fact will not play any role in the following considerations. The action of the whole network on the input creation operators is defined by the application of the product of the two matrices

$$W(M) = U^M \tag{3.92}$$

The matrix U will be called the motif (see Fig.3.1), the application of one of the block diagonal matrices will represent one layer. The properties of the network are determined by the eigenvalues of the matrix U. It was shown [91, 92] that the eigenvalues $\exp(\pm i\lambda_n)$ of the matrix U can be determined from the equation

$$\cos\lambda_n = \cos\theta\cos\phi + \cos\left(\frac{2\pi n}{N}\right)\sin\theta\sin\phi, \tag{3.93}$$

where N is the number of beam splitters in one layer. For balanced beam splitters $\phi = \theta = \pi/4$, we will consider in the following, the equation (3.93) reduces to

$$\cos\lambda_n = \frac{1}{2}\left[1 + \cos\left(\frac{2\pi n}{N}\right)\right]. \tag{3.94}$$

Using these eigenvalues many of the simpler properties of finite networks (finite system of beam splitters with periodic boundary conditions) like recurrences in the mode population for a single photon input can be understood. The propagation of the photon number density was studied in great detail and became known as the quantum random walk [93]. The basic difference in this respect is that the actual single photon distribution across the output modes differs significantly from the classical random walk analogue. The maximum of the probability is not centered close to the input channel but is located at the outer wings of the distribution.

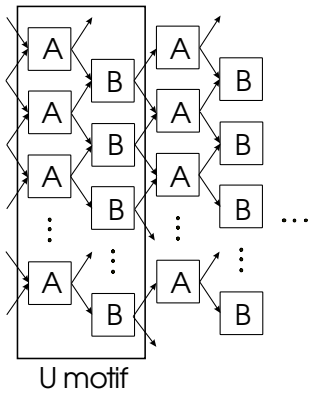

Figure 3.1: Ising-type network with two types of transformations repeated successively. The two layers of beam-splitters of type A and B form the motif U.

The width of the distribution in the quantum case is much larger than in the classical case. The variance of the probability distribution grows quadratically with time (i.e. motifs passed), in contrast with the linear dependence for the classical random walk.

One photon in the balanced network

Let us study the case, when we are sending one excitation into one of the modes (no superposition between the modes at the input) to the infinite network. Because the network is infinite and translation invariant with respect to the inputs it does not matter through which of the inputs the excitation is entering the network.

The propagation of the probability distribution of a single excitation in the network in dependence on the traversed motifs is shown in Fig.3.2. The plot clearly illustrates the well-known unusual behavior, when one of the direction of spreading is preferred. In the next graph Fig.3.3 the propagation of bipartite entanglement along particular motifs is shown.

In agreement with (3.51) we observe that also the propagation of bipartite entanglement prefers the same direction, the concurrence exhibits similar oscillatory behavior like the photon number distribution.

Two photon in the balanced network

Consider two photons entering into the balanced Ising-type network. The way how the entanglement evolves in the Ising-type network is shown in Fig.3.4. The plot starts after the photons have passed through 30 motifs and shows the evolution up to 100 motifs. This is due to the fact

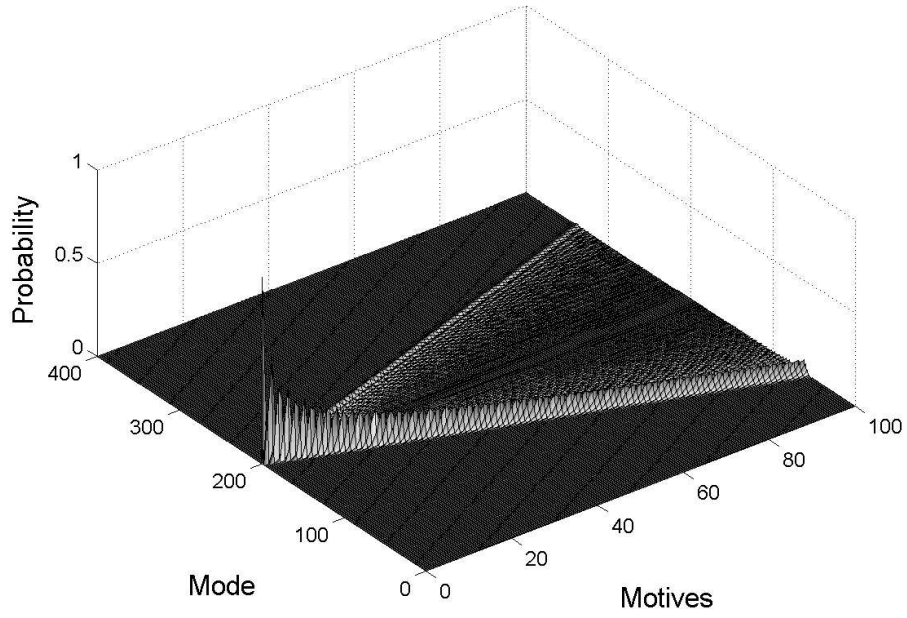

Figure 3.2: The probability of finding the excitation in an arbitrary mode and motif. The excitation starts its propagation in the input state $|1_{200}\rangle$ and is numerically evaluated for 100 motifs.

that for small number of motifs passed we cannot omit the two-photon excitations. After the photons pass through 30 motifs the total probability of detecting two excitations in one mode is smaller than 5 % so we can neglect the two-photon contributions.

Let us analyze the total amount of entanglement in the network, which we measure by the function (3.68). In contrast to the single photon case we cannot give a simple formula for this function due to the complicated form of the bipartite concurrence (3.84). Thus the maximization of the overall entanglement in the two photon case is much more difficult compared to the single photon case. We evaluated numerically the function $\tau(N)$ for the case of balanced Ising network with two photons entering in the state (3.85). We compare this value with the value for the even distribution (note that we have $4N$ modes populated after N motifs applied), for which we obtain

$$C_{ij} = \frac{(4N - 2 - \sqrt{(2N-1)(4N-3)})}{N(4N-1)}, \qquad i \neq j, \tag{3.95}$$

i. e. all populated modes are equally entangled. The overall entanglement has the value

$$\tau_1(N) = \frac{2(4N - 2 - \sqrt{(2N-1)(4N-3)})^2}{N(4N-1)}. \tag{3.96}$$

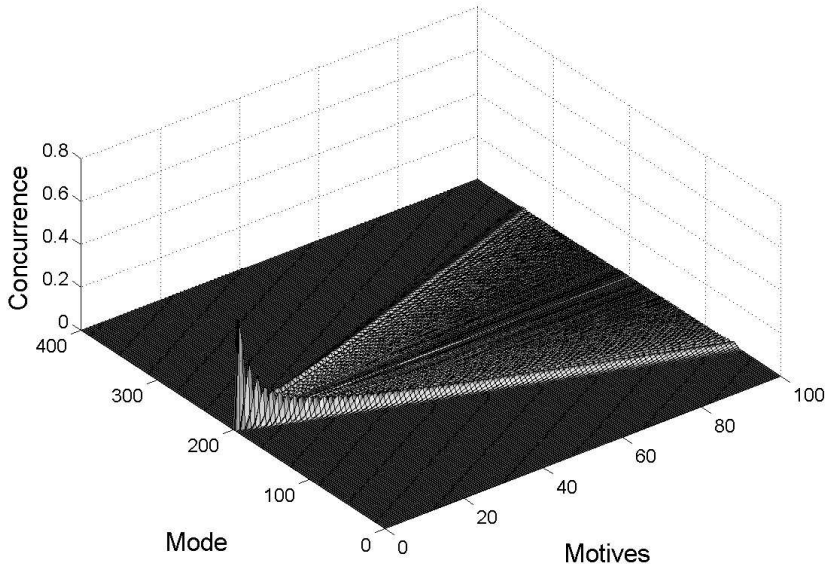

Figure 3.3: Graph of the concurrence between mode 200 and the others in dependence on the number of motifs traversed. The excitation starts its propagation in the input state $|1_{200}\rangle$ and is numerically simulated up to 100 motifs.

The limit value of this function is

$$\lim_{N\to+\infty} \tau_1(N) = 12 - 8\sqrt{2} \approx 0.686, \tag{3.97}$$

thus we can see that the overall entanglement in the network with two excitations is reduced dramatically compared to the network with single excitation, where the limit value was 2. Figure 3.5 illustrates how the total concurrences evolve with the number of motifs passed N. The numerical simulations suggest that they converge, similar to the case of the single photon initial state.

For the case of the single photon input the uniform distribution was the optimal one concerning the overall entanglement. To show that this is no more valid for the case of two photons, we consider the following factorized two photon state of the form

$$|\psi\rangle = \frac{1}{\sqrt{2N}} \sum_{i=1}^{2N} |1_{2i}\rangle \otimes \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} |1_{2i+1}\rangle. \tag{3.98}$$

In this case the two photons are completely independent, one is uniformly distributed over odd modes and the second one over even modes. The bipartite entanglement structure has the

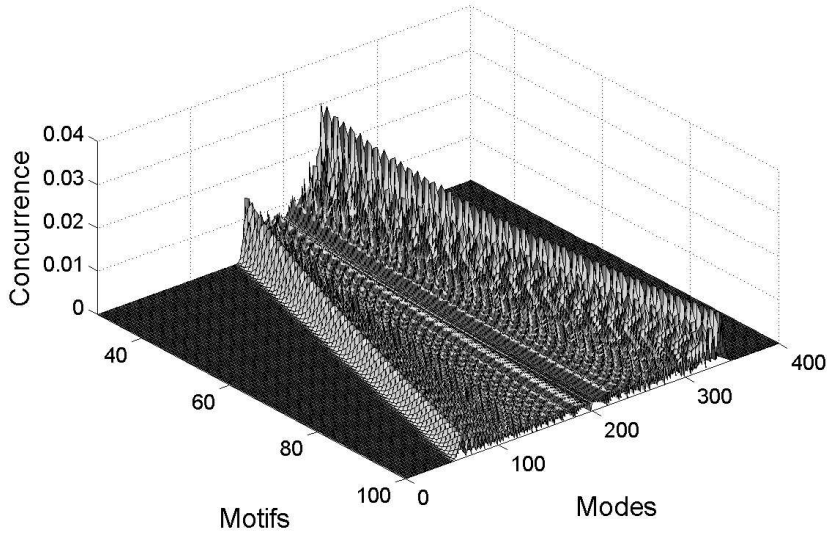

Figure 3.4: Graph of the concurrence between mode 200 and the others in dependence on the number of motifs traversed. The two excitations start the propagation in the input state $|2_{200}\rangle$ and are numerically simulated up to 100 motifs.

following form

$$\begin{aligned} C_{2i,2j+1} &= C_{2j+1,2i} = 0, \qquad i = 1, ..., N,\ j = 0, ..., N-1, \\ C_{2i,2j} &= C_{2i+1,2j+1} = \frac{1}{N}, \qquad i \neq j, \end{aligned} \tag{3.99}$$

i. e. only odd or even modes are equally entangled together, odd modes stay unentangled with the even modes and vice versa. Thus the sum of squared concurrences can be decomposed into the sum over odd and even pairs of indexes and equals to

$$\tau_2(N) = \sum_{kl} C^2_{(ab)} = 4\left(1 - \frac{1}{2N}\right), \tag{3.100}$$

which reaches asymptotically the value 4. Compared to this value the value for the uniformly distributed states (3.96) is very moderate.

The very moderate amount of entanglement for the even distributed state is a price that has to be paid to the additional high symmetry of the bipartite entanglement between the modes. For the uniformly distributed state with the distribution (3.96) all the bipartite concurrences are the same. When we relax this condition states can be found for which the total amount of entanglement will increase.

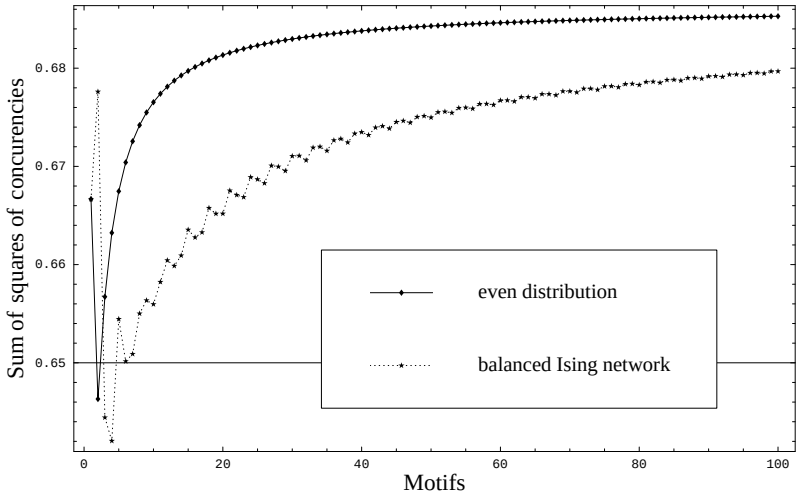

Figure 3.5: Graph of sum of squared concurrencies in dependence on the number of motifs traversed. The two excitations start the propagation in the input state $|2_{200}\rangle$ and are numerically simulated up to 100 motifs.

3.2.6 Conclusion

We studied the evolution of single and two photon states in passive optical network, in particular in passive networks realizing nearest neighbour interaction (Ising model). We derived closed form expression for the degree of entanglement for general passive networks, found the general structure of bipartite entanglement and proved what the maximum entanglement for single photon input is. In addition, we have shown that for special initial states the maximum attainable entanglement can be almost reached with the Ising-type passive network. For two photon inputs we derived closed form expressions for bipartite entanglement for a broad class of states (realized for instance by the Ising-type networks). We have shown that the total amount of entanglement reached in Ising-type networks is rather moderate compared to the maximum obtainable value for special (exhibiting a certain symmetry) two photon states.

Chapter 4

Entanglement in quantum processing

In chapter 1 we have shown that two important quantum information processes: quantum copying and quantum complementing (NOT operation) of an arbitrary unknown state, cannot be done perfectly. These observations have stimulated fresh interest in studying both processes. This chapter deals with results which we have obtained while studying the role of entanglement in quantum processing. The chapter is divided into two main parts. The first part is devoted to cloning of pure two-qubit states with a given degree entanglement. In the second part we study how quantum entanglement influences our ability to perform the quantum NOT operation on pure two-qubit entangled states.

In both cases the system of our interest are two qubits. Our motivation for restricting our investigation to two-qubit input states is threefold. Firstly, qubit states still play a dominant role in the area of quantum information processing. Secondly, it is expected that in this simplest case the intricate relations between entanglement and fundamental limits imposed on quantum copying processes by the fundamental laws of quantum theory are exposed in a particularly transparent way. Thirdly, we can treat the problem analytically. In order to put the problem into perspective let us consider two distinguishable spin-1/2 particles (qubits). Their associated four dimensional Hilbert space $\mathscr{H}$ can be decomposed into *classes of pure two-qubit states* Ω_α *with the same degree of entanglement*. These classes are represented by the sets

$$\Omega_\alpha = \Big\{ \big(U_1 \otimes U_2\big)\big(\alpha|\uparrow\rangle \otimes |\uparrow\rangle + \beta|\downarrow\rangle \otimes |\downarrow\rangle\big) \Big| U_1, U_2 \in \mathsf{SU}(2) \Big\}. \tag{4.1}$$

Thereby the parameter α $(0 \leq \alpha \leq 1)$ with $\beta = \sqrt{1-\alpha^2}$ characterizes the degree of entanglement of the pure states in a given class Ω_α and the kets $|\uparrow\rangle$ and $|\downarrow\rangle$ constitute an orthonormal basis of the two-dimensional single-qubit Hilbert spaces of each of the qubits. Relation (4.1)

takes into account that local unitary operations of the form $U_1 \otimes U_2$ are the most general transformations which leave the degree of entanglement of a bipartite quantum state invariant. Our further investigation is based on the fact that each set of entangled states Ω_α is invariant under the unitary group $\mathsf{SU}(2) \otimes \mathsf{SU}(2)$. It allows us to use the covariant approach for studying of optimal quantum maps proposed in section 1.8.

Due to the symmetry relation $\Omega_\alpha = \Omega_{\sqrt{1-\alpha^2}}$ we can restrict our further considerations to the parameter range $0 \leq \alpha \leq 1/\sqrt{2}$. Note that in the special case $\alpha = 0$ the two-qubit state is separable whereas in the opposite extreme case $\alpha = 1/\sqrt{2}$ it is maximally entangled. Furthermore, it should be noted that each class Ω_α contains an orthonormal basis of $\mathscr{H}$.

4.1 Optimal copying of entangled two-qubit states

Because, as a matter of principle, it is impossible to design a perfect cloning machine we are looking for the best possible approximates. The best possible approximates are called optimal copying machines or optimal copying processes. The definition of the needed process involves several ingredients. It should reflect certain symmetries. The formulation of the problem involves and its output depends on the quantification criteria we impose on the output. The imposed criteria induce an optimization procedure on the output states. In principle, the optimization procedure depends on many factors, like e.g. set of cloned states, asymmetric versus symmetric copying machines (cloner), the chosen figure of merit. The result of the optimization with respect to these factors could be generally different.

Most of previous work [31, 32, 33, 34, 35] focused on so called universal cloning machine (UCM), when the set of the states to be cloned is the whole Hilbert space. One of the simplest problems of UCM, the so called m-to-n cloner (a machine producing n imperfect copies from m identical input quantum systems in a pure state) was completely settled. It was found that the result does not depend on which figure of merit we choose. It was shown that the ideal processes are the same whether we try to optimize the quality of a single copy or the quality of the whole (m-copy) output state with respect to the idealized (m-copy) output state.

First investigations addressing the problem of copying entanglement have been performed recently [39]. In this latter work it was demonstrated that entanglement cannot be copied perfectly. Thus, if one can find a quantum operation which perfectly duplicates entanglement, it necessarily does not preserve separability. Furthermore, for the special case of maximally entangled two-qubit states first copying processes were constructed which maximize the fidelity of each two-qubit copy separately.

In this part we address the general problem of copying pure two-qubit states of an arbitrarily given degree of entanglement in an optimal way. Thus, we are interested in constructing quantum processes T_α which copy an arbitrary pure two-qubit state, say qubit one and two in the state $|\psi\rangle \in \Omega_\alpha$, in an optimal way, i.e.

$$T_\alpha : \rho_0 \equiv \rho_{in} \otimes \rho_{ref} \longrightarrow \rho_{out}, \tag{4.2}$$

with $\rho_{in} = |\psi\rangle\langle\psi|$ denoting the density operator of the input state. The resulting four-qubit output state is denoted by ρ_{out}. The appropriately chosen two-qubit quantum state ρ_{ref} characterizes the state of the copying device and we denote these qubits as qubit three and four. According to the fundamental laws of quantum theory the quantum map T_α has to be a linear and completely positive.

4.1.1 Figures of merit

To be able to decide which process is better we have to use a figure function. We define two measures, quantitative expressions, of how the real output is close to the ideal one. Both definitions arise from the fidelity (see Appendix A), which is well applicable for pure states.

Let us consider two states of a physical system described by density operators, one in a pure state $\sigma = |\phi\rangle\langle\phi|$ and the second with a general density operator ρ. The fidelity reads

$$F(\rho, \sigma) = Tr(\rho\sigma) = \langle\phi|\rho|\phi\rangle. \tag{4.3}$$

Now we have two possibilities. The first one, we can quantify the quality of the whole output ρ_{out}; the *global fidelity* between the real output ρ_{out} and the ideal output $|\phi\rangle\langle\phi| \otimes |\phi\rangle\langle\phi|$

$$\langle\phi|\langle\phi|\rho_{out}|\phi\rangle|\phi\rangle \tag{4.4}$$

and as the figure of merit $F_2(T_\alpha)$ we take the worst case

$$F_2(T_\alpha) = \inf_{|\phi\rangle\in\Omega_\alpha} \{\langle\phi|\langle\phi|\rho_{out}|\phi\rangle|\phi\rangle\} = \inf_{|\phi\rangle\in\Omega_\alpha} \{\langle\phi|\langle\phi|T_\alpha(|\phi\rangle|\phi\rangle\}\,. \tag{4.5}$$

In the following we will call this measure the *four-particle test* and its optimum, *optimal four-particle copying process.*

The second possibility is to gauge each copy separately. We can express the density operators for both subsystems (first subsystem formed by qubits one and two and the second subsystem formed by qubits three and four) and evaluate the *single (individual) fidelities* between the input pure state and these subsystem density operators

$$\langle\phi|\rho_{12}|\phi\rangle, \qquad \langle\phi|\rho_{34}|\phi\rangle, \tag{4.6}$$

where $\rho_{12(34)} = \mathrm{Tr}_{34(12)}\,\rho_{out}$ are density operator of the first (second) copy. Remember that generally, the fidelities between the subsystem density operators and the input state are different and in this case we talk about *asymmetric cloners*. In this text we are interested in and we limit oneself to the study of so called *symmetric cloners*, where both copies are identical $\rho_{12} = \rho_{34}$ and thus both quantities in (4.6) are equal. Again, we define as the figure of merit the worst case, which can happen

$$F_1(T_\alpha) = \inf_{|\phi\rangle\in\Omega_\alpha} \{\langle\phi|\rho_{12}|\phi\rangle\}\,. \tag{4.7}$$

In the following this measure of quality will be called the *two-particle test* and the optimal process, which maximizes the two-particle test, we will call the *optimal two-particle copying process* (or machine).

Thus, constructing an optimal four-particle (resp. two-particle) copying process is equivalent to maximizing $F_2(T_\alpha)$ (resp. $F_1(T_\alpha)$) over all possible quantum processes. Let us denote these optimal fidelities by $F_2^\alpha \equiv \sup_{T_\alpha} F_2(T_\alpha)$ and $F_1^\alpha \equiv \sup_{T_\alpha} F_1(T_\alpha)$. At this point we would like to emphasize that both figures of merit: two-particle and four-particle test are based on merit functions, which fulfill the requirements of covariant optimization introduced in section 1.8. Indeed, both merit functions $\delta_2(\rho,\sigma) = \mathrm{Tr}(\rho\sigma)$ and $\delta_1(\rho,\sigma) = \mathrm{Tr}(\mathrm{Tr}_{34}\,\rho\,\mathrm{Tr}_{34}\,\sigma)$ (with ρ and σ being four-qubit density operators) :

- are linear in both arguments and thus concave in the first argument
- reach their maximum for $\rho = \sigma$
- fulfil the invariance property

$$\delta_{1(2)}(\rho, \mathcal{U}\sigma\mathcal{U}^\dagger) = \delta_{1(2)}(\mathcal{U}^\dagger\rho\mathcal{U}, \sigma) \tag{4.8}$$

for $\mathcal{U} = U_1 \otimes U_2 \otimes U_1 \otimes U_2$ ($U_{1(2)}$ are arbitrary elements of the group $\mathsf{SU}(2)$).

Now, it is simple to check, that the ideal (quantum mechanically non-achievable) copying map $\mathcal{K} : \mathsf{S}(\mathscr{H}) \to \mathsf{S}(\mathscr{H}\otimes\mathscr{H})$ defined as $\mathcal{K}(\rho) = \rho\otimes\rho$, fulfills the covariance condition

$$\mathcal{K}(U\rho U^\dagger) = U\otimes U\mathcal{K}(\rho)U^\dagger\otimes U^\dagger, \tag{4.9}$$

where ρ is an arbitrary density operator acting on the Hilbert space $\mathscr{H}$ and U any element of $\mathsf{SU}(\mathscr{H})$. In particular, the equation (4.9) is valid for $U = U_1\otimes U_2$ with $U_{1(2)} \in \mathsf{SU}(2)$. Therefore all conditions of the covariant approach proposed in section 1.8 are fulfilled:

- an arbitrary set Ω_α of two-qubit states with the same degree entanglement are invariant under a transformation $U = U_1 \otimes U_2$, where $U_{1(2)} \in \mathsf{SU}(2)$,

- the ideal copying process is covariant (4.9),
- both merit functions $\delta_1(\rho,\sigma)$ and $\delta_2(\rho,\sigma)$ are concave with maximum for $\rho=\sigma$ and fulfil the invariance property (4.8).

Hence we know that for any optimal two-particle (resp. four-particle) copying process $T_\alpha^{1(2)}$ one can always find an equivalent covariant quantum process $\widehat{T}_\alpha^{1(2)}:\rho_{in}\otimes\rho_{ref}\rightarrow\rho_{out}^{1(2)}$ with the characteristic covariant property

$$\rho_{\rm out}^{1(2)}(U\rho_{\rm in}U^\dagger) \;=\; U\otimes U\rho_{\rm out}^{1(2)}(\rho_{in})U^\dagger\otimes U^\dagger \tag{4.10}$$

with $U=U_1\otimes U_2$. These equivalent covariant quantum processes yield the same optimal fidelity $\langle\phi|\rho_{12}|\phi\rangle$ (resp. $\langle\phi|\langle\phi|\rho_{out}|\phi\rangle|\phi\rangle$) for all possible two-qubit input states $|\phi\rangle\in\Omega_\alpha$. Thereby, $U_1,U_2\in SU_2$ are arbitrary unitary one-qubit transformations. The proof of this statement was given in section 1.8. This observation allows us to restrict our further search for optimal two-particle (resp. four-particle) copying processes of entangled pure two-qubit states to covariant quantum processes which maximize the corresponding figures of merit 4.7 (resp. 4.5).

4.1.2 Covariant linear quantum processes

In this section all possible covariant copying processes are constructed which are consistent with the linear character of general quantum maps of the form of Eq.(4.64).

In view of the covariance condition (4.10) all possible quantum maps of the form (4.64) can be characterized by the output states $\rho_{out}(\rho_{in})$ which originate from one arbitrarily chosen pure input state, say $|\psi\rangle=\alpha|\uparrow\uparrow\rangle+\sqrt{1-\alpha^2}|\downarrow\downarrow\rangle$ with $0\leq\alpha\leq1/\sqrt{2}$. In order to fulfill Eq.(4.10) the two-qubit reference state ρ_{ref} of Eq.(4.64) has to be invariant under arbitrary local unitary transformations of the form $U_1\otimes U_2$. Therefore, we may choose the initial state of the covariant quantum map in the form [34]

$$\rho_0=\rho_{in}\otimes\frac{1}{4}\mathbf{1}\equiv|\psi\rangle\langle\psi|\otimes\frac{1}{4}\mathbf{1}. \tag{4.11}$$

In order to implement the covariance condition of Eq.(4.10), it is convenient to decompose this quantum state into irreducible two-qubit tensor operators [94, 95] $T^{(1,3)}(J',J)_{KQ}$ and $T^{(2,4)}(J',J)_{KQ}$ with respect to qubits one and three on the one hand and qubits two and four on the other hand. Performing an arbitrary unitary transformation of the form $U_1\otimes U_2\otimes U_1\otimes U_2$ with $U_1,U_2\in\mathsf{SU}(2)$, for example, a product of such tensor operators transforms according to

$$\begin{aligned}&\mathcal{U}\;T^{(1,3)}(J_1'J_1)_{K_1Q_1}\otimes T^{(2,4)}(J_2'J_2)_{K_2Q_2}\mathcal{U}^\dagger=\\&\sum_{q_1,q_2}D(U_1)^{(K_1)}_{q_1Q_1}D(U_2)^{(K_2)}_{q_2Q_2}T^{(1,3)}(J_1'J_1)_{K_1q_1}\otimes T^{(2,4)}(J_2'J_2)_{K_2q_2}\end{aligned} \tag{4.12}$$

with $\mathcal{U} = U_1 \otimes U_2 \otimes U_1 \otimes U_2$. Thereby, $D(U_j)$ $(j = 1, 2)$ denote the relevant rotation operators and $D(U_j)^{(K_j)}_{q_j Q_j}$ are their associated rotation matrices [95]. The quantum numbers J_j, J'_j denote the total angular momenta of the relevant two-qubit quantum states and the parameters K_j indicate the irreducible subspaces of the relevant representations. For the sake of convenience some basic relations of these irreducible two-qubit tensor operators are summarized in Appendix C. It is apparent from Eq.(4.12) that an arbitrary unitary transformation of the form $U_1 \otimes U_2 \otimes U_1 \otimes U_2$ with $U_1, U_2 \in \mathsf{SU}(2)$ mixes the parameters q_1 amd q_2 within each irreducible represenation separately.

In terms of these irreducible tensor operators an arbitrary initial state ρ_0 of the form of Eq.(4.11) can be decomposed according to

$$\begin{aligned} \rho_0 \;\; = \;\; & \sum_{j_1,\ldots,j_4,K,Q,K',Q'} T^{(1,3)}(j_1,j_3)_{KQ} \otimes T^{(2,4)}(j_2,j_4)_{K'Q'} \\ & \langle T^{(1,3)\dagger}(j_1,j_3)_{KQ} T^{(2,4)\dagger}(j_2,j_4)_{K'Q'} \rangle \end{aligned} \tag{4.13}$$

with the expansion coefficients

$$\begin{aligned} & \langle T^{(1,3)\dagger}(j_1,j_3)_{KQ} T^{(2,4)\dagger}(j_2,j_4)_{K'Q'} \rangle = \\ & Tr\big\{ (T^{(1,3)\dagger}(j_1,j_3)_{KQ} \otimes T^{(2,4)\dagger}(j_2,j_4)_{K'Q'}) \rho_0 \big\}. \end{aligned} \tag{4.14}$$

In view of the basic transformation property of Eq.(4.12) the most general output state resulting from a linear and covariant quantum map is given by

$$\begin{aligned} \rho_{out}(\rho_{in}) \;\; = \;\; & \sum_{j_1,\ldots,j_4,K,Q,K',Q'} \alpha(j_1,j_3,j_2,j_4)_{KK'} T^{(1,3)}(j_1,j_3)_{KQ} T^{(2,4)}(j_2,j_4)_{K'Q'} \times \\ & \langle T^{(1,3)\dagger}(j_1,j_3)_{KQ} T^{(2,4)\dagger}(j_2,j_4)_{K'Q'} \rangle. \end{aligned} \tag{4.15}$$

The yet unknown coefficients $\alpha(j_1,j_3,j_2,j_4)_{KK'}$ have to be determined by the restrictions imposed by quantum theory, namely ρ_{out} has to be a non-negativ operator. In particular, being a Hermitian operator the output state ρ_{out} has to fulfill the relations

$$\alpha(j_1,j_3,j_2,j_4)_{KK'} = \alpha(j_3,j_1,j_4,j_2)_{KK'}. \tag{4.16}$$

Further restrictions on these unknown coefficients are obtained from the explicit form of the

input state ρ_0, i.e.

$$\begin{aligned}
\rho_0 = \frac{|\alpha|^2}{4}\Big\{ & \frac{1}{\sqrt{2}}T^{(1,3)}(1,1)_{10} + \frac{3}{2}T^{(1,3)}(1,1)_{00} + \\
& \frac{1}{2}T^{(1,3)}(0,0)_{00} - \frac{1}{2}T^{(1,3)}(0,1)_{1,0} + \frac{1}{2}T^{(1,3)}(1,0)_{10}\Big\} \otimes \\
& \Big\{\frac{1}{\sqrt{2}}T^{(2,4)}(1,1)_{10} + \frac{3}{2}T^{(2,4)}(1,1)_{00} + \\
& \frac{1}{2}T^{(2,4)}(0,0)_{00} - \frac{1}{2}T^{(2,4)}(0,1)_{1,0} + \frac{1}{2}T^{(2,4)}(1,0)_{10}\Big\} + \\
& \frac{|\beta|^2}{4}\Big\{\frac{-1}{\sqrt{2}}T^{(1,3)}(1,1)_{10} + \frac{3}{2}T^{(1,3)}(1,1)_{00} + \\
& \frac{1}{2}T^{(1,3)}(0,0)_{00} + \frac{1}{2}T^{(1,3)}(0,1)_{1,0} - \frac{1}{2}T^{(1,3)}(1,0)_{10}\Big\} \otimes \\
& \Big\{\frac{-1}{\sqrt{2}}T^{(2,4)}(1,1)_{10} + \frac{3}{2}T^{(2,4)}(1,1)_{00} + \\
& \frac{1}{2}T^{(2,4)}(0,0)_{00} + \frac{1}{2}T^{(2,4)}(0,1)_{1,0} - \frac{1}{2}T^{(2,4)}(1,0)_{10}\Big\} + \\
& \frac{\alpha\beta^*}{8}\Big\{ - \sqrt{2}T^{(1,3)}(1,1)_{11} + T^{(1,3)}(0,1)_{11} - \\
& T^{(1,3)}(1,0)_{11}\Big\} \otimes \Big\{ - \sqrt{2}T^{(2,4)}(1,1)_{11} + T^{(2,4)}(0,1)_{11} - \\
& T^{(2,4)}(1,0)_{11}\Big\} + \frac{\alpha^*\beta}{8}\Big\{\sqrt{2}T^{(1,3)}(1,1)_{1-1} - \\
& T^{(1,3)}(0,1)_{1-1} + T^{(1,3)}(1,0)_{1-1}\Big\} \otimes \Big\{\sqrt{2}T^{(2,4)}(1,1)_{1-1} - \\
& T^{(2,4)}(0,1)_{1-1} + T^{(2,4)}(1,0)_{1-1}\Big\}. \qquad (4.17)
\end{aligned}$$

Thus, according to Eq.(4.17) the most general output state of Eq.(4.15) generally depends on 17 coefficients, namely

$$\begin{aligned}
& \alpha(1,1,1,1)_{11} = A_1, \quad \alpha(1,1,1,1)_{10} = A_2, \quad \alpha(1,1,1,0)_{11} = A_3, \\
& \alpha(1,1,0,0)_{10} = A_4 \quad \alpha(1,1,1,1)_{01} = A_5, \quad \alpha(1,1,1,1)_{00} = A_6, \\
& \alpha(1,1,1,0)_{11} = A_7, \quad \alpha(1,1,0,0)_{00} = A_8, \quad \alpha(1,0,1,1)_{11} = A_9, \\
& \alpha(1,0,1,1)_{10} = A_{10}, \quad \alpha(1,0,1,0)_{11} = A_{11}, \quad \alpha(1,0,0,0)_{10} = A_{12}, \\
& \alpha(0,0,1,1)_{01} = A_{13}, \quad \alpha(0,0,1,1)_{00} = A_{14}, \quad \alpha(0,0,1,0)_{01} = A_{15}, \\
& \alpha(0,0,0,0)_{00} = A_{16}, \quad \alpha(1,0,0,1)_{11} = A_{17}. \qquad (4.18)
\end{aligned}$$

These parameters determine all linear covariant quantum processes with a Hermitian output state $\rho_{out}(\rho_{in})$ provided the coefficients $A_1, A_3, A_6, A_7, A_8, A_9, A_{11}, A_{14}, A_{16}, A_{17}$ are real-valued.

Due to the covariance condition (4.10) and using the new notation (4.18) the output state (4.15) can be decomposed into a direct sum of density operators according to

$$\rho_{out}(\rho_{in}) \quad = \quad M_1 \oplus M_2 \oplus M_3 \oplus M_4 \oplus M_5 \tag{4.19}$$

with

$$\begin{aligned}
M_1 \quad = \quad & [(2\alpha^2-1)(A_2+A_5)+A_1+A_6]|11;11\rangle\langle 11;11| + A_6|10;10\rangle\langle 10;10| + \\
& A_8|10;00\rangle\langle 10;00| + A_{16}|00;00\rangle\langle 00;00| + A_{14}|00;10\rangle\langle 00;10| + \\
& [(1-2\alpha^2)(A_2+A_5)+A_1+A_6]|00;1-1\rangle\langle 00;1-1| + \\
& 2\alpha\sqrt{1-\alpha^2}[A_1|11;11\rangle\langle 10;10| + A_1^*|10;10\rangle\langle 11;11|] - \\
& 2\alpha\sqrt{1-\alpha^2}[A_3|11;11\rangle\langle 10;00| + A_3^*|10;00\rangle\langle 11;11|] + \\
& 2\alpha\sqrt{1-\alpha^2}[A_{11}[|11;11\rangle\langle 00;00| + A_{11}^*|00;00\rangle\langle 11;11|] - \\
& 2\alpha\sqrt{1-\alpha^2}[A_9[|11;11\rangle\langle 00;10| + A_9^*|00;10\rangle\langle 11;11|] + \\
& (2\alpha^2-1)[A_7|10;10\rangle\langle 10;00| + A_7^*|10;00\rangle\langle 10;10|] + \\
& [A_{11}|10;10\rangle\langle 00;00| + A_{11}^*|00;00\rangle\langle 10;10|] + \\
& (2\alpha^2-1)[A_{10}|10;10\rangle\langle 00;10| + A_{10}^*|00;10\rangle\langle 10;10|] + \\
& 2\alpha\sqrt{1-\alpha^2}[A_1^*|10;10\rangle\langle 00;1-1| + A_1|00;1-1\rangle\langle 10;10|] + \\
& (2\alpha^2-1)[A_{12}|10;00\rangle\langle 00;00| + A_{12}^*|00;00\rangle\langle 10;00|] + \\
& [A_{17}|10;00\rangle\langle 00;10| + A_{17}^*|00;10\rangle\langle 10;00|] + \\
& 2\alpha\sqrt{1-\alpha^2}[A_3^*|10;00\rangle\langle 00;1-1| + A_3|00;1-1\rangle\langle 10;00|] + \\
& (2\alpha^2-1)[A_{15}^*|00;00\rangle\langle 00;10| + A_{15}|00;10\rangle\langle 00;00|] + \\
& 2\alpha\sqrt{1-\alpha^2}[A_{11}^*|00;00\rangle\langle 00;1-1| + A_{11}|00;1-1\rangle\langle 00;00|] + \\
& 2\alpha\sqrt{1-\alpha^2}[A_9^*|00;10\rangle\langle 00;1-1| + A_9|00;1-1\rangle\langle 00;10|],
\end{aligned}$$

$$\begin{aligned}
M_2 \quad &= \quad [(2\alpha^2-1)(A_2-A_5)-A_1+A_6]|11;11\rangle\langle 11;11|, \\
M_3 \quad &= \quad [(2\alpha^2-1)(-A_2+A_5)-A_1+A_6]|1-1;11\rangle\langle 1-1;11|,
\end{aligned}$$

$$
\begin{aligned}
M_4 &= [(2\alpha^2-1)A_4+A_8)]|11;00\rangle\langle 11;00| + [-(2\alpha^2-1)A_5+A_6)]|10;1-1\rangle\langle 10;1-1| + \\
&\quad [-(2\alpha^2-1)A_{13}+A_{14})]|00;1-1\rangle\langle 00;1-1| + [(2\alpha^2-1)A_2+A_6)]|11;10\rangle\langle 11;10| + \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_3^*|11;00\rangle\langle 10;1-1| + A_3|10;1-1\rangle\langle 11;00|] - \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_{17}|11;00\rangle\langle 00;1-1| + A_{17}^*|00;1-1\rangle\langle 11;00|] + \\
&\quad (2\alpha^2-1)[(A_7^*+A_3^*)|11;00\rangle\langle 11;10| + (A_7+A_3)|11;10\rangle\langle 11;00|] + \\
&\quad (2\alpha^2-1)[(A_{10}-A_9)|10;1-1\rangle\langle 00;1-1| + (A_{10}^*-A_9^*)|00;1-1\rangle\langle 10;1-1|] + \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_1|10;1-1\rangle\langle 11;10| + A_1^*|11;10\rangle\langle 10;1-1|] - \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_9^*|00;1-1\rangle\langle 11;10| + A_9|11;10\rangle\langle 00;1-1|], \\
M_5 &= [-(2\alpha^2-1)A_4+A_8)]|1-1;00\rangle\langle 1-1;00| + [(2\alpha^2-1)A_5+A_6)]|10;11\rangle\langle 10;11| + \\
&\quad [(2\alpha^2-1)A_{13}+A_{14})]|00;11\rangle\langle 00;11| + [-(2\alpha^2-1)A_2+A_6)]|1-1;10\rangle\langle 1-1;10| - \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_3^*|1-1;00\rangle\langle 10;11| + A_3|10;11\rangle\langle 1-1;00|] - \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_{17}|1-1;00\rangle\langle 00;11| + A_{17}^*|00;11\rangle\langle 1-1;00|] + \\
&\quad (2\alpha^2-1)[(A_7^*-A_3^*)|1-1;00\rangle\langle 1-1;10| + (A_7-A_3)|1-1;10\rangle\langle 1-1;00|] + \\
&\quad (2\alpha^2-1)[(A_{10}+A_9)|10;11\rangle\langle 00;11| + (A_{10}^*+A_9^*)|00;11\rangle\langle 10;11|] + \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_1|10;11\rangle\langle 1-1;10| + A_1^*|1-1;10\rangle\langle 10;11|] + \\
&\quad 2\alpha\sqrt{1-\alpha^2}[A_9^*|00;11\rangle\langle 1-1;10| + A_9|1-1;10\rangle\langle 00;11|]. \qquad (4.20)
\end{aligned}
$$

Thereby, the basis states $|JM;J'M'\rangle$ involve eigenstates of the total angular momenta of qubits one and three on the one hand and qubits two and four on the other hand, i.e. $|JM;J'M'\rangle = |JM\rangle_{(1,3)} \otimes |J'M'\rangle_{(2,4)}$ with (J,M) and (J',M') denoting the relevant total angular momentum and magnetic quantum numbers.

As we are interested in deterministic quantum processes which produce the output state $\rho_{out}(\rho_{in})$ with a probability of unity we impose the additional normalization condition $Tr\{\rho_{out}(\rho_{in})\} = 1$ which implies

$$\frac{1}{16}(9A_6 + 3A_8 + 3A_{14} + A_{16}) = 1. \qquad (4.21)$$

The problem of positivity of the general output turns out to be quite complicated, but to find the optimal copying processes it is not necessary to know all the mathematical conditions of positivity of the general output. Instead of the complete solution of positivity we will calculate and maximize the two-particle (resp. four-particle) test with respect to a sufficient number of conditions, which follow from positivity of the output matrix. The non-negativity of the output

state (4.19) necessarily implies that all diagonal matrix elements have to be non-negative. The resulting constraints give rise to the inequalities

$$\begin{aligned} &A_6 \geq 0, A_8 \geq 0, A_{14} \geq 0, A_{16} \geq 0, |A_1| \leq A_6, \\ &\left|(2\alpha^2-1)A_4\right| \leq A_8, \left|(2\alpha^2-1)A_{13}\right| \leq A_{14}, \\ &\left|(2\alpha^2-1)A_2\right| \leq A_6, \left|(2\alpha^2-1)A_5\right| \leq A_6. \end{aligned} \tag{4.22}$$

Furthermore, using the relation $\langle\chi|\rho_{out}(\rho_{in})|\chi\rangle \geq 0$ for appropriately chosen pure states $|\chi\rangle$ yields the inequalities

$$\begin{aligned} &|\ A_{11}\ |^2 \leq A_{16}A_6; \qquad \text{using} \quad |\chi\rangle = a|10;10\rangle + b|00;00\rangle, \\ &|\ A_{17}\ |^2 \leq A_{14}A_8; \qquad \text{using} \quad |\chi\rangle = a|10;00\rangle + b|00;10\rangle, \\ &A_6\ |\ (2\alpha^2-1)(A_2+A_5)\ |^2 \leq (A_1+A_6)^2A_6 - 8\alpha^2(1-\alpha^2)A_1^2(A_1+A_6); \\ &\qquad\qquad \text{using} \quad |\chi\rangle = a|11;11\rangle + b|00;1-1\rangle + c|10;10\rangle \end{aligned} \tag{4.23}$$

with a, b and c denoting arbitrary complex-valued coefficients.

In particular, in the special case $A_1 = A_6 \neq 0$ the last inequality of (4.23) implies

$$|\ (2\alpha^2-1)(A_2+A_5)\ | \leq \sqrt{4A_6^2 - 16\alpha^2(1-\alpha^2)A_6^2}. \tag{4.24}$$

Now we have all important relations and we are able to solve the problem of maximizing figures of merit.

4.1.3 Optimal copying processes

In this section the special covariant quantum processes are determined which copy pure entangled two-qubit states of a given degree of entanglement with the highest possible figures of merit. We will start with searching for optimal four-particle processes.

Optimal four-particle copying process

The fidelity F of the general output state $\rho_{out}(\rho_{in})$ with respect to the ideal pure two-qubit output state $|\psi\rangle \otimes |\psi\rangle$ with $|\psi\rangle = (\alpha|\uparrow\uparrow\rangle + \sqrt{1-\alpha^2}|\downarrow\downarrow\rangle)$ is given by

$$\begin{aligned} F \quad \equiv \quad &\langle\psi| \otimes \langle\psi|\rho_{out}|\psi\rangle \otimes |\psi\rangle = \frac{1}{16}\Big\{A_1(1+2\alpha^2(1-\alpha^2)) + \\ &(2\alpha^2-1)^2(A_2+A_5) + A_6(1-\alpha^2(1-\alpha^2)) + \\ &\alpha^2(1-\alpha^2)A_{16} + 6\alpha^2(1-\alpha^2)\mathrm{Re}(A_{11})\Big\}. \end{aligned} \tag{4.25}$$

Besides the parameter α determining the degree of entanglement this fidelity depends on the six parameters $A_1, A_2, A_5, A_6, A_{11}, A_{16}$ which partly characterize a possible covariant copying process. An upper bound of the fidelity (4.25) can be derived with the help of the inequalities (4.23), (4.24) and the relation $A_{16} \leq 16-9A_6$ which is obtained from the normalization condition (4.21), i.e.

$$\begin{aligned} F &\leq \frac{1}{16}\Big\{A_6(4-16\alpha^2(1-\alpha^2)) + 16\alpha^2(1-\alpha^2) + \\ &\quad 6\alpha^2(1-\alpha^2)\sqrt{A_6(16-9A_6)}\Big\}. \end{aligned} \tag{4.26}$$

This upper bound is attained provided the conditions $A_{16} = 16 - 9A_6$, $A_{11} = \sqrt{A_6(16-9A_6)}$ and $A_1 = A_6 = (A_2 + A_5)/2$ are fulfilled. Maximizing the right hand side of Eq.(4.26) with respect to the single parameter A_6 we finally arrive at the inequality

$$F \leq F_2 \equiv \frac{2}{9}(1-4\alpha^2(1-\alpha^2))(1+\sqrt{v}) + \alpha^2(1-\alpha^2)(1+\sqrt{1-v}) \tag{4.27}$$

with

$$v = 1 - \frac{81\alpha^4(1-\alpha^2)^2}{145\alpha^4(1-\alpha^2)^2 - 32\alpha^2(1-\alpha^2)+4}. \tag{4.28}$$

This new upper bound is reached provided the parameters of the covariant copying process fulfill the relations

$$\begin{aligned} A_1 &= \frac{A_2+A_5}{2} = A_6 \equiv A_6^{max} = \frac{8}{9}(1+\sqrt{v}) \\ A_{16} &= 16-9A_6,\ A_{11} = \sqrt{A_6(16-9A_6)}. \end{aligned} \tag{4.29}$$

Consistent with the inequalities (4.22), (4.23) and with Eq.(4.20) the remaining parameters which do not explicitly determine the fidelity can be chosen in the following way

$$\begin{aligned} &A_2 - A_5 = A_4 = A_3 = A_7 = A_8 = A_9 = A_{10} = 0 \\ &A_{12} = A_{13} = A_{14} = A_{15} = A_{17} = 0. \end{aligned} \tag{4.30}$$

With the help of Eq.(4.20) it is straigthforward to check that for these parameters the output state $\rho_{out}(\rho_{in})$ is a non-negative operator.

Thus, consistent with the fundamental laws of quantum theory the output state of a covariant quantum process which copies all pure two-qubit states of the same degree of entanglement α with the maximal four-particle fidelity test F_2 is given by Eq.(4.15) (compare also with Eq.(4.20)) with the parameters (4.18) being determined by Eqs.(4.29) and (4.30).

Optimal two-particle copying process

We are looking for symmetric cloners, i.e. both copies are the same $\rho_{12} = \rho_{34}$. In the standard basis $\{|\uparrow\rangle, |\downarrow\rangle\}$ this condition reads

$$0 = \rho_{12} - \rho_{34} = \frac{1}{16}\begin{pmatrix} A+B+C & 0 & 0 & 4\alpha\beta C \\ 0 & -A+B-C & 0 & 0 \\ 0 & 0 & A-B-C & 0 \\ 4\alpha\beta C & 0 & 0 & -A-B+C \end{pmatrix} \tag{4.31}$$

with

$$A = (\alpha^2-\beta^2)Re(A_{15}+3A_7), \quad B = (\alpha^2-\beta^2)Re(A_{12}+3A_{10}), \quad C = 2Re(A_3+A_9). \tag{4.32}$$

This is fulfilled only if $A = B = C = 0$. If we use this result for evaluating the two-particle test of an arbitrary symmetric covariant process, then the result depends on 7 parameters

$$\begin{aligned} &F_1(A_1, A_2, A_4, A_5, A_{11}, A_{13}, A_{17}) = \langle\phi|\rho_{12}|\phi\rangle = \\ &\frac{1}{32}(\alpha^2-\beta^2)^2(A_{13}+A_4+3A_2+3A_5) \\ &+\frac{1}{32}(1+8\alpha^2\beta^2)(Re(A_{17}+A_{11})+2A_1)+\frac{1}{4}, \end{aligned} \tag{4.33}$$

where $|\phi\rangle$ is the input state $|\phi\rangle = \alpha|\uparrow\uparrow\rangle + \beta|\downarrow\downarrow\rangle$. We have to optimize (4.2) with respect to several positivity conditions. We leave aside the details of the optimization procedure and give just the result. The optimum of the two-particle test, which one can achieve, is

$$F_1 = \frac{1}{32}\left\{6(\alpha^2-\beta^2)A_6^{max} + (1+8\alpha^2\beta^2)(\sqrt{A_6^{max}(16-9A_6^{max})}+2A_6^{max})+8\right\}. \tag{4.34}$$

This maximum is attained only for one process specified by the following set of parameters

$$\begin{aligned} &A_6 = A_6^{max} = \frac{q+\sqrt{q^2-4pr}}{2p}, \qquad A_{16} = 16-9A_6, \\ &A_{11} = \sqrt{A_6(16-9A_6)}, \qquad A_1 = A_2 = A_5 = A_6, \\ &A_4 = A_3 = A_7 = A_8 = A_9 = A_{10} = A_{12} = A_{13} = A_{14} = A_{15} = A_{17} = 0 \end{aligned} \tag{4.35}$$

with

$$\begin{aligned} p &= 81(1+8\alpha^2\beta^2)^2 + 36\left(3(\alpha^2-\beta^2)+(1+8\alpha^2\beta^2)\right)^2 \\ q &= 144(1+8\alpha^2\beta^2)^2 + 64\left(3(\alpha^2-\beta^2)+(1+8\alpha^2\beta^2)\right)^2 \\ r &= 64(1+8\alpha^2\beta^2)^2. \end{aligned} \tag{4.36}$$

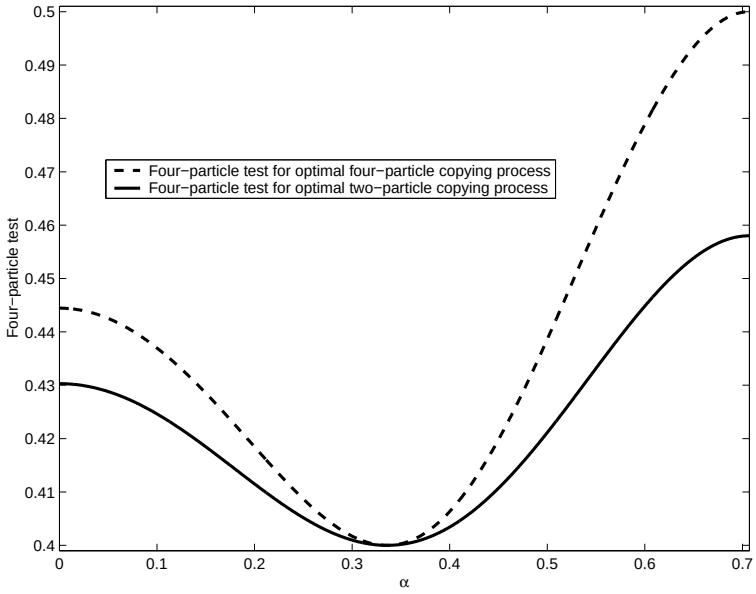

Figure 4.1: Four-particle test of an optimal two-particle (solid line) and four-particle (dashed line) covariant copying process and their dependence on the degree of entanglement α of a pure two-qubit input state.

It is important to note that A_6 is the positive root of the quadratic equation $pA_6^2 + qA_6 + r = 0$. Let us now compare both optimal copying processes.

4.1.4 Comparison and discussion

Both discussed processes differ only in the parameter $A_6(\alpha)$. We found out, that there is only one class of entangled states Ω_α for which both optimal processes are identical, namely for $\alpha_{min} = \sqrt{1/2 - \sqrt{15}/10} \approx 0.3357$ (the point is the solution of the equation $\alpha^2\beta^2 = 0.1$). This process corresponds to the optimal universal four-dimensional copying process (see [34]). This particular covariant two-qubit copying process maximizes both the global fidelity (with the optimal value 0.4) and the single fidelity (with the optimal value 0.7) with respect to all possible two-qubit pure input states independent of their degree of entanglement. Indeed, our optimal copying process for the class $\Omega_{\alpha_{min}}$ is characterized by coefficients $A_6 = A_1 = A_{16} = A_{11} = 1.6$ and therefore the four-particle test (fidelity) is equal to 0.4 and the two-particle test equals 0.7 for all pure states, independently of a chosen class of entangled pure states Ω_α.

Let us look at Fig. 4.1 – shows the dependence of the optimal four-particle test on classes of entangled states, characterized by the parameter α. Naturally, the optimal four-particle copying

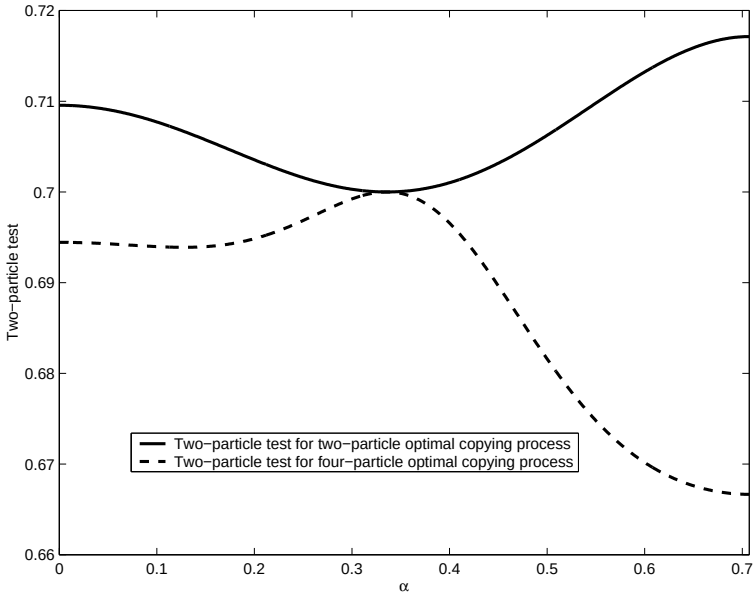

Figure 4.2: The two-particle test of an optimal two-particle (solid line) and four-particle (dashed line) covariant copying process and their dependence on the degree of entanglement α of a pure two-qubit input state.

process achieves a better four-particle test then the optimal two-particle one for all classes of entangled states. Both processes show a rather similar behavior with respect to the four-particle test. They gradually decrease from $\alpha = 0$ to the global minimum at α_{min} and then they grow to the global maximum corresponding to $\alpha = \frac{1}{\sqrt{2}}$. In particular, the four-particle test of the optimal four-particle copying process oscillates between a minimum value of $F = 0.4$ which is assumed at α_{min} and a maximum value of $F = 1/2$ which is assumed at $\alpha = 1/\sqrt{2}$. The value $\alpha = 0$ corresponds to the optimal copying of two arbitrary (generally different) qubit in s separable state. Consistently with known results [34] on optimal cloning of arbitrary single qubit states in this latter case the four-particle test assumes the value $F_2 = (2/3)^2$. In other words, the optimal four-particle copying process for separable states is equivalent to the one-qubit optimal universal copying process (in this case we do not have to specify which fidelity - global or single - is used because both of them lead to the same process) applied to each of the qubits separately.

The next graph 4.2 shows how the quality of cloning depends on a given degree of entanglement as quantified by the two-particle fidelity test. Again both processes differ in the two-particle test maximally by about 0.05. Starting from separable states $\alpha = 0$ the quality

of the optimal two-particle copying process decreases very slowly to the global minimum 7/10 at the point α_{min} and then grows gradually to the global maximum $(5+\sqrt{13})/12$ at the point $\alpha = 1/\sqrt{2}$ (maximally entangled states), which agrees with the result obtained in [39]. For factorizable states the two-particle test equals to $(17+\sqrt{73})/36$.

Here we would like to mention that copying of the class of entangled two-qubit pure states $\Omega_{\alpha_{min}}$ achieves the worst quality in comparison with other classes Ω_α. As we have already mentioned, the optimal cloning process for this class $\Omega_{\alpha_{min}}$ is the optimal universal four-dimensional copying process. Therefore it appears that this class is responsible for the optimal quality of copying of the whole four-dimensional Hilbert space.

4.1.5 Optimal covariant copying processes as completely positive quantum operations

In this section we demonstrate that all the obtained covariant optimal four-particle (resp. two-particle) copying processes with output states of the form of Eq.(4.15) with parameters as given by Eqs.(4.29) and (4.30) (resp. (4.35)) can be realized by completely positive deterministic quantum operations. Furthermore, possible isometric representations of these quantum operations are presented. As we have already mentioned, the optimal two-particle and four-particle copying processes differ only in the parameter A_6. Therefore the following considerations are valid for both type of optimal copying processes.

Using Eqs.(4.15), (4.29), and (4.30) (resp. (4.35)) it is straightforward to demonstrate that the output state of the optimal covariant quantum copying process can be written in the form

$$\rho_{out}(|\psi\rangle\langle\psi|) = K|\psi\rangle\langle\psi| \otimes \frac{1}{4}\mathbf{1}K^\dagger = \sum_{i,j=0,1} \mathcal{K}_{ij}|\psi\rangle\langle\psi|\mathcal{K}_{ij} \tag{4.37}$$

with the operators

$$\begin{aligned} K &= \sqrt{A_1}P_T^{(1,3)} \otimes P_T^{(2,4)} + \sqrt{A_{16}}P_S^{(1,3)} \otimes P_S^{(2,4)} = K^\dagger, \\ \mathcal{K}_{ij} &= \frac{K}{2}|i\rangle_3 \otimes |j\rangle_4. \end{aligned} \tag{4.38}$$

Thereby, $P_T^{(a,b)} = \sum_{M=0,\pm1} |1\ M\rangle\langle 1\ M| \otimes |1\ M\rangle\langle 1\ M|$ and $P_S^{(a,b)} = |00\rangle\langle 00| \otimes |00\rangle\langle 00|$ are projection operators onto the triplet and singlet subspaces of qubits a and b and $|J\ M\rangle$ denote the corresponding (pure) two-qubit quantum states with total angular momentum quantum number J and magnetic quantum number M. The states $\{|i\rangle_3; i = 0,1\}$ and $\{|j\rangle_4; j = 0,1\}$ denote orthonormal basis states in the one-qubit Hilbert spaces of qubits three and four, respectively. According to Eqs.(4.37) and (4.38) the four Kraus operators [96] $\mathcal{K}_{ij}$ $(i,j = 0,1)$ characterize a

quantum operation acting on qubits one and two which results in the output state $\rho_{out}(|\psi\rangle\langle\psi|)$. These Kraus operators map two-qubit states into four-qubit states and fulfill the completeness relation

$$\sum_{i,j=0,1} \mathcal{K}_{ij}^{\dagger}\mathcal{K}_{ij} \;\; = \;\; \mathbf{1}_{12} \tag{4.39}$$

where $\mathbf{1}_{12}$ denotes the unit operator acting in the Hilbert space of qubits one and two. Thus, they represent a deterministic quantum operation [96, 97, 111] acting on the two qubits which are to be copied. Furthermore, the Kraus representation of Eq.(4.37) also demonstrates that the optimal covariant copying process considered so far is not only a linear and positive quantum map but that it is also completely positive [96, 111].

Alternatively, the quantum operation of Eq.(4.37) may also be implemented by an associated linear and isometric transformation U which involves two additional ancilla qubits. Denoting the orthonormal basis states of these additional ancilla qubits by $\{|\mu_{\alpha\beta}\rangle; \alpha, \beta = 0, 1\}$ and the orthonormal basis states of the two-qubit state space of the system by $\{|k\rangle \otimes |l\rangle; k, l = 0, 1\}$ U can be defined by

$$U|k\rangle_1 \otimes |l\rangle_2 \otimes |\mu_{\alpha\beta}\rangle_{56} \;\; = \;\; \sum_{i,j=0,1} (\mathcal{A}_{ij}^{(\alpha\beta)}|k\rangle_1 \otimes |l\rangle_2) \otimes |\mu_{ij}\rangle_{56}, \tag{4.40}$$

for example, with

$$\begin{aligned}
\mathcal{A}_{ij}^{(00)} &= \mathcal{K}_{ij} \equiv (\sqrt{\frac{A_1}{4}} P_T^{(1,3)} \otimes P_T^{(2,4)} + \\
&\quad \sqrt{\frac{A_{16}}{4}} P_S^{(1,3)} \otimes P_S^{(2,4)})|i\rangle_3 \otimes |j\rangle_4, \\
\mathcal{A}_{ij}^{(11)} &= (\sqrt{\frac{A_{16}}{36}} P_T^{(1,3)} \otimes P_T^{(2,4)} - \\
&\quad \sqrt{\frac{9A_1}{4}} P_S^{(1,3)} \otimes P_S^{(2,4)})|i\rangle_3 \otimes |j\rangle_4, \\
\mathcal{A}_{ij}^{(01)} &= \sqrt{\frac{4}{3}} P_T^{(1,3)} \otimes P_S^{(2,4)}|i\rangle_3 \otimes |j\rangle_4, \\
\mathcal{A}_{ij}^{(10)} &= \sqrt{\frac{4}{3}} P_S^{(1,3)} \otimes P_T^{(2,4)}|i\rangle_3 \otimes |j\rangle_4.
\end{aligned} \tag{4.41}$$

Thereby, the subscripts of the state vectors label the qubits they are referring to.

Accordingly, the optimal covariant copying process of Eq.(4.37) can be realized also with the help of this isometric transformation U in the following way: In a first step one applies this

transformation to the intial state $|\psi\rangle_{12} \otimes |\mu_{00}\rangle_{56}$ of the system and ancilla qubits, i.e.

$$U|\psi\rangle_{12} \otimes |\mu_{00}\rangle_{56\ 56}\langle\mu_{00}| \otimes_{12} \langle\psi|U^{\dagger} = \sum_{i,j,i',j'=0,1} \mathcal{K}_{ij}|\psi\rangle_{12} \otimes |\mu_{ij}\rangle_{56\ 56}\langle\mu_{i'j'}| \otimes_{12} \langle\psi|\mathcal{K}^{\dagger}_{i'j'}. \tag{4.42}$$

In a second step one discards the ancilla qubits in the orthogonal basis $\{|\mu_{ij}\rangle_{56}; i,j = 0,1\}$. Finally, this discarding yields the output state $\rho_{out}(|\psi\rangle\langle\psi|)$ of Eq.(4.37).

4.1.6 Properties of optimal copying machines

In this section the degree of entanglement and purity of the output states produced by the optimal covariant copying processes are discussed.

If we would be able to copy ideally, we would make copies with the same entanglement and statistical correlations as in the input state. The copies would not be correlated with each other and also with the environment. In reality it is not possible and during the copying procedure our systems interact with each other and with the "environment" and become correlated. Therefore, one possibility of how to study the copying processes is thorough their correlation properties. We characterize the correlation properties by measures of entanglement (see section 2.2.3): concurrence and negativity.

In the next sections we analyze the correlation properties of both optimal copying processes, two-particle and four-particle. At this point it is important to recall the fact, that both processes have the same structure and they differ only by the function $A_6(\alpha)$. Therefore all explicit formulas for correlations have the same form in terms of the parameter A_6 and we will write them always in one compact form.

Let us now investigate entanglement of the output state $\rho_{out}(\rho_{in})$ with respect to the first and the second qubit.

Entanglement of qubit one and two

Consider first of all a two-qubit input state of the form $\rho_{in} = |\psi\rangle\langle\psi|$ with $|\psi\rangle \in \Omega_{\alpha}$. Its concurrence is given by

$$C(\rho_{in}) = 2|\alpha\sqrt{1-\alpha^2}|. \tag{4.43}$$

The corresponding reduced density operator $\rho^{(1,2)}_{out}$ of qubits one and two after an optimal covariant copying process can be determined straightforwardly from Eqs.(4.15), (4.18),(4.29), and

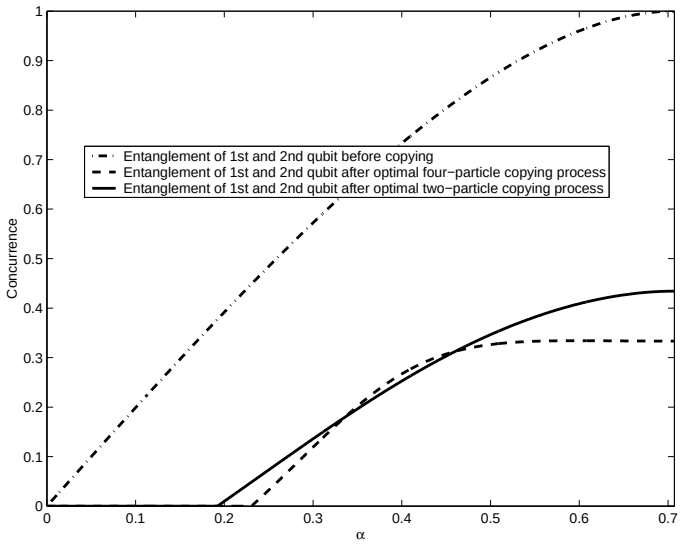

Figure 4.3: The concurrence between qubit 1 and 2. Dot-dashed line represents entanglement before copying, the solid line represents entanglement after the optimal two-particle copying process and the dashed line represents entanglement after the optimal four-particle copying process

.

(4.30) (resp. (4.35)). In particular, its concurrence is given by

$$C(\rho_{out}^{(1,2)}) = \max\left\{0, \frac{1}{16}\left(4|\alpha\beta|(2A_6 + A_{11}) - 8 + 2A_6 + A_{11}\right)\right\}. \tag{4.44}$$

Because all optimal covariant copying processes are symmetric, the reduced density operators of qubits one and two on the one hand and qubits three and four on the other hand are equal. Therefore, all results obtained for the pairs of qubits one and two are also valid for qubits three and four. In Fig. 4.3 the concurrence of the quantum states of qubits one and two before and after the optimal two-particle and four-particle covariant copying process and their dependence on the degree of entanglement α are depicted.

The concurrence of the pure input state increases smoothly from its minimum value zero at $\alpha = 0$ to its maximum value of unity at $\alpha = 1/\sqrt{2}$. The corresponding values of the output states with respect to qubits one and two exhibit a rather different behavior. Both studied optimal processes need a certain minimal input entanglement in order to achieve entanglement between qubits one and two in the resulting output state. The optimal two-particle copying process achieves output entanglement earlier, for $\alpha = 0.192$, whereas the optimal four-particle copying

process for $\alpha = 0.231$. Then the concurrence of the output state of the optimal two-particle copying process increases to its maximum value 0.4343 at $\alpha = \frac{1}{\sqrt{2}}$ (for maximally entangled states) and the concurrence of the output state of the optimal four-particle copying saturates at a rather moderate value around 0.3 at which it becomes almost independent of the value of α. Its maximum entanglement between qubits one and two is not achieved exactly for maximally entangled initial states with $\alpha = 1/\sqrt{2}$ but for values slightly below. However, this difference is very small. The optimal four-particle copying process achieves a higher value of entanglement between qubits one and two only for $\alpha \in \langle \alpha_{min}, 0.4604 \rangle$.

Correlation of qubit one and three

How does the same situation looks for qubits one and three? In view of the structure of the input state ρ_0 of Eq.(4.11) the entanglement and statistical correlation between qubits one and three vanish. The concurrence of the reduced density operator of the output state of optimal covariant copying processes with respect to these qubits is given by

$$C_{13}^{(out)} = \max\left\{0, \frac{1}{4}\left(|-4+3A_6| - 3A_6\alpha\beta\right)\right\}. \tag{4.45}$$

This concurrence of the output state and its dependence on the degree of entanglement specified by α of the input state are depicted in Figs. 4.4.

Characteristically, the concurrence of the output state after both optimal copying processes decreases almost linearly to zero which the optimal two-particle process achieves at $\alpha = 0.213$ and the optimal four-particle process at $\alpha = 0.239$. During the slope, values of the concurrence after the optimal four-particle copying process is about 0.043 bigger then the value of the concurrence after the optimal two-particle copying process.

Entanglement between two copies

To conclude the discussion about entanglement we show, how mutually entangled are both copies. The dimension of both copies is equal to 4. Therefore we use the negativity (see section 2.2.3) to express the degree of entanglement between them. Its dependence on the degree of entanglement α of the pure two-qubit input state is depicted in Fig. 4.5.

The plot illustrates several interesting features. First, the negativity indicates that the output states of both optimal copying processes are entangled over the whole range of the parameter α. Second, it is apparent, that the optimal two-particle copying process entangles

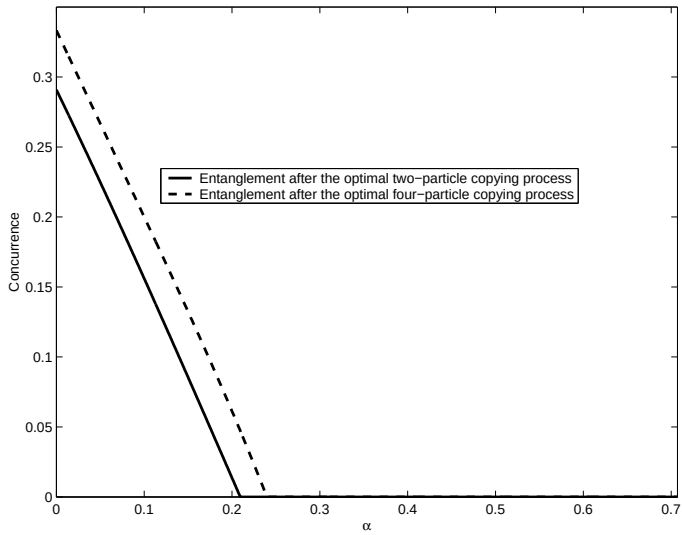

Figure 4.4: The concurrence of qubits 1 and 3. Solid line represents the concurrence after optimal two-particle copying process and dashed line represents the index of correlation after optimal four-particle copying process.

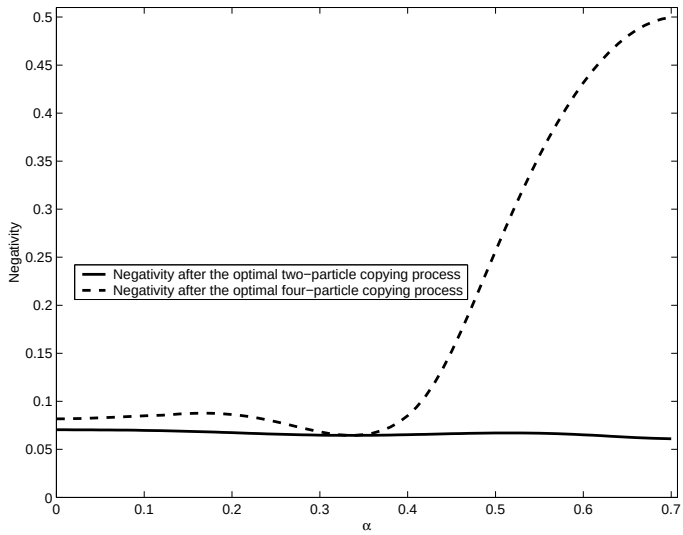

Figure 4.5: The negativity of subsystems formed by copies. Solid line represents the negativity after the optimal two-particle copying process and dashed line represents the negativity after the optimal four-particle copying process

.

both copies weaker then the optimal four-particle one. The only exception is naturally the class Ω_α with $\alpha = \alpha_{min}$, where both optimal copying processes are the same.

To be more precise, the negativities of both optimal processes are almost constant to the point $\alpha = \alpha_{min}$. This point coincides with the global minimum of negativity of the four-particle copying process 0.065. Then the negativity of the optimal four-particle copying process grows fast to its maximum 0.5 at the point $\alpha = 1/\sqrt{2}$ (maximally entangled states), whereas the negativity of the optimal two-particle copying process remains almost unchanged about the value 0.65.

Purity of the outputs

Naturally, one additional important question arises. How is it possible, that the optimal two-particle process shows better correlation properties then the optimal four-particle one? Does the four-particle test express, how close we come to two separable copies? Not exactly. It expresses, how close we come to two pure separable copies. For a better understanding we plot in the next graph Fig. 4.6 the purity of the output state for both optimal copying processes. The purity is measured by the von Neumann entropy (the definition is given in section 2.2.2).

The graph shows close relationship of the output entropy with the output negativity presented in Fig.4.5. First, the optimal four-particle copying process exhibits better (meaning smaller) entropy in the whole range of the parameter α. Second, up to the point $\alpha = \alpha_{min}$ the entropies of both optimal copying processes grow very slowly and with mutually small differences to their global maxima. Then the optimal two-particle copying process decreases slowly to its minimum at the point $\alpha = 1/\sqrt{2}$ whereas the optimal four-particle copying process decreases considerably faster to the minimum for maximally entangled states.

4.1.7 Conclusion

We studied the problem of copying of pure entangled quantum states with respect to two different measures of the output state quality. We showed that the two figures of merit lead to two different processes in contrast to the results obtained for the copying of arbitrary unknown quantum states. Even though the two processes are different they can be written in a formally very similar way. The processes can be realized involving the same projection operators but with different coefficients. The output states exhibit quite different properties with respect to mutual entanglement. Let us point out that the copying processes for two-particle and four-particle measure is a generalization of the previous results [39] to arbitrary initial pure entangled

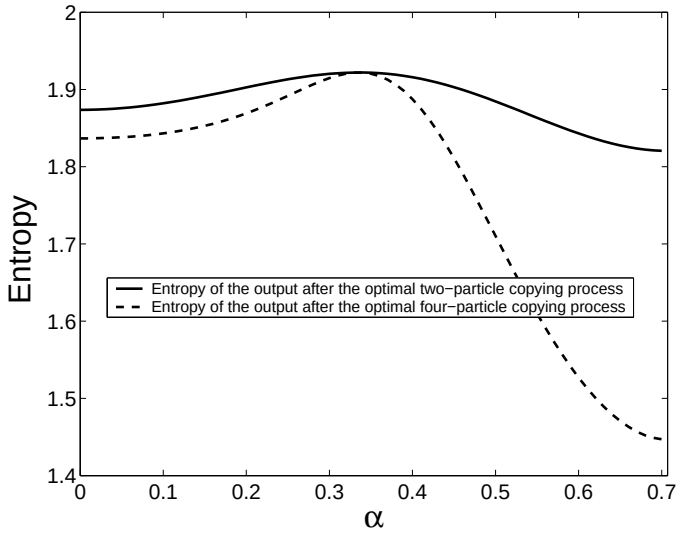

Figure 4.6: The entropy of whole output of optimal copying processes. Solid line represents the entropy after the optimal two-particle copying process and dashed line represents the entropy after the optimal four-particle copying process

.

states. Here it is important to recall, that at least partly the same problem were solved in [98]. Using the concept of covariant maps they have found optimal two-particle copying processes for all classes of pure two-qubit states Ω_α. A big advantage of our mathematical framework is that we were able to treat all problems analytically. It reveals us a simple relationship between both types of optimal copying processes.

Finally, we would like draw attention to the fact that worst case is to copy the class of entangled states Ω_α with $\alpha = \alpha_{min}$. Despite of two different figures of merit we have received the same result. On top of that, this interesting observation is amplified by another fact. In [98] authors studied whether classical communication can improve local cloning of unknown pure two-qubit states. They showed that surprisingly the answer is 'yes', if this unknown copied pure two-qubit state contains more then certain critical degree entanglement. This critical value is again $\alpha = \alpha_{min}$. In the following chapter we will show that this class plays an important role also in constructing the NOT operation.

4.2 Covariant two-qubit quantum channels and optimal NOT operations for entangled qubit pairs

As we have already discussed in section 1.7, an ideal quantum NOT operation acting on the whole Hilbert space has to be anti-linear and hence it is not possible to represent its operation by a complete positive quantum operation. In view of this no-go property of quantum mechanics it is of interest to construct quantum operations which approximate a quantum NOT operations in the best possible way.

Recently, the problem of optimizing quantum NOT operations with respect to arbitrary one-qubit input states stimulated both theoretical [40] and experimental investigations [42]. By now many aspects of optimal quantum NOT operations are well understood at least as far as general n-qubit input states [5] or one-qudit input states [40] are concerned. Nevertheless, much less is known about optimal quantum NOT operations for entangled input states. In particular, if one is interested in constructing quantum NOT operations which are optimal for entangled input states of a particular degree of entanglement only, the general no-go theorem for quantum NOT operations does not apply because the input states form a restricted subset and not a complex linear subspace of the Hilbert space.

The main aim of this chapter is twofold. Firstly, the general structure of completely positive quantum processes is investigated which transform all possible pure two-qubit inputs states of a given degree of entanglement in a covariant way. Surprisingly it turns out that all these processes can be represented in a systematic way by convex sums of four special quantum processes some of which have already been discussed previously in the literature. Using their simple convex form we prove several interesting properties of these covariant processes and present a network of quantum gates which is capable of implementing a large variety of covariant two qubit processes.

Secondly, based on this general analysis the structure of two-qubit quantum processes is discussed which transform an arbitrary pure two-qubit input state of a given degree of entanglement into an orthogonal quantum state in an optimal way. It is shown that in the special case of maximally entangled pure input states such quantum NOT operations can be performed perfectly and the general structure of these perfect quantum NOT operations is presented. The general structure of these perfect quantum NOT operations is presented and using these perfect NOT operations we propose a remote state protocol for two maximally entangled qubits.

4.2.1 Completely positive covariant two-qubit quantum processes

In this section the general structure of all completely positive quantum processes, which transform pure two-qubit input states of a given degree of entanglement in a covariant way, is investigated.

Let us start by considering a general quantum operation (see section 1.2), $\mathcal{P}$, which maps an arbitrary two-qubit mixed input state, ρ_{in}, onto a mixed two-qubit output state, ρ_{out}, i.e.

$$\mathcal{P}: \quad \rho_{in} \longrightarrow \rho_{out}. \tag{4.46}$$

If this is to treat pure two-qubit input states of a given degree of entanglement in a covariant way it has to fulfill the covariance condition (see section 1.5)

$$\mathcal{P}\left(U_1 \otimes U_2 \rho_{in} U_1^\dagger \otimes U_2^\dagger\right) = U_1 \otimes U_2 \mathcal{P}(\rho_{in}) U_1^\dagger \otimes U_2^\dagger. \tag{4.47}$$

This requirement has to be satisfied for arbitrary unitary one-qubit transformations U_1,$U_2 \in \mathsf{SU}(2)$ [95]. The restriction of the quantum map (4.46) to quantum operations reflects the physical requirement that $\mathcal{P}$ should be implementable by a unitary transformation possibly involving also additional quantum systems but under the constraint that initially the two-qubit system of interest and these additional ancillary systems are uncorrelated [111]. As will be seen later, the covariance condition (4.47) implies the requested independence of the quality of performance of this quantum operation on the possible input states.

For implementing the covariance condition (4.47) on the quantum process of (4.46), it is convenient to decompose the input state ρ_{in} into its angular-momentum irreducible tensor components $T(\frac{1}{2},\frac{1}{2})_{K,q}$ [94], i.e.

$$\rho_{in} = \sum_{K,q;K',q'} Tr\left\{\left[T\left(\frac{1}{2},\frac{1}{2}\right)^\dagger_{K,q} \otimes T\left(\frac{1}{2},\frac{1}{2}\right)^\dagger_{K',q'}\right]\rho_{in}\right\} T\left(\frac{1}{2},\frac{1}{2}\right)_{K,q} \otimes T\left(\frac{1}{2},\frac{1}{2}\right)_{K',q'} \tag{4.48}$$

with

$$\begin{aligned} T\left(\frac{1}{2},\frac{1}{2}\right)_{0,0} &= \frac{1}{\sqrt{2}} I, \quad T\left(\frac{1}{2},\frac{1}{2}\right)_{1,1} = -(\sigma_1 + i\sigma_2)/2, \\ T\left(\frac{1}{2},\frac{1}{2}\right)_{1,0} &= \sqrt{2}\sigma_3/2, \quad T\left(\frac{1}{2},\frac{1}{2}\right)_{1,-1} = (\sigma_1 - i\sigma_2)/2 \end{aligned} \tag{4.49}$$

and with $K \in \{0,1\}$ and $-K, -K+1, ... \leq q \leq ..., K-1, K$. Thereby, σ_i with $i = 1,2,3$ are the three orthogonal components of the Pauli spin operators with respect to fixed orthogonal

xyz-axes

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.50}$$

(For the sake of convenience some basic facts about angular-momentum tensor operators are summarized in Appendix C). The corresponding most general linear covariant output state has the form (see section 4.1.2)

$$\rho_{out} = \sum_{K,q;K',q'} \lambda(K,K') \qquad \mathrm{Tr}\left\{\left[T\left(\frac{1}{2},\frac{1}{2}\right)^{\dagger}_{K,q} \otimes T\left(\frac{1}{2},\frac{1}{2}\right)^{\dagger}_{K',q'}\right]\rho_{in}\right\} \times$$
$$T\left(\frac{1}{2},\frac{1}{2}\right)_{K,q} \otimes T\left(\frac{1}{2},\frac{1}{2}\right)_{K',q'}. \tag{4.51}$$

According to equation (4.48) the most general two-qubit input state can be written in the form

$$\rho_{in}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{M}) = \frac{1}{4}\left\{I\otimes I + \sum_{i=1}^{3} P_i\sigma_i \otimes I + \sum_{i=1}^{3} Q_i I \otimes \sigma_i + \sum_{i,j=1}^{3} M_{ij}\sigma_i \otimes \sigma_j\right\}. \tag{4.52}$$

with the aid of the two local vectors of coherence, $\boldsymbol{P} = (P_x, P_y, P_z)$ and $\boldsymbol{Q} = (Q_x, Q_y, Q_z)$, and with the correlation-tensor $\boldsymbol{M} = (M_{ij})_{i,j=x,y,z}$ [99]. Because we are looking for trace preserving maps, we obtain the condition $\lambda(0,0) = 1$. Using the notation $V = \lambda(1,0)$, $X = \lambda(0,1)$, $Y = \lambda(1,1)$ the corresponding output state of (4.51) is given by

$$\begin{aligned}\rho_{out} \quad &= \frac{1}{4}\left\{I\otimes I + \sum_{i=1}^{3}(VP_i)\sigma_i \otimes I + \sum_{i=1}^{3}(XQ_i) I\otimes\sigma_i + \sum_{i,j=1}^{3}(YM_{ij})\sigma_i\otimes\sigma_j\right\} \\ &\equiv \rho_{in}(V\boldsymbol{P}, X\boldsymbol{Q}, Y\boldsymbol{M}).\end{aligned} \tag{4.53}$$

In the special case of a normalized pure input state $|\psi\rangle = \alpha|\uparrow\uparrow\rangle + \beta|\downarrow\downarrow\rangle$ which is quantized in the z-direction this yields the explicit matrix representation

$$\rho_{out} = \begin{pmatrix} \frac{1+Y}{4} + \frac{X+V}{4}(2|\alpha|^2-1) & 0 & 0 & Y\alpha\beta^* \\ 0 & \frac{1-Y}{4} + \frac{V-X}{4}(2|\alpha|^2-1) & 0 & 0 \\ 0 & 0 & \frac{1-Y}{4} + \frac{X-V}{4}(2|\alpha|^2-1) & 0 \\ Y\alpha^*\beta & 0 & 0 & \frac{1+Y}{4} - \frac{X+V}{4}(2|\alpha|^2-1) \end{pmatrix} \tag{4.54}$$

in the eigenbasis of $\sigma_z \otimes \sigma_z$. Therefore, an arbitrary triple (X, V, Y) defines the most general covariant map between an input state (4.52) and an output state (4.53). With the help of

Jamiołkowski-Choi theorem 1.4.1 we can determine for which parameters (V, X, Y) the covariant quantum process $\mathcal{P}_{V,X,Y}$ is completely positive. The covariance condition (4.47) associates an arbitrary input state (4.52) to the output state (4.53). We can express this relation between the input and output state by the linear transformation

$$\rho_{out} = \mathcal{P}_{V,X,Y}\left(\rho_{in}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{M})\right) = \sum_{i,j=0}^{3} l_{ij} L_{ij} \rho_{in}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{M}) L_{ij}^{\dagger} \tag{4.55}$$

with

$$\begin{aligned} l_{00} &= \frac{1}{16}(1+3X+3V+9Y), \qquad l_{i0} = \frac{1}{16}(1+3X-V-3Y), \\ l_{0i} &= \frac{1}{16}(1+3V-X-3Y), \qquad l_{ij} = \frac{1}{16}(1-X-V+Y), \end{aligned} \tag{4.56}$$

and with

$$\begin{aligned} L_{00} &= I \otimes I, \qquad L_{i0} = \sigma_i \otimes I, \\ L_{0i} &= I \otimes \sigma_i, \qquad L_{ij} = \sigma_i \otimes \sigma_j. \end{aligned} \tag{4.57}$$

If $l_{ij} \geq 0$ for all $i, j \in \{x, y, z\}$ the covariant process $\mathcal{P}_{V,X,Y}$ is completely positive. That these conditions are also necessary follows from theorem 1.4.1. With the aid of (4.55) one can check easily that the eigenvalue spectrum of the operator $\mathcal{J}(\mathcal{P}_{V,X,Y}) = \sum_{ij=1}^{4} \mathcal{P}_{V,X,Y}(P_{ij}) \otimes P_{ij}$ is given by

$$\begin{aligned} \sigma\left(\mathcal{J}(\mathcal{P}_{V,X,Y})\right) = \quad & \Big\{\frac{1}{4}(1+3X+3V+9Y), \frac{1}{4}(1-X-V+Y), \\ & \frac{1}{4}(1+3V-X-3Y), \frac{1}{4}(1+3X-V-3Y)\Big\}. \end{aligned} \tag{4.58}$$

Hence, the covariant process $\mathcal{P}_{V,X,Y}$ is completely positive if and only if the following conditions are fulfilled

$$1+3X+3V+9Y \geq 0, \quad 1+3X-V-3Y \geq 0, \quad 1-X+3V-3Y \geq 0, \quad 1-X-V+Y \geq 0, \tag{4.59}$$

or equivalently

$$\begin{aligned} \max\left\{-\frac{1+3X+3V}{9}, -1+X+V\right\} \leq \quad & Y \quad \leq \frac{1+3\min\{X,V\}-\max\{X,V\}}{3}, \\ -\frac{1}{3} \leq \quad & X, V \quad \leq 1. \end{aligned} \tag{4.60}$$

Thus, provided these relations are fulfilled the process defined by the covariant output state (4.53) is completely positive. A Kraus-representation of this deterministic quantum operation is given by

$$\rho_{out} = \mathcal{P}_{V,X,Y}\left(\rho_{in}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{M})\right) = \sum_{i,j=0,x,y,z} K_{ij}\rho_{in}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{M})K_{ij}^{\dagger} = \rho_{in}(V\boldsymbol{P},X\boldsymbol{Q},Y\boldsymbol{M}) \quad (4.61)$$

with

$$\begin{aligned} K_{00} &= \frac{1}{4}\left(1+3X+3V+9Y\right)^{\frac{1}{2}} I\otimes I, \quad K_{i0} = \frac{1}{4}\left(1+3X-V-3Y\right)^{\frac{1}{2}} \sigma_i\otimes I, \\ K_{0i} &= \frac{1}{4}\left(1-X+3V-3Y\right)^{\frac{1}{2}} I\otimes \sigma_i, \quad K_{ij} = \frac{1}{4}\left(1-X-V+Y\right)^{\frac{1}{2}} \sigma_i\otimes\sigma_j, \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i,j\in\{x,y,z\}. \end{aligned} \quad (4.62)$$

Trace preservation is implied by the relation

$$\sum_{i,j=0,x,y,z} K_{ij}^{\dagger}K_{ij} = I. \quad (4.63)$$

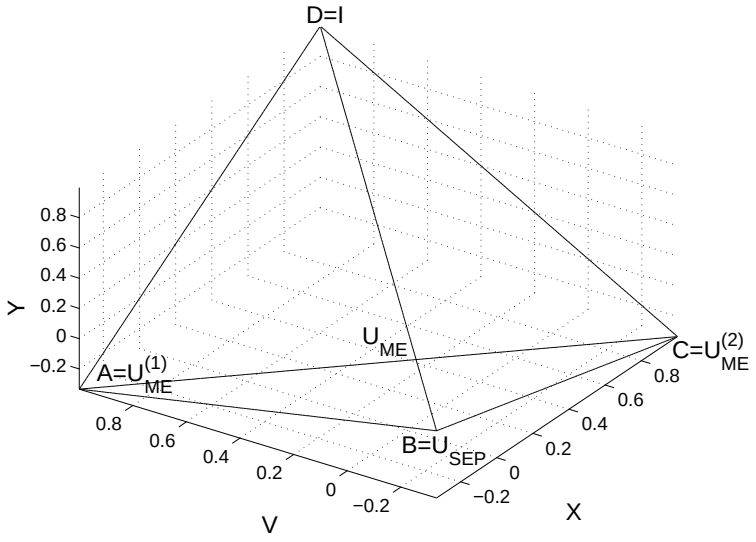

Figure 4.7: The parameter space of points (V,X,Y) for which the covariant process $\mathcal{P}_{V,X,Y}$ is completely positive forms the tetrahedron $\overline{ABCD}$.

The set of all possible completely positive universal quantum operations characterized by triples (V,X,Y) is represented by the convex tetrahedron $\overline{ABCD}$ of Fig. 4.2.1. The physical significance of the extremal points of this tetrahedron is discussed in Sec.4.2.5.

4.2.2 Optimal quantum NOT operations for pure entangled qubit pairs

Starting from the general results of Sec. 4.2.1 we can specify different types of completely positive covariant quantum processes. In the following we determine quantum processes which describe a quantum NOT operation acting on arbitrary pure two-qubit states of a given degree of entanglement in an optimal way.

We are interested in constructing linear and completely positive quantum processes U_α which map an arbitrary pure input state, say $|\phi\rangle \in \Omega_\alpha$, in an optimal way onto its orthogonal complement, i.e.

$$U_\alpha : \rho_{in} = |\phi\rangle\langle\phi| \longrightarrow \rho_{out}. \tag{4.64}$$

For the solution of this optimization problem a measure is needed which quantifies how close the output state ρ_{out} is to the orthogonal complement of the input state $|\phi\rangle$.

Figure of merit

Definitely, the Hilbert space of two qubits $\mathscr{H}$ is the direct sum of two Hilbert spaces, namely the span of the vector $|\phi\rangle$, say $\mathscr{H}_\phi$, and its three-dimensional orthogonal complement $\mathscr{H}_\phi^\perp$. Therefore, a convenient measure is given by the minimal distance between the output state ρ_{out} and all mixed states contained in the orthogonal complement of the input, i.e.

$$D(\rho_{out}|\Gamma(\mathscr{H}_\phi^\perp)) = \min_{\sigma\in\Gamma(\mathscr{H}_\phi^\perp)} Tr\{\rho_{out} - \sigma\}^2. \tag{4.65}$$

Thereby, $\Gamma(\mathscr{H}_\phi^\perp)$ denotes the linear convex set of all density operators formed by convex sums of pure states of the Hilbert space $\mathscr{H}_\phi^\perp$. This measure is based on the well known Hilbert-Schmidt norm for Hilbert-Schmidt operators A and B, i.e. $||A-B|| = \sqrt{Tr\,\{A-B\}^2}$. We omitted the square root as it is unimportant for our purposes. We will prove, that the minimal distance of (4.65) can be express in the more convenient form

$$D(\rho_{out}|\Gamma(\mathscr{H}_\phi^\perp)) = 2\langle\phi|\rho_{out}^2|\phi\rangle - \frac{2}{3}\langle\phi|\rho_{out}|\phi\rangle^2. \tag{4.66}$$

Proof: Consider an arbitrary two-qubit density operator ρ. Let us denote the eigenvectors of its restriction onto the three dimensional subspace orthogonal to $|\phi\rangle$, $\mathscr{H}_\phi^\perp$, by $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_3\rangle$. The orthonormal vectors $|\phi\rangle$, $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_3\rangle$ form an orthonormal basis in which this

density operator takes the form

$$\rho = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 \\ \lambda_2^* & \beta_1 & 0 & 0 \\ \lambda_3^* & 0 & \beta_2 & 0 \\ \lambda_4^* & 0 & 0 & \beta_3 \end{pmatrix}, \quad \text{with} \qquad \lambda_1 + \sum_{i=1}^{3} \beta_i = 1 \qquad \lambda_1, \beta_i \geq 0. \tag{4.67}$$

The coefficients λ_i and β_i are restricted by the requirement of positivity of ρ. In this base an arbitrary quantum state which is located entirely in the orthogonal subspace spanned by the states $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_3\rangle$ can be represented by a matrix of the form

$$\sigma = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \alpha_{11} & \alpha_{12} & \alpha_{13} \\ 0 & \alpha_{12}^* & \alpha_{22} & \alpha_{23} \\ 0 & \alpha_{13}^* & \alpha_{23}^* & \alpha_{33} \end{pmatrix}, \quad \text{with} \qquad \sum_{i=1}^{3} \alpha_{ii} = 1, \qquad \alpha_{ii} \geq 0. \tag{4.68}$$

Again the coefficients α_{ij} have to be consistent with the positivity of σ. In this notation the measure $D(\rho|\Gamma(\mathscr{H}_\phi^\perp))$ assumes the form

$$\begin{aligned} D(\rho|\Gamma(\mathscr{H}_\phi^\perp)) &= \min_{\sigma\in\Gamma({\mathcal{H}_\phi}^\perp)} Tr\{\rho-\sigma\}^2 = \min_{\sigma\in\Gamma({\mathcal{H}_\phi}^\perp)} \left\{Tr(\rho^2) - 2Tr(\rho\sigma) + Tr(\sigma^2)\right\} \\ &= \min_{\sigma\in\Gamma({\mathcal{H}_\phi}^\perp)} \left\{ Tr(\rho^2) - 2\sum_{i=1}^{3}\beta_i\alpha_{ii} + \sum_{i=1}^{3}\alpha_{ii}^2 + 2\sum_{i,j=1;i<j}^{3} |\alpha_{ij}|^2 \right\} \\ &= \min_{\sigma\in\mathrm{diag}\Gamma({\mathcal{H}_\phi}^\perp)} \left\{ Tr(\rho^2) - 2\sum_{i=1}^{3}\beta_i\alpha_{ii} + \sum_{i=1}^{3}\alpha_{ii}^2 \right\}. \end{aligned} \tag{4.69}$$

In the last equation we used the fact that the minimum is achieved on the set of density matrices $\Gamma(\mathscr{H}_\phi^\perp)$ which are diagonal in the base $|\phi\rangle$, $|\phi_1\rangle$, $|\phi_2\rangle$, $|\phi_3\rangle$. The set of these density operators we denoted by $\mathrm{diag}\Gamma(\mathscr{H}_\phi^\perp)$. Therefore, the quantity (4.69) has to be minimized with respect to nonnegative coefficients α_{ii} constrained by the condition $\sum_{i=1}^{3}\alpha_{ii} = 1$. Using the method of Lagrangian multipliers one obtains the minimum at the point $\alpha_{ii} = \beta_i + \frac{1}{3}\lambda_1$ and its value is given by

$$D(\rho|\Gamma(\mathscr{H}_\phi^\perp)) = 2\sum_{i=2}^{4}|\lambda_i|^2 + \frac{4}{3}\lambda_1^2 = 2\sum_{i=2}^{4}|\langle\phi|\rho|\phi_i\rangle|^2 + \frac{4}{3}\langle\phi|\rho|\phi\rangle^2. \tag{4.70}$$

This expression can also be rewritten in the equivalent form

$$\begin{aligned} D(\rho|\Gamma(\mathscr{H}_\phi^\perp)) &= 2\left\{\sum_{i=2}^{4}\langle\phi|\rho|\phi_i\rangle\langle\phi_i|\rho|\phi\rangle + \langle\phi|\rho|\phi\rangle\langle\phi|\rho|\phi\rangle\right\} - \frac{2}{3}\langle\phi|\rho|\phi\rangle^2 \\ &= 2\langle\phi|\rho^2|\phi\rangle - \frac{2}{3}\langle\phi|\rho|\phi\rangle^2. \end{aligned} \tag{4.71}$$

■

This form (4.66) explicitly exhibits the independence of this measure on the diagonalization procedure used in its derivation.

Correspondingly, the largest achievable distance, i.e.

$$\Delta(U_\alpha) = \sup_{\phi\in\Omega_\alpha} D(\rho_{out}|\Gamma(\mathscr{H}_\phi^\perp)) = \sup_{\phi\in\Omega_\alpha}\left\{2\langle\phi|\rho_{out}^2|\phi\rangle - \frac{2}{3}\langle\phi|\rho_{out}|\phi\rangle^2\right\}, \tag{4.72}$$

is a convenient *error measure* characterizing the quality of the NOT operation for a given class of input states with a given degree of entanglement. This error measure has three important properties. Firstly, the positivity of density operators implies that it achieves its minimal (zero) value if and only if the NOT operation is ideal for all input states $|\phi\rangle \in \Omega_\alpha$, i.e.

$$\Delta(U_\alpha) = 0 \qquad \Longleftrightarrow \sup_{|\phi\rangle\in\Omega_\alpha}\langle\phi|\rho_{out}|\phi\rangle = 0. \tag{4.73}$$

Secondly, this error measure is invariant under the unitary group $\mathsf{U}(4)$. Hence, from equation (4.66) it is straightforward to prove that the distance $D(\rho|\Gamma(\mathscr{H}_\phi^\perp))$ for covariant processes (4.61) is unbiased with respect to all states from a given class Ω_α.

Proof: Suppose we have an arbitrary covariant process $\mathcal{P}$ and an input state $|\phi\rangle \in \Omega_\alpha$. We denote its associated output state by ρ_ϕ ($\rho_\phi = \mathcal{P}(|\phi\rangle\langle\phi|)$). Let us now take another input state $|\psi\rangle \in \Omega_\alpha$ connected with the state $|\phi\rangle$ by a unitary transformation $U = U_1 \otimes U_2$ ($U_1, U_2 \in \mathsf{SU}(2)$). The distance $D(\rho_\psi|\Gamma(\mathscr{H}_\psi^\perp))$ between this state and its associated output state $\rho_\psi = \mathcal{P}(|\psi\rangle\langle\psi|)$ is given by

$$\begin{aligned} D\left(\rho_\psi|\Gamma(\mathscr{H}_\psi^\perp)\right) &= 2\langle\psi|\rho_\psi^2|\psi\rangle - \frac{2}{3}\langle\psi|\rho_\psi|\psi\rangle^2 = 2\langle\psi|\mathcal{P}(|\psi\rangle\langle\psi|)^2|\psi\rangle \\ &- \frac{2}{3}\langle\psi|\mathcal{P}(|\psi\rangle\langle\psi|)|\psi\rangle^2 = 2\langle\phi|U^\dagger\mathcal{P}(U|\phi\rangle\langle\phi|U^\dagger)^2U|\phi\rangle \\ &- \frac{2}{3}\langle\phi|U^\dagger\mathcal{P}(U|\phi\rangle\langle\phi|U^\dagger)U|\phi\rangle^2. \end{aligned} \tag{4.74}$$

With the help of the covariance condition (4.47) this expression can be rewritten in the form

$$\begin{aligned} D\left(\rho_\psi|\Gamma(\mathscr{H}_\psi^\perp)\right) &= 2\langle\phi|U^\dagger U\mathcal{P}(|\phi\rangle\langle\phi|)^2U^\dagger U|\phi\rangle - \frac{2}{3}\langle\phi|U^\dagger U\mathcal{P}(|\phi\rangle\langle\phi|)U^\dagger U|\phi\rangle^2 \\ &= D\left(\rho_\phi, |\Gamma(\mathscr{H}_\phi^\perp)\right). \end{aligned} \tag{4.75}$$

■

Hence, a covariant quantum operation yields the same error (4.66) for all states of a given entanglement class Ω_α. Thus, for these processes we can omit the supremum in (4.72) and we can calculate the error as the distance (4.66) associated with an arbitrarily chosen state of the class Ω_α.

Thirdly, this error is a convex function of the quantum operation U_α. Indeed, this can be seen by considering a convex combination of two arbitrary two-qubit mixed states, say ρ and σ, and an arbitrary two-qubit pure input state, say $|\phi\rangle$. The distance $D(\rho|\Gamma(\mathscr{H}_\phi^\perp))$ fulfills the inequality

$$\begin{aligned} &D(\eta\rho + (1-\eta)\sigma|\Gamma(\mathscr{H}_\phi^\perp)) = \eta D(\rho|\Gamma(\mathscr{H}_\phi^\perp)) + (1-\eta)D(\sigma|\Gamma(\mathscr{H}_\phi^\perp)) - \\ &\eta(1-\eta)D(\rho-\sigma|\Gamma(\mathscr{H}_\phi^\perp)) \leq \eta D(\rho|\Gamma(\mathscr{H}_\phi^\perp)) + (1-\eta)D(\sigma|\Gamma(\mathscr{H}_\phi^\perp)) \end{aligned} \tag{4.76}$$

and is therefore convex. Our error measure Δ is defined as the supremum of a set of convex expressions in U_α and hence is also convex.

We have shown that the error measure Δ is a well defined figure of merit and fulfils all requirements of our covariant optimization approach presented in section 1.8. Having a well defined figure of merit, in general, the construction of an optimal quantum NOT operation is equivalent to minimizing the error measure $\Delta(U_\alpha)$ over all possible processes. In the following the resulting optimal error measure will be denoted by $\Delta_\alpha = \inf_{U_\alpha} \Delta(U_\alpha)$.

4.2.3 Non-covariant quantum NOT operations for maximally entangled qubit pairs

Before dealing with the general case let us focus on quantum NOT operations for the special class of maximally entangled (ME) pure input states $\Omega_{1/\sqrt{2}}$. Surprisingly, in this special case one is able to construct even perfect quantum NOT operations which map an arbitrary pure input state onto a pure output state but which are typically not covariant.

In order to determine the general structure of all physically feasible quantum NOT operations $\mathcal{U}$ for ME states let us impose the natural additional requirement that, if the quantum NOT operation $\mathcal{U}$ is applied twice the resulting operation is proportional to the identity operator. Therefore, the quantum NOT operation $\mathcal{U}$ we are looking for should fulfill the following requirements:

- *Orthogonality*: It maps an arbitrary pure state onto a pure state according to

$$\langle\phi|\mathcal{U}|\phi\rangle = 0 \qquad \forall\ |\phi\rangle \in \Omega_{1/\sqrt{2}} \tag{4.77}$$

- *Unitarity*

$$\mathcal{U}\mathcal{U}^\dagger = I \tag{4.78}$$

- *Cyclic property*

$$\mathcal{U}^2 = \lambda I, \qquad \text{where} \quad \lambda \in \mathbb{C}, |\lambda| = 1. \tag{4.79}$$

For our analysis we take advantage of the special basis states (sometimes referred to as the magic base) [39]

$$\begin{aligned} |e_1\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \quad |e_2\rangle = \frac{i}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\ |e_3\rangle &= \frac{i}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \quad |e_4\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right), \end{aligned} \tag{4.80}$$

in which all maximally entangled two-qubit states can be written as real-valued linear combination of these basis states. Indeed, the concurrence of an arbitrary normalized two-qubit superposition state $|\Gamma\rangle = \sum_i \gamma_i |e_i\rangle$ with complex values of γ_i is given by

$$C\left(|\Gamma\rangle\langle\Gamma|\right) = \left|\sum_i \gamma_i^2\right|. \tag{4.81}$$

Hence, for ME states this concurrence has to be equal to unity. This happens if and only if all coefficients γ_i are real-valued. In this sense all ME states form a four dimensional real Hilbert space. Expressing condition (4.77) in this magic base it turns out that all possible quantum NOT operations form a vector space of real-valued 4x4 antisymmetric matrices. The dimension of this vector space equals six and a possible basis is given by the matrices

$$\begin{aligned} U_1 &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \; U_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \; U_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \\ V_1 &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \; V_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \; V_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}. \end{aligned} \tag{4.82}$$

This set of matrices has the following interesting algebraic properties

$$\begin{aligned} &\{U_i, U_j^\dagger\} = -\{U_i, U_j\} = 2\delta_{ij} I, \;\; U_i^T = -U_i, \;\; U_i U_j = -\delta_{ij} I + \varepsilon_{ijk} U_k, \\ &\{V_i, V_j^\dagger\} = -\{V_i, V_j\} = 2\delta_{ij} I, \;\; V_i^T = -V_i, \;\; V_i V_j = -\delta_{ij} I + \varepsilon_{ijk} V_k, \;\; [U_i, V_j] = 0. \end{aligned} \tag{4.83}$$

As a consequence every linear operation with the property (4.77) is a linear superposition of U_i, V_i, i.e.

$$\mathcal{U} = \sum_{i=1}^{3} \alpha_i U_i + \beta_i V_i, \qquad \alpha_i, \beta_i \in \mathbb{R}. \tag{4.84}$$

Property (4.83) and requirement (4.78) imply the relation

$$\begin{aligned} I &= \mathcal{U}\mathcal{U}^\dagger = \sum_{i=1}^{3} \alpha_i^2 U_i U_i^\dagger + \beta_i^2 V_i V_i^\dagger + \sum_{(ij)} \left[\alpha_i\alpha_j(U_iU_j^\dagger + U_j^\dagger U_i) + \beta_i\beta_j(V_iV_j^\dagger + V_j^\dagger V_i)\right] \\ &+ \sum_{i,j=1}^{3} \alpha_i\beta_j(U_iV_j^\dagger + V_jU_i^\dagger) = \left(\sum_{i=1}^{3} \alpha_i^2 + \beta_i^2\right) I - 2\sum_{i,j=1}^{3} \alpha_i\beta_j U_iV_j. \end{aligned} \tag{4.85}$$

Taking into account the structure of the matrices U_iV_j this yields the conditions

$$\alpha_i\beta_j = 0 \qquad \Longrightarrow \begin{cases} \alpha_i = 0 \quad \wedge \quad \sum\limits_{i=1}^{3} \beta_i^2 = 1 \\ \beta_i = 0 \quad \wedge \quad \sum\limits_{i=1}^{3} \alpha_i^2 = 1 \end{cases}. \tag{4.86}$$

The quantum NOT operation fulfilling requirements (4.77), (4.78) and (4.79) has the general structure

$$\left(\mathcal{U} = \sum_{i=1}^{3} \alpha_i U_i, \quad \sum_{i=1}^{3} \alpha_i^2 = 1, \alpha_i \in \mathbb{R}\right) \vee \left(\mathcal{U} = \sum_{i=1}^{3} \beta_i V_i, \quad \sum_{i=1}^{3} \beta_i^2 = 1, \beta_i \in \mathbb{R}\right). \tag{4.87}$$

In both cases the condition (4.79)is fulfilled automatically, i.e.

$$\mathcal{U}^2 = -I. \tag{4.88}$$

Therefore, for maximally entangled two-qubit states the ideal quantum NOT operation is not unique. Its most general form is given by (4.87).

Based on the obtained perfect NOT operations for maximally entangled states, in the following section, we propose remote state protocol for maximally entangled states.

Remote state protocol for maximally entangled two qubits

Two important information tasks have attracted attention of many scientists: teleportation [13] and remote state preparation (RSP) [100]. We formulate both tasks as follows. The sender (usually called as Alice) has at her site a quantum state, which she wants to create at a distant receiver's site (usually called as Bob). In quantum teleportation Alice and Bob do not know

the identity of the state. In remote state preparation Alice wants to prepare the state at Bob's site, thus she knows the state which is to be remotely prepared.

Pati [100] and Lo [101] showed that special ensembles of states (e.g. qubit states on the equator of the Bloch sphere) can be remotely prepared using one classical bit (*cbit*) and one maximally entangled pair of qubits (*ebit*). Lo conjectured that if Alice wants to prepare remotely an arbitrary qubit she still may require two cbits and one ebit like in the teleportation protocol. The general reason why RSP protocols do not work for all states of a Hilbert space is that we are not able to perform the already mentioned perfect quantum NOT operation on an unknown quantum state. Bennet *et al* [102] found that in the presence of a large amount of prior entanglement the cost of RSP for general one-qubit states can be reduced to one cbit per qubit. Moreover, they showed that RSP (unlike teleportation) exhibits a nontrivial tradeoff between classical communication and entanglement. Devetak and Berger have proposed a low entanglement protocol [103] for an arbitrary quantum state. Zeng and Zhang generalized a minimal resources consuming RSP to higher dimensions [104]. The remote state protocol for mixed states was studied by Berry and Sanders [105]. The RSP protocol have been implemented using NMR devices over atomic distances [106] or qubits encoded into polarization of photons [107].

In this part we present a remote state protocol for the set of maximally entangled two-qubit pure states. We start with a more detailed description of Alice's task. Alice has a maximally entangled two-qubit state, let say $|\phi\rangle$. She has a complete knowledge of this state and she wants to prepare remotely this state at Bob's lab. Bob only knows, that Alice chooses the remotely prepared state from the set of maximally entangled states.

Alice's two-qubit state $|\phi\rangle$, being maximally entangled, can be decomposed according to

$$|\phi\rangle = \alpha_1|e_1\rangle + \alpha_2|e_2\rangle + \alpha_3|e_3\rangle + \alpha_4|e_4\rangle. \tag{4.89}$$

The coefficients α_i are real and fulfill the normalization condition $\sum_{i=1}^{4} \alpha_i^2 = 1$. Let us assume Alice and Bob share four qubits prepared in a pure entangled state

$$|\psi\rangle = \frac{1}{2}\left(|e_1\rangle|e_1\rangle + |e_2\rangle|e_2\rangle + |e_3\rangle|e_3\rangle + |e_4\rangle|e_4\rangle\right). \tag{4.90}$$

In the orthonormal basis $\{|0\rangle, |1\rangle\}$ this state reads

$$|\psi\rangle = \frac{1}{2}\left(|0011\rangle + |1100\rangle - |0110\rangle - |1001\rangle\right). \tag{4.91}$$

This state is sometimes called a dark state (see [108]). The 'dark' here means that the state $|\psi\rangle$ is invariant under an arbitrary local unitary transformation $U \otimes U$, where the same U acts on

both subsystems (each formed of two qubits)

$$U \otimes U|\psi\rangle = |\psi\rangle, \qquad U \in \mathsf{U}(4). \tag{4.92}$$

The equation (4.92) leads to the following important property

$$U \otimes I|\psi\rangle = I \otimes U^{\dagger}|\psi\rangle. \tag{4.93}$$

This remarkable property allows Alice to simulate an arbitrary unitary operation $U^{\dagger}$ on Bob's half of qubits by performing the unitary transformation U on her half of shared qubits. The second important property of the state (4.90) is that, it can be written as $|\Xi_{13}\rangle \otimes |\Xi_{24}\rangle$, where the ket $|\Xi\rangle$ denotes the singlet state

$$|\Xi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \tag{4.94}$$

Therefore, in principle Alice and Bob share two ebits. Alice's goal is to transform their shared state $|\psi\rangle$ into the state $|\psi_{\phi}\rangle$

$$|\psi_{\phi}\rangle = \frac{1}{2}\left\{|e_1\rangle|\phi\rangle + |e_2\rangle|\phi_1^{\perp}\rangle + |e_3\rangle|\phi_2^{\perp}\rangle + |e_4\rangle|\phi_3^{\perp}\rangle\right\} \tag{4.95}$$

where

$$|\phi_1^{\perp}\rangle = -\alpha_2|e_1\rangle + \alpha_1|e_2\rangle - \alpha_4|e_3\rangle + \alpha_3|e_4\rangle, \tag{4.96}$$

$$|\phi_2^{\perp}\rangle = -\alpha_4|e_1\rangle - \alpha_3|e_2\rangle + \alpha_2|e_3\rangle + \alpha_1|e_4\rangle, \tag{4.97}$$

$$|\phi_3^{\perp}\rangle = -\alpha_3|e_1\rangle + \alpha_4|e_2\rangle + \alpha_1|e_3\rangle - \alpha_2|e_4\rangle. \tag{4.98}$$

The kets $|\phi_1^{\perp}\rangle$, $|\phi_2^{\perp}\rangle$, $|\phi_3^{\perp}\rangle$ are chosen in order to form the orthonormal basis of the complementary subspace of the ket $|\phi\rangle$. Consider now the unitary operator

$$U_{\phi} = \begin{pmatrix} \alpha_1 & -\alpha_2 & -\alpha_4 & -\alpha_3 \\ \alpha_2 & \alpha_1 & -\alpha_3 & \alpha_4 \\ \alpha_3 & -\alpha_4 & \alpha_2 & \alpha_1 \\ \alpha_4 & \alpha_3 & \alpha_1 & -\alpha_2 \end{pmatrix}. \tag{4.99}$$

Using this operator, we can rewrite the state $|\psi_{\phi}\rangle$ into the form

$$|\psi_{\phi}\rangle = I \otimes U_{\phi}|\phi\rangle. \tag{4.100}$$

As was pointed out in (4.93), the same effect is obtained, if Alice performs the inverse unitary operation $U_{\phi}^{\dagger}$ on her part of shared qubits, i.e.

$$|\psi_{\phi}\rangle = U_{\phi}^{\dagger} \otimes I|\phi\rangle, \tag{4.101}$$

Alice's measured state	**Bob's state after measurement**	**Bob's correcting operation**
$\|e_1\rangle$	$\|\phi\rangle$	I
$\|e_2\rangle$	$\|\phi_1^{\perp}\rangle$	U_1
$\|e_3\rangle$	$\|\phi_2^{\perp}\rangle$	U_2
$\|e_4\rangle$	$\|\phi_3^{\perp}\rangle$	U_3

Figure 4.8: The table shows all possible outcomes of Alice's measurement, Bob's corresponding states and correcting NOT operations, which Bob has to perform in order to obtain the desire state.

with

$$U_{\phi}^{\dagger} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ -\alpha_2 & \alpha_1 & -\alpha_4 & \alpha_3 \\ -\alpha_4 & -\alpha_3 & \alpha_2 & \alpha_1 \\ -\alpha_3 & \alpha_4 & \alpha_1 & -\alpha_2 \end{pmatrix}. \tag{4.102}$$

Hence, using the local unitary transformation $U_{\phi}^{\dagger}$, Alice transforms their shared four-qubit state $|\psi\rangle$ into the state $|\psi_{\phi}\rangle$. Then Alice performs a von Neumann measurement in the magic basis. She gets one of the four possible results, each with probability 1/4. Every result corresponds to one state, which is created at Bob's site. If Alice finds out that the output state of her measurement is $|e_1\rangle$, she can be sure that Bob's remaining half of shared qubits is in the desired state $|\phi\rangle$. In the opposite case, Bob obtains one of the orthogonal states $|\phi_1^{\perp}\rangle$, $|\phi_2^{\perp}\rangle$, $|\phi_3^{\perp}\rangle$ depending on Alice's result of measurement. Therefore Alice sends two classical bits to communicate to Bob the outcome of the measurement. Consequently, carrying out the corresponding NOT transformation or leaving it unmodified, Bob obtains the desired state $|\phi\rangle$. Let us bring together the possible outputs and the corresponding corrections which Bob should do to get the required state. The summary of these different variants is given in Tab.(4.8). Let us emphasize, that the crucial ingredient of our approach is the use of quantum NOT operations for maximally entangled states and the use of multi-particle dark state as a source of quantum entanglement. We have found out that Alice needs to send only 2 classical bits and consumes two ebits. Depending on the information sent by Alice, Bob only performs one of the four recovery operations. It should be noted that our protocol does not require back-communication, since it is based on teleportation.

4.2.4 Optimal covariant quantum NOT operations

Motivated by results for maximally entangled states we start to solve a general problem, namely searching for optimal NOT operations for an arbitrary set of entangled states Ω_α. Our first step is to show that all requirements of our covariant optimization approach presented in section 1.8 are fulfilled.

Presumptions of covariant optimization approach

First, as we have already mentioned the set of input states Ω_α is invariant under the action of the unitary group $\mathsf{SU}(2) \otimes \mathsf{SU}(2)$ and an arbitrary pair of elements of the set Ω_α is connected by the transition action of the unitary group $\mathsf{SU}(2) \otimes \mathsf{SU}(2)$. Given an input pure state $\rho = |\phi\rangle\langle\phi|$, the corresponding set of possible outputs of ideal NOT operations is $\mathcal{K}(\rho) = \Gamma(\mathscr{H}_\phi^\perp)$. Hence, it is simple to check that it satisfies the covariance condition

$$\mathcal{K}(U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger) = U_1 \otimes U_2 \mathcal{K}(\rho) U_1^\dagger \otimes U_2^\dagger, \tag{4.103}$$

for every $U_1, U_2 \in \mathsf{SU}(2)$ and each $|\phi\rangle \in \Omega_\alpha$.

We have already proved that the merit function $D(\rho|\Gamma(\mathscr{H}_\phi^\perp))$ is convex in its first argument, achieves its minimum for $\rho \in \Gamma(\mathscr{H}_\phi^\perp)$ and fulfills the invariance property

$$D(\sigma|U_1 \otimes U_2 \mathcal{K}(\rho) U_1^\dagger \otimes U_2^\dagger) = D(U_1^\dagger \otimes U_2^\dagger \sigma U_1 \otimes U_2 | \mathcal{K}(\rho)) \tag{4.104}$$

for all $U_1, U_2 \in \mathsf{SU}(2)$, $|\phi\rangle \in \Omega_\alpha$ and an arbitrary two-qubit density operator σ. The property (4.104) is a simple consequence of the equation (4.66).

Because all requirements of our covariant optimization approach are fulfilled, we know that for any optimal quantum NOT operation U_α always an equivalent covariant quantum process (4.61), say $\hat{U}_\alpha$, can be found which fulfills the covariance condition (4.47). Thus, this latter quantum NOT process yields the same optimal error measure Δ_α for all possible two-qubit input states $|\phi\rangle \in \Omega_\alpha$. This basic observation allows us to restrict our search for the optimal quantum NOT operation for an arbitrary class Ω_α to covariant quantum processes of the form of (4.61) which minimize the error measure (4.72).

Determination of optimal two-qubit quantum NOT operations

The error measure of the output state (4.54) with respect to the normalized pure two-qubit input state $|\phi\rangle = \alpha|\uparrow\uparrow\rangle + \beta|\downarrow\downarrow\rangle$ is given by

$$\begin{aligned}\Delta(Z = V + X, Y) &= \frac{1}{12}\Big\{\big[1 + Z(1 - 4\alpha^2\beta^2) + Y(1 + 8\alpha^2\beta^2)\big]^2 \\ &\quad +6\alpha^2\beta^2(1 - 4\alpha^2\beta^2)(Z - 2Y)^2\Big\}. \end{aligned} \tag{4.105}$$

Our goal is to determine optimal two-qubit quantum NOT operations for all values of the entanglement parameter $0 \leq \alpha \leq 1/\sqrt{2}$. For this purpose we have to minimize the error of (4.105) under the constraints of complete positivity as given by the relations (4.59).

Let us first of all consider the case of non-entangled states, i.e. $\alpha = 0$. The lower bound of the error (4.105) can be derived with the help of inequality (4.59), i.e. $Y \geq -\frac{1}{9} - \frac{1}{3}(X + V)$, which yields

$$\Delta(Z = V + X, Y) \geq \frac{4}{3}\left\{\frac{1}{6}(Z)(1 - 10\alpha^2\beta^2) + \frac{2}{9}(1 - \alpha^2\beta^2)\right\}^2. \tag{4.106}$$

Minimizing the right hand side of inequality (4.106) with respect to the parameters X and V yields the minimal error

$$\Delta_0 = \frac{4}{243} \tag{4.107}$$

for $X = V = -\frac{1}{3}$. Hence, from relations (4.59) we obtain the result $Y = \frac{1}{9}$.

The same approach can be used for maximally entangled states with $\alpha = 1/\sqrt{2}$. Now, an estimation of a lower bound can be based on inequality (4.59) rewritten in the form $X + V \geq -\frac{1}{3} - 3Y$. The resulting lower bound is given by

$$\Delta(Z = V + X, Y) \geq \frac{4}{3}\left\{\frac{1}{6}(1 + 2\alpha^2\beta^2) + \frac{1}{2}Y(-1 + 10\alpha^2\beta^2)\right\}^2. \tag{4.108}$$

The minimization of this lower bound leads to the minimal error

$$\Delta_{1/\sqrt{2}} = 0. \tag{4.109}$$

It is achieved for quantum processes characterized by parameters (V, X, Y) which are element of the line segment $Y = -\frac{1}{3}$, $X + V = Z = -\frac{1}{3}$, and $X + V = \frac{2}{3}$.

Let us now consider the general case $\alpha \in (0, 1/\sqrt{2})$. Local extrema of relation (4.105) are determined by the conditions

$$\frac{\partial\Delta(Z = V + X, Y)}{\partial Z} = 0 \quad \wedge \quad \frac{\partial\Delta(Z = V + X, Y)}{\partial Y} = 0 \quad \Rightarrow \quad V = X = Y = -\frac{1}{3}. \tag{4.110}$$

The point $V = X = Y = -1/3$ at which this local minimum is reached is not contained in the tetrahedron $\overline{ABCD}$. Therefore, the minimum error has to be attained at points of the triangles which form the surface of the tetrahedron $\overline{ABCD}$. It can be checked in a straightforward way that the minima for all values of $\alpha \in (0, 1/\sqrt{2})$ are contained in the triangle $\overline{ABC}$. This latter triangle is defined by the relation $Z = X + V = -3Y - \frac{1}{3}$ with $-\frac{1}{3} \leq Y \leq \frac{1}{9}$ and $-\frac{1}{3} \leq X, V \leq 1$. With the help of the substitution $Z = -3Y - \frac{1}{3}$ in (4.105) we obtain a quadratic function of Y which is minimal at the point

$$Y_{min} = -\frac{1}{3} \; \frac{2 - 31\alpha^2\beta^2 + 20\alpha^4\beta^4}{-2 - 35\alpha^2\beta^2 + 100\alpha^4\beta^4}. \tag{4.111}$$

This condition is valid for all values of $\alpha \in (0, 1/\sqrt{2})$. However, the relation $Y \leq 1/9$ is valid only as long as $\alpha \geq \alpha_0$ with $\alpha_0 = \sqrt{(1 - \sqrt{1 - 4K})/2}$ and $K = (8 - 3\sqrt{6})/20$. The minimal error in the range $\alpha \leq \alpha_0$ is achieved by the largest Y value satisfying the condition $Y \leq 1/9$, i.e. by $Y = 1/9$. As a result we obtain the relations

$$\Delta_\alpha = \begin{cases} \frac{1}{243}\left(4 + 160\alpha^2\beta^2 - 128\alpha^4\beta^4\right), & Y = \frac{1}{9}, X = V = -\frac{1}{3}, \quad \text{for} \quad \alpha \leq \alpha_0 \\ \frac{4\alpha^2\beta^2(1-4\alpha^2\beta^2)}{2+35\alpha^2\beta^2-100\alpha^4\beta^4}, & Y_{min}, X + V = -3Y - \frac{1}{3}, \quad \text{for} \quad \alpha \geq \alpha_0 \end{cases}.$$

From (4.112) we can easily determine the value of α for which Δ_α is maximal. This happens at $\alpha_{max} = \sqrt{1/2 - \sqrt{3/20}}$. The corresponding maximum error is given by $\Delta_{\alpha_{max}} = \frac{4}{75}$ and the associated optimal quantum NOT operation is characterized by the parameter range $Y = -1/15$, $X + V = -2/15$ with $-1/3 \leq X, V \leq 1$.

Discussion

We discuss obtained optimal NOT operations and compare them with known results in literature. It was shown that for all classes of states Ω_α all optimal quantum NOT processes are determined by points (V, X, Y) of the triangle $\overline{ABC}$ of Fig.4.2.1. Therefore, for an optimal quantum NOT process the operator K_{00} of the Kraus representation (4.61) vanishes. Thus, minimizing the quantity (4.105) with respect to points of the triangle $\overline{ABC}$ yields the final solution. Depending on the value of α two cases can be distinguished. For $\alpha \leq \alpha_0$ with $\alpha_0 = \sqrt{\frac{1-\sqrt{1-4K}}{2}} \approx 0.1836$ and $K = \frac{8-3\sqrt{6}}{20}$ the minimal error

$$\Delta_\alpha = \frac{1}{243}\left(4 + 160\alpha^2\beta^2 - 128\alpha^4\beta^4\right) \tag{4.112}$$

is obtained. The resulting optimal quantum NOT operation is independent of the parameter α and is characterized by the point $(V = -\frac{1}{3}, X = -\frac{1}{3}, Y = \frac{1}{9})$. It turns out that this particular optimal quantum NOT process U_{SEP} consists of two one-qubit optimal covariant U-NOT

processes u^1 applied to each of the qubits separately, i.e. $U_{SEP} = u^1 \otimes u^1$ with

$$u^1(\rho) = \frac{1}{3}\left(2I - \rho\right). \tag{4.113}$$

These latter optimal one-qubit U-NOT quantum processes were studied in detail in [5]. According to (4.61) a Kraus representation of the optimal two-qubit quantum NOT operation U_{SEP} is given by

$$U_{SEP}(\rho_{in}) = \sum_{i,j=1}^{3} K_{ij}\rho_{in}K_{ij}^{\dagger} \qquad \text{with} \quad K_{ij} = \frac{1}{3}\sigma_i \otimes \sigma_j. \tag{4.114}$$

Optimal quantum NOT processes with $\alpha \geq \alpha_0$ yield an error of magnitude

$$\Delta_\alpha = \frac{4\alpha^2\beta^2(1 - 4\alpha^2\beta^2)}{2 + 35\alpha^2\beta^2 - 100\alpha^4\beta^4} \tag{4.115}$$

and they are characterized by points (V, X, Y) on the straight line

$$Y = -\frac{1}{3}\frac{2 - 31\alpha^2\beta^2 + 20\alpha^4\beta^4}{-2 - 35\alpha^2\beta^2 + 100\alpha^4\beta^4}, \;\; X + V = \frac{2}{3}\frac{4 - 29\alpha^2\beta^2 - 20\alpha^4\beta^4}{-2 - 35\alpha^2\beta^2 + 100\alpha^4\beta^4}, \;\; X, V \geq -\frac{1}{3}. \tag{4.116}$$

Each triple of parameters (V, X, Y) from this one-parameter line segment defines the Kraus representation (4.61) of the optimal two-qubit quantum NOT operation $\widehat{U}_\alpha(V)$ for a particular class of states Ω_α.

These considerations show that an ideal covariant two-qubit quantum NOT process with zero-valued error measure can only be obtained for maximally entangled states. Such a process is characterized by any point (V, X, Y) satisfying the conditions $Y = -\frac{1}{3}, X + V = Z = \frac{2}{3}$, $(X, V \geq -\frac{1}{3})$. Therefore, ideal covariant two-qubit quantum NOT processes form a one-parameter family. This reflects the fact that there is a huge class of non-covariant ideal quantum NOT operations (4.87). Each element $\mathcal{U}$ of this class corresponds to some covariant counterpart $\widehat{\mathcal{U}}$ with the same error (4.72). Thus, for maximally entangled states the ideal covariant two-qubit NOT operations are characterized by the parameter range $-\frac{1}{3} \leq V \leq 1$. A Kraus representation of these processes is given by

$$U_{ME}(V)(\rho_{in}) = \sum_{i=1}^{3}\left(K_{0i}\rho_{in}K_{0i}^{\dagger} + K_{i0}\rho_{in}K_{i0}^{\dagger}\right), \tag{4.117}$$

with

$$K_{0i} = \frac{1}{2}\left(\frac{1}{3} + V\right)^{1/2}\sigma_i \otimes I, \quad K_{i0} = \frac{1}{2}\left(1 - V\right)^{1/2} I \otimes \sigma_i. \tag{4.118}$$

The error Δ_α achieves its maximal value for $\alpha^2\beta^2 = \frac{1}{10}$, i.e. $\alpha_{max} = \sqrt{\frac{1}{2} - \sqrt{\frac{3}{20}}}$. The corresponding maximal error is given by $\Delta_{\alpha_{max}} = \frac{4}{75}$ and its associated quantum processes are

characterized by the points (V, X, Y) with $Y = -\frac{1}{15}$ and $X + V = Z = -\frac{2}{15}$ $(X, V \geq -\frac{1}{3})$. One of the processes satisfying these conditions is the four-dimensional covariant U-NOT process $\mathcal{G}_{NOT}$ introduced in [40]. This particular covariant two-qubit U-NOT process minimizes the error with respect to all possible two-qubit pure input states independent of their degree of entanglement. This special process is characterized by the parameters $X = V = Y = -\frac{1}{15}$ and it maps an arbitrary two-qubit input state ρ onto the output state

$$\rho_{out} = \mathcal{G}_{NOT}(\rho) = \frac{1}{15}\left(4I - \rho\right). \tag{4.119}$$

Analogous to the case of cloning entangled pure two-qubit states it appears that the set $\Omega_{\alpha_{max}}$ with the maximal error measure determines the quality of global NOT operations $\mathcal{G}$. Moreover, surprisingly both these classes ($\Omega_{\alpha_{max}}$ and $\Omega_{\alpha_{min}}$ - see section 4.1.4) are the same, i.e. $\alpha_{max} = \alpha_{min}$.

In summary, the smallest achievable errors Δ_α for these optimal covariant two-qubit quantum NOT processes $\hat{U}_\alpha$ are given by

$$\Delta_\alpha = \begin{cases} \frac{1}{243}\left(4 + 160\alpha^2\beta^2 - 128\alpha^4\beta^4\right), & U_{SEP} = u^1 \otimes u^1, \quad \text{for} \quad \alpha \leq \alpha_0 \\ \frac{4\alpha^2\beta^2(1-4\alpha^2\beta^2)}{2+35\alpha^2\beta^2-100\alpha^4\beta^4}, & \widehat{U}_\alpha(V), \quad \text{for} \quad \alpha \geq \alpha_0 \\ \frac{4}{75}, & U_{\alpha_{max}} = \mathcal{G}_{NOT}, \quad \text{for} \quad \alpha = \alpha_{max} \\ 0, & U_{ME}(V), \quad \text{for} \quad \alpha = \frac{1}{\sqrt{2}} \end{cases}$$

and their dependence on the degree of entanglement α is depicted in Fig. 4.2.4. The optimal way to complement two-qubit pure separable states with $\alpha = 0$ is to perform one-qubit covariant U-NOT quantum operations on each qubit independently. The resulting minimum error for separable states is given by $\Delta_0 = \frac{4}{243}$. This quantum process also yields the minimal error for two-qubit pure states with $\alpha \leq \alpha_0$. But the minimum error Δ_α increases monotonically with the degree of entanglement up to the critical value $\alpha_0 \approx 0.1836$ with $\Delta_{\alpha_0} \approx 0.0373$. For $\alpha \geq \alpha_0$ the covariant processes $\widehat{U}_\alpha(V)$ are optimal. These processes reach their maximum error at $\alpha_{max} = \sqrt{\frac{1}{2} - \sqrt{\frac{3}{20}}}$ and for maximally entangled states with $\alpha = 1/\sqrt{2}$ the error vanishes.

These results demonstrate that only in the case of ME states one is able to construct ideal covariant quantum NOT processes. This implies that there are no non-covariant ideal quantum NOT processes for non-maximally entangled pure states. This can be proved indirectly. Suppose that such processes existed. In this case we were able to construct to each ideal non-covariant quantum NOT process a corresponding ideal covariant process. However, this is in direct contradiction with our findings. Moreover, this fact also tells us that there is no magic base for sets of states Ω_α $(\alpha \neq \frac{1}{\sqrt{2}})$. Only maximally entangled states make up a real subspace

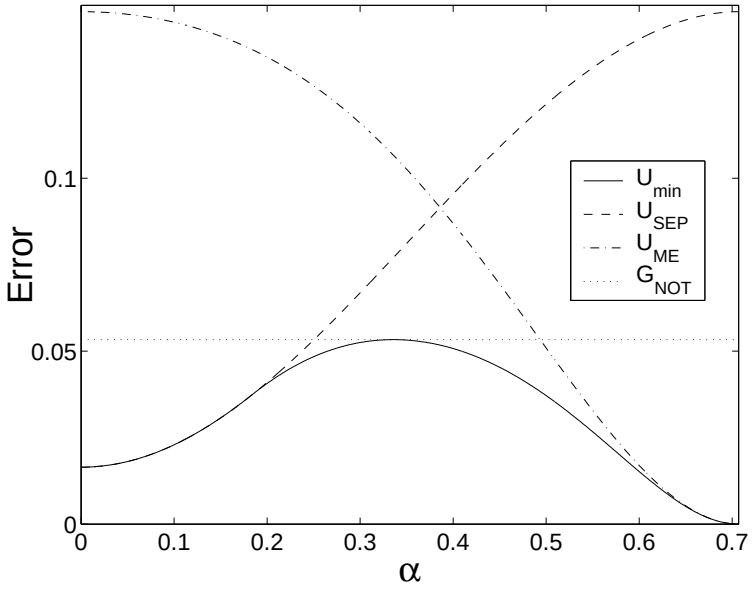

Figure 4.9: The minimum error (4.72) and the errors of the three relevant U-NOT processes and their dependence on the degree of entanglement α. The solid line represents the optimal minimum error. The dashed line U_{SEP} corresponds to an independent application of two one-qubit covariant U-NOT operations u^1 to each qubit from the entangled pair. The dashed-dotted line U_{ME} corresponds to the ideal covariant U-NOT map for maximally entangled states. The dotted line represents the minimum achievable error for an unknown two-qubit pure state if its degree of entanglement is unknown.

of the Hilbert space of two qubits. This emphasizes once more the special character of the set of maximally entangled states in comparison with all other pure entangled states. Finally, searching for optimal NOT operations suggested special significance of the class of pure entangled two-qubit states Ω_α with $\alpha = \alpha_{min} = \alpha_{max}$. In both cases, cloning and complementing entangled two-qubit pure states, this class exhibits the worst quality and the optimal copying and complementing processes for this class are identical with the global ones. In other words, if one is searching for an universal cloning machine for all pure two-qubit states we can restrict ourselves to the class Ω_α with $\alpha = \alpha_{min} = \alpha_{max}$.

4.2.5 General representation of covariant two-qubit processes

Based on the results of Sec.4.2.4 all possible completely positive covariant two-qubit processes as defined by (4.61) can be represented by convex combinations of four basic quantum processes which correspond to the corners of the tetrahedron $\overline{ABCD}$ of Fig.4.2.1. For this purpose let us briefly summarize the graphical representation of these completely positive covariant quantum maps. According to the results of Appendix 4.2.4 all optimal two-qubit quantum NOT operations have to be presented by points of the triangle $\overline{ABC}$. Thereby, point $B = (V = -\frac{1}{3}, X = -\frac{1}{3}, Y = \frac{1}{9})$ characterizes a quantum NOT operation minimizing the error (4.72) for classes of states Ω_α with $\alpha \leq \alpha_0$. Points on straight lines specified by the parameters (4.116) characterize optimal quantum NOT processes minimizing the error (4.72) for the classes of states Ω_α with $\alpha \geq \alpha_0$. In particular, points with $Y = -\frac{1}{3}, X + V = Z = \frac{2}{3}$,$(X, V \geq -\frac{1}{3})$ define optimal quantum NOT processes for maximally entangled states. The line segments $\overline{AD}$ and $\overline{CD}$ correspond to the restrictions $V = 1$ and $X = 1$. Therefore, they specify completely positive covariant processes which do not change the reduced density operator of the first or the second qubit. The process corresponding to the point D leaves both reduced density operators unchanged. So, it represents the identity operations. Furthermore, the processes represented by the points $(A = V = 1, X = -\frac{1}{3}, Y = -\frac{1}{3})$ and $(C = V = -\frac{1}{3}, X = 1, Y = -\frac{1}{3})$ are ideal covariant quantum NOT operations for maximally entangled states and moreover they do not change the reduced density operators of the first and second qubit. Therefore, we have the correspondences

$$U_{ME}^{(1)} \longleftrightarrow A, \qquad U_{SEP} \longleftrightarrow B, \qquad U_{ME}^{(2)} \longleftrightarrow C, \qquad I \longleftrightarrow D. \tag{4.120}$$

In terms of these special quantum processes all possible completely positive covariant two-qubit processes can be represented as their convex combinations. Thus, a two-qubit quantum operation (4.46) is completely positive and fulfills the covariance condition (4.47) if and only if it can be expressed as a linear convex combination of these basic quantum operations, i.e. (4.120)

$$\mathcal{P}_{a_1,a_2,a_3,a_4} = a_1 I + a_2 U_{SEP} + a_3 U_{ME}^{(1)} + a_4 U_{ME}^{(2)}, \qquad a_i \geq 0 \quad \text{and} \quad \sum_{i=1}^{4} a_i = 1. \tag{4.121}$$

In the following we show how to calculate the coefficients (a_i) appearing in the convex decomposition (4.121) for an arbitrary covariant two-qubit process and point out some useful properties and relations between the covariant processes. The hinge of our approach is the fact that the basic covariant processes I, U_{SEP}, $U_{ME}^{(1)}$ and $U_{ME}^{(2)}$ are mutually orthogonal. One can

check the orthogonal property simply by expressing these maps in the standard computational base ($P^{(mn)}$) of $4x4$-matrices, defined as $P_{ij}^{(mn)} = \delta_{im}\delta_{jn}$. For explicit forms of these maps see [109]. Using these expressions it is now easy to prove that the maps I, U_{SEP}, $U_{ME}^{(1)}$ and $U_{ME}^{(2)}$ are indeed mutually orthogonal. Among the properties of the analyzed operators let us point out that they are also traceless, i.e.

$$\begin{aligned} Tr\left(U_{SEP}\right) &= 0, \qquad Tr\left(U_{ME}^{(1)}\right) = 0, \qquad Tr\left(U_{ME}^{(1)}\right) = 0, \\ Tr\left(U_{ME}^{(1)}U_{SEP}\right) &= 0, \quad Tr\left(U_{ME}^{(2)}U_{SEP}\right) = 0, \quad Tr\left(U_{ME}^{(1)}U_{ME}^{(2)}\right) = 0. \end{aligned} \tag{4.122}$$

Let us now consider an arbitrary fixed covariant two-qubit covariant process, let say D, and denote its corresponding coefficients of convex decomposition (4.121) by d_i, i.e.

$$D = d_1 I + d_2 U_{SEP} + d_3 U_{ME}^{(1)} + d_4 U_{ME}^{(2)}.$$

Being aware of (4.122) one can show finally

$$d_1 = \frac{1}{4}Tr\left(D\right), \quad d_2 = \frac{Tr\left(DU_{SEP}\right)}{Tr\left(U_{SEP}^2\right)}, \quad d_3 = \frac{Tr\left(DU_{ME}^{(1)}\right)}{Tr\left({U_{ME}^{(1)}}^2\right)}, \quad d_4 = \frac{Tr\left(DU_{ME}^{(2)}\right)}{Tr\left({U_{ME}^{(2)}}^2\right)}. \tag{4.123}$$

For example, the covariant two-qubit NOT process $\mathcal{G}_{NOT}$ (studied in [40]), which is the optimal NOT operation with respect to all possible two-qubit pure input states independent of their degree of entanglement, has the convex decomposition (4.121) in the form

$$\mathcal{G}_{NOT} = 0.6U_{SEP} + 0.2U_{ME}^{(1)} + 0.2U_{ME}^{(2)}. \tag{4.124}$$

The other feature of covariant two-qubit processes is that, if we apply two successive in general different covariant two-qubit processes we obtain again an covariant two-qubit process

$$\mathcal{P} \ -\text{covariant}, \ \mathcal{Q} \ -\text{covariant} \implies \mathcal{P}\mathcal{Q} \ -\text{covariant}. \tag{4.125}$$

It is easy to prove the latter statement and the following table (4.2.5) shows how to obtain corresponding coefficients of convex decomposition of the covariant process $\mathcal{P}\mathcal{Q}$.

We would like to draw attention to two interesting facts. First, the base covariant processes I, U_{SEP}, $U_{ME}^{(1)}$ and $U_{ME}^{(2)}$ commutate with each other. As a simple consequence we have commutativity of arbitrary two covariant processes. In other words, it does not matter in which order we apply a sequence of covariant two-qubit processes. Second, the successive application of NOT operations $U_{ME}^{(1)}$ and $U_{ME}^{(2)}$ is equivalent to the application of U_{SEP}

$$U_{ME}^{(1)}U_{ME}^{(2)} = U_{SEP}. \tag{4.126}$$

Covariant process	a_1	a_2	a_3	a_4
U_{SEP}^2	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{2}{9}$	$\frac{2}{9}$
${U_{ME}^{(1)}}^2$	$\frac{1}{3}$	0	$\frac{2}{3}$	0
${U_{ME}^{(2)}}^2$	$\frac{1}{3}$	0	0	$\frac{2}{3}$
$U_{SEP}U_{ME}^{(1)}$	0	$\frac{2}{3}$	0	$\frac{1}{3}$
$U_{ME}^{(1)}U_{SEP}$	0	$\frac{2}{3}$	0	$\frac{1}{3}$
$U_{SEP}U_{ME}^{(2)}$	0	$\frac{2}{3}$	$\frac{1}{3}$	0
$U_{ME}^{(2)}U_{SEP}$	0	$\frac{2}{3}$	$\frac{1}{3}$	0
$U_{ME}^{(1)}U_{ME}^{(2)}$	0	1	0	0
$U_{ME}^{(2)}U_{ME}^{(1)}$	0	1	0	0

Table 4.1: Convex decompositions (4.121) of products of basic covariant processes.

4.2.6 Physical implementation of covariant processes

The previous section demonstrated how to obtain the appropriate coefficients of the convex decomposition (4.121). In this part we will introduce an unitary implementation of an arbitrary covariant two-qubit process based on our knowledge of its convex decomposition (4.121). Our approach consists of two main ingredients: a master unitary operator, which is always the same for all covariant processes and a control ancillary system, which is changed according to a given covariant process to be implemented.

To be precise let us start with some useful notation. Our principal system of two qubits is four-dimensional and we will denote its Hilbert space by $\mathscr{H}$. Further, we introduce a new 16-dimensional ancillary Hilbert space $\mathscr{H}_{ancilla}$, e.g. system of four qubits, and we choose some its orthonormal base $|e_1\rangle$, $|e_2\rangle$, ..., $|e_{16}\rangle$.

Our consecution results from two facts. First, Kraus operators (acting on the Hilbert space $\mathscr{H}$) in Kraus representation (4.61) are unitary up to a normalization. Second, Kraus operators in the decompositions of extremal covariant processes I, U_{SEP}, $U_{ME}^{(1)}$ and $U_{ME}^{(2)}$ have no intersections. Indeed, the identity is simply represented by a Kraus operator $K_{00}(X = V =$

$Y = 1) = I$, the covariant process $U^{(1)}_{ME}$ is represented by Kraus operators $K_{0j}(X = Y = -1/3, V = 1) = 1/\sqrt{3}I \otimes \sigma_j$, the covariant process $U^{(2)}_{ME}$ is represented by Kraus operators $K_{j0}(V = Y = -1/3, X = 1) = 1/\sqrt{3}\sigma_j \otimes I$, and the covariant process $U^{(1)}_{SEP}$ is represented by Kraus operators $K_{ij}(X = V = -1/3, Y = 1/9) = 1/3\sigma_i \otimes \sigma_i$, $i, j \in \{1, 2, 3\}$. All other Kraus operators in the enumerated decompositions are vanishing. Hence, let us define new operators

$$\begin{aligned} F_{00} &= K_{00}(X = V = Y = 1) = I, \\ F_{0j} &= \sqrt{3}K_{0j}(X = Y = -1/3, V = 1) = I \otimes \sigma_j, \\ F_{j0} &= \sqrt{3}K_{j0}(V = Y = -1/3, X = 1) = \sigma_j \otimes I, \\ F_{ij} &= 3K_{ij}(X = V = -1/3, Y = 1/9) = \sigma_i \otimes \sigma_i \\ & \qquad\qquad i, j \in \{1, 2, 3\}. \end{aligned} \tag{4.127}$$

All these operators are unitary and we can design a master block diagonal unitary operator acting on the Hilbert space $\mathscr{H} \otimes \mathscr{H}_{ancilla}$

$$\mathcal{U} = \begin{pmatrix} F_{00} & & & & & & & & & & & & & & & \\ & F_{01} & & & & & & & & & & & & & & \\ & & F_{02} & & & & & & & & & & & & & \\ & & & F_{03} & & & & & & & & & & & & \\ & & & & F_{10} & & & & & & & & & & & \\ & & & & & F_{20} & & & & & & & & & & \\ & & & & & & F_{30} & & & & & & & & & \\ & & & & & & & F_{11} & & & & & & & & \\ & & & & & & & & F_{12} & & & & & & & \\ & & & & & & & & & F_{13} & & & & & & \\ & & & & & & & & & & F_{21} & & & & & \\ & & & & & & & & & & & ... & & & & \\ & & & & & & & & & & & & F_{33} & & & \end{pmatrix}. \tag{4.128}$$

Hence, for example the operator F_{01} acts on the space $\mathscr{H} \otimes span\{|e_2\rangle\}$ and so on.

Let us now choose an arbitrary but fixed covariant two-qubit process, let say $\mathcal{A}$, and suppose its convex decomposition in the form $\mathcal{A} = a_1 I + a_2 U_{SEP} + a_3 U^{(1)}_{ME} + a_4 U^{(2)}_{ME}$. For an unitary implementation of this covariant process we need ancillary subsystem to be in the state

$$\begin{aligned} \sigma(a_1, a_2, a_3, a_4) &= a_1|e_1\rangle\langle e_1| + \frac{a_2}{3}\left(|e_2\rangle\langle e_2| + |e_3\rangle\langle e_3| + |e_4\rangle\langle e_4|\right) + \frac{a_3}{3}\big(|e_5\rangle\langle e_5| + \\ & \quad |e_6\rangle\langle e_6| + |e_7\rangle\langle e_7|\big) + \frac{a_4}{9}\left(|e_8\rangle\langle e_8| + ... + |e_{16}\rangle\langle e_{16}|\right). \end{aligned} \tag{4.129}$$

Now, we can formulate the main result of this part.

Theorem 4.2.1

$$\mathcal{A}(\rho) = Tr_{\mathcal{H}_{ancilla}} \mathcal{U} \left\{ \rho \otimes \sigma(a_1, a_2, a_3, a_4) \right\} \mathcal{U}^{\dagger}. \tag{4.130}$$

Proof: If we specify the trace operation in terms of base vectors $|e_i\rangle$, we get step by step

$$\begin{aligned}
Tr_{\mathcal{H}_{ancilla}} \quad & \mathcal{U} \left\{ \rho \otimes \sigma(a_1, a_2, a_3, a_4) \right\} \mathcal{U}^{\dagger} = \sum_{k=1}^{16} \langle e_k | \mathcal{U} \left\{ \rho \otimes \sigma(a_1, a_2, a_3, a_4) \right\} \mathcal{U}^{\dagger} | e_k \rangle \\
& = a_1 \langle e_1 | \mathcal{U} | e_1 \rangle \rho \langle e_1 | \mathcal{U} | e_1 \rangle + a_2 \left\{ \sum_{i=2}^{4} \frac{1}{\sqrt{3}} \langle e_i | \mathcal{U} | e_i \rangle \rho \frac{1}{\sqrt{3}} \langle e_i | \mathcal{U} | e_i \rangle \right\} + \\
& a_3 \left\{ \sum_{i=5}^{7} \frac{1}{\sqrt{3}} \langle e_i | \mathcal{U} | e_i \rangle \rho \frac{1}{\sqrt{3}} \langle e_i | \mathcal{U} | e_i \rangle \right\} + a_4 \left\{ \sum_{i=8}^{16} \frac{1}{3} \langle e_i | \mathcal{U} | e_i \rangle \rho \frac{1}{3} \langle e_i | \mathcal{U} | e_i \rangle \right\} \\
& = a_1 F_{00} \rho F_{00}^{\dagger} + a_2 \left\{ \sum_{i=1}^{3} \frac{1}{\sqrt{3}} F_{0i} \rho \frac{1}{\sqrt{3}} F_{0i}^{\dagger} \right\} + a_3 \left\{ \sum_{i=1}^{3} \frac{1}{\sqrt{3}} F_{i0} \frac{1}{\sqrt{3}} F_{i0}^{\dagger} \right\} \\
& + a_4 \left\{ \sum_{i=1}^{3} \sum_{j=1}^{3} \frac{1}{3} F_{ij} \rho \frac{1}{3} F_{ij}^{\dagger} \right\} = a_1 K_{00} \rho K_{00}^{\dagger} + a_2 \left\{ \sum_{i=1}^{3} K_{0i} \rho K_{0i}^{\dagger} \right\} \\
& + a_3 \left\{ \sum_{i=1}^{3} K_{i0} \rho K_{i0}^{\dagger} \right\} + a_4 \left\{ \sum_{i=1}^{3} \sum_{j=1}^{3} K_{ij} \rho E_{ij}^{\dagger} \right\} = \\
& a_1 \rho + a_2 U_{SEP}(\rho) + a_3 U_{ME}^{(1)}(\rho) + a_4 U_{ME}^{(2)}(\rho) = \mathcal{A}(\rho).
\end{aligned} \tag{4.131}$$

■

Let us make the situation more comprehensible by analyzing in detail the case of the covariant process $U_{ME}^{(1)}$. In this particular case we introduce control ancillary two-qubit system in the state $\sigma = \frac{1}{3} \{ |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| \}$ and the unitary transformation

$$\mathcal{U}_{ME}^{(1)} = \begin{pmatrix} F_{01} & & & \\ & F_{02} & & \\ & & F_{03} & \\ & & & I \end{pmatrix}, \tag{4.132}$$

acting on the tensor product of our principal system and the ancillary system, both written in the standard computational basis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Composing these two ingredients we can implement the covariant NOT operation for maximally entangled states $U_{ME}^{(1)}$ as

$$U_{ME}^{(1)}(\rho) = Tr_{ancilla} \mathcal{U}_{ME}^{(1)} \left\{ \rho \otimes \sigma \right\} {\mathcal{U}_{ME}^{(1)}}^{\dagger}. \tag{4.133}$$

4.2.7 Quantum circuit scheme

In this section we propose a quantum network, which performs the master unitary transformation (4.128). Let us consider four control qubits (ancillary system) and chose the basis $\{|e_i\rangle\}$ as the standard computational basis:

$$\begin{aligned}
&|e_1\rangle = |0000\rangle, \quad |e_2\rangle = |0001\rangle, \quad |e_3\rangle = |0010\rangle, \quad |e_4\rangle = |0011\rangle, \quad |e_5\rangle = |0100\rangle,\\
&|e_6\rangle = |0101\rangle, \quad |e_7\rangle = |0110\rangle, \quad |e_8\rangle = |0111\rangle, \quad |e_9\rangle = |1000\rangle, \quad |e_{10}\rangle = |1001\rangle,\\
&|e_{11}\rangle = |1010\rangle, \quad |e_{12}\rangle = |1011\rangle, \quad |e_{13}\rangle = |1100\rangle, \quad |e_{14}\rangle = |1101\rangle, \quad |e_{15}\rangle = |1110\rangle,\\
&|e_{16}\rangle = |1111\rangle. \qquad (4.134)
\end{aligned}$$

As can be seen from the form of the master unitary transformation (4.128), these four qubits control which unitary transformation F_{ij} will be applied on our principal system of two qubits. For instance, if the control ancillary system is in the state $|e_2\rangle$, the unitary transformation $F_{01} = I \otimes X$ will be performed on our principal system. Hence we introduce five qubit $C^4(U)$ operations (see Fig. (4.10)). Suppose we have 5 qubits (4 control qubits and 1 target qubit) and U is an one-qubit unitary operation acting on our target qubit. Then we define the controlled operation $C^4(U)$ as follows

$$C^4(U)|x_1x_2x_3x_4\rangle|\psi\rangle \equiv |x_1x_2x_3x_4\rangle U^{x_1x_2x_3x_4}|\psi\rangle, \qquad (4.135)$$

where $x_1x_2x_3x_4$ in the exponent of U means the product of the bits $x_1, x_2, x_3, x_4 \in \{0, 1\}$. In other words, the unitary operation U will be applied on the state $|\psi\rangle$ only if four control qubits are set to the state $|e_{16}\rangle = |1111\rangle$. Gates which implement the conditional operation (4.135) was studied in [110].

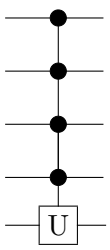

Figure 4.10: Circuit representation for the $C^4(U)$ operation, where U is a unitary operator on one qubit.

Using the controlled operation $C^4(U)$ we can design various conditional gates on the target qubit. For instance, suppose we wish to implement a five-qubit gate in which the fifth qubit is transformed by a unitary transformation U, conditional on the first, second, third (control) qubit being set to zero and the fourth qubit being set to one. In Fig. 4.11 we introduce a circuit notation for this gate, together with an equivalent circuit in terms of the gate $C^4(U)$ and the well-known X-gate, which implements one-qubit unitary transformation σ_1.

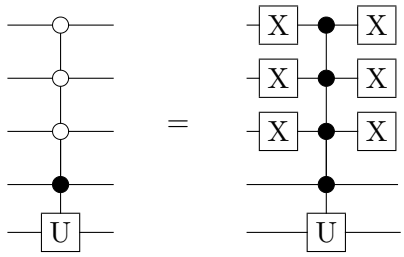

Figure 4.11: Controlled operation with a U gate being performed on the fifth qubit, conditional on the first, second, third qubit being set to zero and the fourth qubit being set to one.

Furthermore, in our network we use so-called multi-target conditional gates. This is a natural generalization of one-qubit conditional gates, which we have introduced above. It supposes that we have more target qubits, let say d qubits, and a set of one-qubit unitary operations $\{U_i\}_{i=1}^d$ (each unitary operation U_i acts on qubit i). These unitary operations are simultaneously performed on its qubits, if controlled qubits are set to the prescribed state. In Fig. 4.12 we define a useful circuit notation for the case in which an operation U is performed on the fifth qubit and an operation V is performed on the sixth qubit, conditional on the first four qubits.

Using these conditional gates we can finally design a quantum network, which performs the master unitary transformation (4.128). The circuit scheme for this network is depicted in Fig. 4.13. The first four qubits form the control ancillary system, which enters into the network in the state (4.129). Our principal system of last two qubits comes into the network in the state ρ. The composite system of these six qubits is governed by the master unitary transformation (4.128), which is implemented by the network displayed in figure 4.13. At the output we discard the first four control qubits leaving our principal system in the desired state $\mathcal{A}(\rho)$ (4.130).

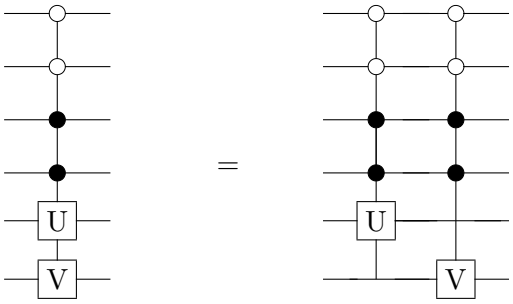

Figure 4.12: Circuit implementation of the gate which performs an operation U on the fifth qubit and an operation V on the sixth qubit, conditional on the first four qubits.

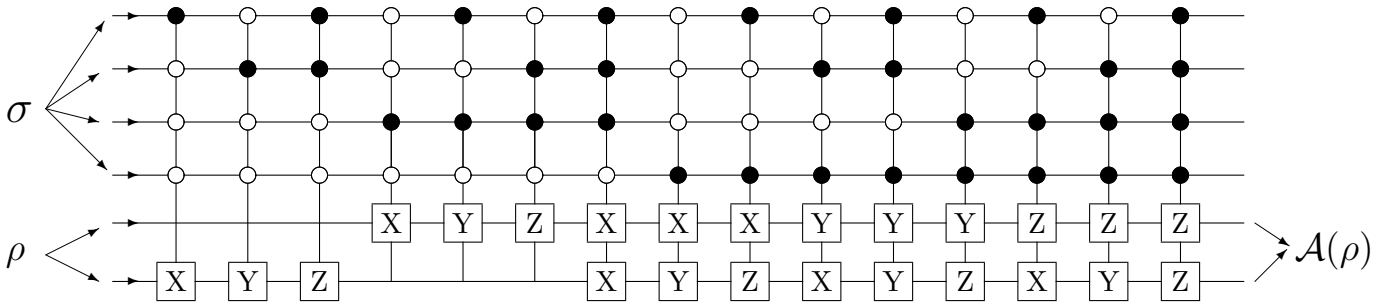

Figure 4.13: Quantum network which performs the master unitary network (4.128).

4.2.8 Conclusion

A classification of all possible completely positive covariant two-qubit quantum processes, which fulfill the covariance condition (4.47), was presented. It was shown that any of these processes can be represented by a convex sum of four special covariant two-qubit quantum processes. On the basis of this general classification all possible completely positive covariant quantum processes were constructed which describe quantum NOT operations acting on pure two-qubit states of a particular degree of entanglement in an optimal way. It was shown that for maximally entangled pure two-qubit input states even an ideal covariant quantum NOT operations can be constructed. Furthermore, for this particular class of input states it is possible to find the general structure of all possible ideal quantum NOT operations. We have presented a network of

quantum gates which is capable of implementing a large variety of universal two qubit processes. The design is based on several interesting properties of covariant processes which were briefly discussed.

Chapter 5

Summary and conclusions

In this thesis we investigated two related topics, namely the sharing bipartite entanglement in multi-qubit states and the role of entanglement in quantum information processing.

First, in order to describe bipartite entanglement structures in multi-qubit states we proposed a concept of weighted entangled graphs and found a broad class of weighted graphs for which there are multi-qubit states having bipartite entanglement structures described by this set of graphs.

Second, we have analyzed the possibility of generating multi-qubit entangled states in passive optical networks with one and two excitations. In particular, we have derived explicit expressions for the concurrence for single and two particle initial states in arbitrary passive networks. Based on these formulas we have found the general structure of entanglement in networks with one excitation and we have discussed the maximum attainable entanglement in passive networks in general. We have designed linear passive networks leading to a prescribed bipartite entanglement pattern. We specified all obtained results for Ising-type networks.

Third, we investigated optimal copying of two entangled pure qubits. We considered a cloning machine whose input consists of a pair of qubits with a given degree of entanglement and which should produce two copies of the input pure state. The problem of finding the optimal cloning transformation can be viewed as the determination of completely positive maps which maximize a given figure of merit. Moreover, we require the copying process works equally well on all states of our interest, i.e. we require the same quality for all input states. With the view to settle the copying of entangled qubits we have constructed a family of covariant transformations. Based on this construction we have found optimal copying processes for all sets of two-qubit pure states with a given degree of entanglement and with respect to two different figures of

merit, i.e. two-particle test (local fidelity) and four-particle test (global fidelity). Surprisingly, these different figures of merit generates different optimal copying processes. We have analyzed and discussed properties of both of them.

Finally, we have studied the role of entanglement in an special quantum information process called the NOT operation or complementing a quantum state. The starting point in this problem was the fact that maximally entangled two-qubit states form a real subspace in the whole two-qubit Hilbert space. It implies the possibility to design perfect quantum NOT operations for this set of maximally entangled states. We have found the general structure of these operations and based on this we have proposed a remote state protocol for maximally entangled states. Motivated by this result we have analyzed how initial quantum entanglement affects the quality of optimal NOT operations. We have considered a set of input pure two-qubit states with a given degree entanglement and we have searched for quantum operations which map an arbitrary state from this set on its orthogonal complement in an optimal way. In order to find the optimal NOT operations for all sets of entangled states we have explored a convex set of completely positive quantum operations which transform two-qubit states of a given degree of entanglement in a covariant way. Using our general analysis all optimal quantum operations were determined which perform such a quantum NOT operation for all possible two-qubit pure input states of a given degree of entanglement with the same quality. We have shown that the aforesaid convex set is generated by four elementary two-qubit quantum operations (identity, the optimal NOT operation for separable states and two optimal NOT operations for maximally entangled states), which form the vertices of a three dimensional polytope. In addition, special algebraic properties of this convex set were found. Based on these properties we have proposed a systematic approach to the problem of designing elementary quantum gate sequences which implement the family of covariant quantum operations. With the help of additional auxiliary qubits it is possible to design a quantum network which involves a particular sequence of conditional unitary qubit gates. Depending on the preparation of the auxiliary qubits any covariant quantum operation within this convex set can be implemented by this quantum network. The advantage of this particular network implementation is that the sequence of conditional unitary qubit gates involved is independent of the covariant quantum operation under consideration.

Appendix A

Fidelity

Distance measures are quantitative parameters of how close two quantum states are. In this part we present properties of the distance measure usually called as *fidelity*.

Let ρ and σ are two states of $\mathsf{S}(\mathscr{H})$. Then the fidelity of states ρ and σ is defined to be

$$F(\rho,\sigma) \equiv \mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{A.1}$$

We have to emphasize that fidelity is not a metric on density operators. However, this distance does give rise to a useful measure with interesting properties:

- From the definition (A.1) the fidelity for a pure state $|\psi\rangle$ and a general state ρ reads

$$F(|\psi\rangle,\rho) = \mathrm{Tr}\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|} = \sqrt{\langle\psi|\rho|\psi\rangle}. \tag{A.2}$$

  Hence, the fidelity equals the square root of the overlap between $|\psi\rangle$ and ρ. This is an important result and reason why this measure is often used. For simplicity, the square root is usually omitted

- Fidelity is invariant under unitary transformations

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho,\sigma). \tag{A.3}$$

- A very useful theorem was proved by Uhlmann [112]

  Theorem A.0.2 *Let ρ and σ are states of a quantum system H. Introduce a second quantum system G which is a copy of H. Then*

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle, \tag{A.4}$$

  where the maximization is taken over all purification $|\psi\rangle$ of ρ and $|\phi\rangle$ of σ into HG.

- Using this theorem we can prove the monotonicity of the fidelity.

  Theorem A.0.3 *Any trace-preserving quantum operation* $\mathcal{E} : \mathsf{L}(\mathscr{H}_A) \to \mathsf{L}(\mathscr{H}_B)$ *(A and B denote an input and an output quantum system) cannot decrease the fidelity between density operators* ρ *and* σ *from the set of states* $\mathsf{S}(\mathscr{H}_A)$

  $$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq F(\rho, \sigma). \tag{A.5}$$

  Proof: The proof of the theorem A.0.3 can be done in the following way. Any trace-preserving operation has its own unitary dilation (see theorem 1.2.3) and therefore $\mathcal{E}$ can be written in the form

  $$\mathcal{E}(\rho) = \mathrm{Tr}_L \left[U(\rho \otimes |\phi_R\rangle\langle\phi_R|)U^\dagger \right], \tag{A.6}$$

  where L denotes a measurement ancillary system, R a preparation ancillary system, $|\phi_R\rangle \in \mathsf{S}(\mathscr{H}_R)$. Let $|\psi\rangle$ and $|\phi\rangle$ be purifications of ρ and σ into a joint system AG such that $F(\rho, \sigma) = |\langle\psi|\phi\rangle|$. It means that $\rho = \mathrm{Tr}_G |\psi\rangle\langle\psi|$ and $\sigma = \mathrm{Tr}_G |\phi\rangle\langle\phi|$. Then because the partial transpose commutes with the operation $U \otimes I_G$, it is simple to check that

  $$\mathcal{E}(\rho) = \mathrm{Tr}_{L+G} \left[U \otimes I_G(|\psi\rangle\langle\psi| \otimes |\phi_R\rangle\langle\phi_R|)U^\dagger \otimes I_G \right], \tag{A.7}$$

  where I_G is the identity operator on the purification system G. A similar equation we get for $\mathcal{E}(\sigma)$. Hence $U \otimes I_G|\psi\rangle|\phi_R\rangle$ is a purification of $\mathcal{E}(\rho)$ and $U \otimes I_G|\phi\rangle|\phi_R\rangle$ is a purification of $\mathcal{E}(\sigma)$. Using Uhlmann's theorem (A.0.2) we receive finally monotonicity of the fidelity

  $$F(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq |\langle\psi|\langle\phi_R|UU^\dagger \otimes I_G|\phi\rangle|\phi_R\rangle| = F(\rho, \sigma). \tag{A.8}$$

  ■

- The fidelity satisfies strong concavity.

  Theorem A.0.4 *Let* p_i *and* q_i *are probability distributions over the same index set,* ρ_i *and* σ_i *density operators also indexed over the same set. Then*

  $$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i \right) \geq \sum_i \sqrt{p_i q_i} F\rho_i, \sigma_i. \tag{A.9}$$

Appendix B

Group theory

This section briefly summarizes group-theoretical techniques used in the thesis. For more details see [113].

B.1 Elements of group theory

A group is a set of elements $\mathbf{G}$ equipped with an multiplication operation $gk \in \mathbf{G}$ on pair of elements : $\mathbf{G} \times \mathbf{G} \to \mathbf{G}$ obeying the following rules

i) $(gh)k = g(hk)$ for all g,h,$k \in \mathbf{G}$ (associativity)

ii) $\exists e \in \mathbf{G}$ such that $ge = eg = e$ for all $g \in \mathbf{G}$ (existence of identity)

iii) $(\forall g \in \mathbf{G})(\exists g^{-1} \in \mathbf{G})$ such that $gg^{-1} = g^{-1}g = e$ (existence of an inverse)

A subgroup $\mathbf{H}$ of the group $\mathbf{G}$ is a subset of $\mathbf{G}$ containing the unit element e closed with respect to multiplication and the inverse operation.

A topological group is a group equipped with a Hausdorff topology such that the maps

$$\begin{aligned} \mathbf{G} \times \mathbf{G} &\to \mathbf{G} : & (g,h) &\to gh \\ \mathbf{G} &\to \mathbf{G} : & g &\to g^{-1} \end{aligned} \tag{B.1}$$

are continuous. A compact group is a topological group with a compact topological space.
In the center of our interest lie the so-called operator groups. Let us introduce three types of unitary groups:

i) The unitary group $\mathsf{U}(\mathscr{H})$ is the set of all unitary operators acting on Hilbert space $\mathscr{H}$

$$\mathsf{U}(\mathscr{H}) = \left\{ U \in \mathsf{L}(\mathscr{H}) | UU^\dagger = U^\dagger U = I_{\mathscr{H}} \right\}, \tag{B.2}$$

where $U^\dagger$ denotes the conjugate operator to the operator U.

ii) The unitary group of degree N $\mathsf{U}(N)$ is a set of all matrices $\mathbb{C}^{n,n}$ which are unitary

$$\mathsf{U}(N) = \left\{ U \in \mathbb{C}^{n,n} | UU^\dagger = U^\dagger U = I \right\}, \tag{B.3}$$

where $U^\dagger$ denotes the conjugate matrix to the matrix U.

iii) The special unitary group of degree N $\mathsf{SU}(N)$ is the subgroup of all unitary matrices $\mathsf{U}(N)$ with unit determinant

$$\mathsf{SU}(N) = \left\{ U \in \mathbb{C}^{n,n} | UU^\dagger = U^\dagger U = I \ \wedge \ \mathrm{Det}(U) = 1 \right\}, \tag{B.4}$$

where $U^\dagger$ denotes the conjugate matrix to the matrix U.

The symbol $I_{\mathscr{H}}$ (resp. I) denotes the identity operator acting on Hilbert space $\mathscr{H}$ (resp. the identity matrix of dimension n). The unitary group $\mathsf{U}(\mathscr{H})$ is compact and therefore all its subgroups are compact.

B.2 Unitary representation of a group

A unitary (projective) representation on $\mathscr{H}$ of the group $\mathbf{G}$ is a homomorphism $g \in \mathbf{G} \mapsto U_g \in \mathsf{U}(\mathscr{H})$, with U_g unitary operator, such that the composition law is preserved:

$$U_g U_h = \omega(g,h) U_{gh}. \tag{B.5}$$

The cocycle $\omega(g,h)$ is a phase, i. e. $|\omega(g,h)| = 1$, for all $g, h \in \mathbf{G}$, and it satisfies the relations

$$\begin{aligned} &\omega(gh,k)\omega(g,h) = \omega(g,hk)\omega(h,k) \\ &\omega(g,g^{-1}) = 1. \end{aligned} \tag{B.6}$$

Consider an arbitrary subgroup $\mathbf{U}_g$ of the unitary group $\mathsf{U}(\mathscr{H})$. A simple case of a unitary representation on $\mathscr{H}$ of the group $\mathbf{U}_g$ is the identity map, which assigns to an arbitrary element $U \in \mathbf{U}_g$ the operator U.

Two representations U^1 and U^2 of $\mathbf{G}$ on $\mathscr{H}_1$ and $\mathscr{H}_2$, respectively, are called *equivalent* if there exists a unitary map $T : \mathscr{H}_1 \to \mathscr{H}_2$ such that $TU^1_g = U^2_g T$, for all $g \in \mathbf{G}$. A unitary representation is called *irreducible* (UIR) if there are no proper subspaces of $\mathscr{H}$ left invariant to the action of all its elements.

B.3 Haar measure

A Haar measure on a group $\mathbf{G}$ is a left-invariant measure $\mu : \Sigma \to [0, +\infty)$, with Σ being a σ-algebra containing all Borel subsets of $\mathbf{G}$, such that

i) $\mu(\mathbf{G}) = 1$,

ii) $\mu(gS) = \mu(S)$ for all $g \in \mathbf{G}$, $S \in \Sigma$, where gS is defined as $gS = \{gs | s \in S\}$.

The first property is our requirement of normalization (probability measure), the second property reflects our requirement of left-invariance.

Using the general theory of Lebesgue integration, one can define an integral (a bounded linear functional E) for all Borel measurable functions $f \in L^1(\mathbf{G}, \Sigma, \mu)$ on $\mathbf{G}$

$$E(f) = \int_G f(g) d\mu(g) = \int_G f(g) dg. \tag{B.7}$$

This integral is called the Haar integral. Because the Haar integral is generated by the left-invariant Haar measure, the following equation is fulfilled

$$\int_G f(sg) dg = \int_G f(g) dg \qquad \text{for } \forall s \in \mathbf{G}. \tag{B.8}$$

A next important theorem says that this construction based on a Haar measure is possible for all compact groups [114].

Theorem B.3.1 *Let* $\mathbf{G}$ *be a compact group. There is a* σ*-algebra, let say* Σ*, of subsets of* $\mathbf{G}$ *that contains all Borel subsets of* $\mathbf{G}$ *and is invariant under left and right multiplication and under inversion, i.e.*

$$\begin{aligned} S \in \Sigma, g \in \mathbf{G} \Longrightarrow \quad & gS = \{gs | s \in S\} \in \Sigma \\ & Sg = \{sg | s \in S\} \in \Sigma \\ & S^{-1} = \{s^{-1} | s \in S\} \in \Sigma \end{aligned} \tag{B.9}$$

and there is a measure $\mu : \Sigma \to [0, +\infty)$ *such that*

$$\begin{aligned} & \mu(gS) = \mu(Sg) = \mu(S^{-1}) = \mu(S) \qquad \text{for } \forall S \in \Sigma, \\ & \mu(\mathbf{G}) = 1. \end{aligned} \tag{B.10}$$

Appendix C

Irreducible tensor operators

In this appendix basic properties of irreducible tensor operators of the group SU(2) are summarized. These irreducible tensor operators are convenient tools for implementing the covariance conditions (4.10) and (4.47).

Rotation properties of quantum states described by the continuous group O(3) or its universal covering group SU(2) are conveniently analyzed by representing the density operator of this quantum state in irreducible tensor components. In terms of orthonormal angular momentum eigenstates $|Jm\rangle$ (with $-2J, -2J+1, ... \leq m \leq ..., 2J-1, 2J$ and J being half integer or integer) a set of irreducible tensor operators $T(J_1 J_2)_{KQ}$ (with $|J_1 - J_2| \leq K \leq J_1 + J_2$ and $-K, -K+1, ... \leq q \leq ..., K-1, K$) is defined by [94, 95]

$$T(J_1, J_2)_{Kq} = \sum_{m_1 m_2} (-1)^{J_1 - m_1} \sqrt{2K+1} \times \begin{pmatrix} J_1 & J_2 & K \\ m_1 & -m_2 & -q \end{pmatrix} |J_1 m_1\rangle \otimes \langle J_2 m_2|. \tag{C.1}$$

The irreducible tensor components are special cases of complete orthogonal sets of operators T_{LM} with simple transformation properties under a given group. For the irreducible tensor operators defined by (C.1) these key properties read

- *Orthogonality*

$$\mathrm{Tr}[T(J_1, J_1')_{KQ} T(J_2, J_2')^{\dagger}_{K'Q'}] = \delta_{J_1 J_2} \delta_{J_1' J_2'} \delta_{KK'} \delta_{QQ'}. \tag{C.2}$$

- *Completness*

  Consider Hilbert space with base of momentum states $|JM\rangle$. Every operator A acting on

this Hilbert space can be written in terms of irreducible tensor components

$$A = \sum_{J'JKQ} \left\langle T(J'J)^{\dagger}_{KQ} \right\rangle T(J'J)_{KQ}, \tag{C.3}$$

where

$$\left\langle T(J'J)^{\dagger}_{KQ} \right\rangle = \mathrm{Tr}\left\{ AT(J'J)^{\dagger}_{KQ} \right\}. \tag{C.4}$$

- *Transformation under rotations*

  Let U be an unitary operator representing arbitrary rotation of Hilbert space. Then tensor components are transformed according to

$$UT(J_1J_2)_{KQ}U^{\dagger} = \sum_{q} T(J_1J_2)_{Kq} D(U)^{(K)}_{qQ}, \tag{C.5}$$

  with $D(U)^{(K)}_{qQ}$ denoting rotation matrix elements [94]. These latter matrix elements fulfill the orthogonality relation

$$\int D(\gamma\beta\alpha)^{(j)*}_{mm'} D(\gamma\beta\alpha)^{(J)}_{MM'} \sin\beta \; d\beta d\alpha d\gamma = \frac{8\pi^2}{2J+1} \delta_{jJ}\delta_{mM}\delta_{m'M'}. \tag{C.6}$$

  Thereby, α, β, and γ denote the Euler angles characterizing a particular rotation. According to (C.5) the quantum numbers J_1, J_2, and K characterize a particular irreducible representation of the rotation group.

From the definition (C.1) and its properties follow the relations

$$\begin{aligned} \left\langle T(J,J')^{\dagger}_{KQ} \right\rangle > &= \sum_{MM`} (-1)^{J-M} \sqrt{2K+1} \begin{pmatrix} J & J' & K \\ M & -M' & -Q \end{pmatrix} \langle JM|\rho_{\mathrm{in}}|J'M'\rangle, \\ |JM\rangle\langle J'M'| &= \sum_{KQ} (-1)^{J-M} \sqrt{2K+1} \begin{pmatrix} J & J' & K \\ M & -M' & -Q \end{pmatrix} T(J,J')_{KQ}. \end{aligned} \tag{C.7}$$

For details consult e.g. ([94]), Some useful relations are summarized here:

$$
\begin{aligned}
&\mathrm{Tr}[T(J,J')_{KQ}] = \delta_{JJ'}\delta_{K0}\delta_{Q0}\sqrt{2J+1},\\
&T(J,J')^{\dagger}_{KQ} = (-1)^{J-J'+Q}\; T(J',J)_{K-Q},\\
&\mathrm{Tr}[T(J,J')_{KQ}T(J,J')^{\dagger}_{K'Q'}] = \delta_{KK'}\delta_{QQ'},\\
&\langle JM|\rho|J'M'\rangle = \sum_{KQ}(-1)^{J-M}\sqrt{2K+1}\begin{pmatrix} J & J' & K\\ M & -M' & -Q\end{pmatrix} < T(J,J')^{\dagger}_{KQ} >,\\
&|(jj')JM\rangle = \sum_{mm'}|jm\rangle|j'm'\rangle\sqrt{2J+1}(-1)^{j-j'-M}\begin{pmatrix} j & j' & J\\ m & m' & -M\end{pmatrix},\\
&|jm\rangle|j'm'\rangle = \sum_{JM}\sqrt{2J+1}(-1)^{-j+j'+M}\begin{pmatrix} j & j' & J\\ m & m' & -M\end{pmatrix}|(jj')JM\rangle.
\end{aligned}
$$

As the tensor operators of (C.1) form a complete set any operator including the density operator ρ can be decomposed according to

$$\rho = \sum_{J_1J_2Kq}\mathrm{Tr}\left\{T(J_1J_2)^{\dagger}_{Kq}\;\rho\right\}T(J_1J_2)_{Kq}. \tag{C.8}$$

In the special case of two qubits with angular momenta $J=\frac{1}{2}$, for example, in such a decomposition the irreducible tensor operators $T(\frac{1}{2},\frac{1}{2})_{Kq}$ (with $K\in\{0,1\}$ and $-K\leq q\leq K$) appear for each qubit. Their explicit form is given by (4.49). Obviously, the set of tensor products of irreducible tensor operators is also a complete set of operators on the two-qubit Hilbert space and we can express an arbitrary two-qubit density operator in the form of (4.48). With the help of the relation (C.6), finally, it is straightforward to prove that the most general form of an output state fulfilling the covariance condition (4.10) (resp. (4.47)) is given by (4.15) (resp. (4.51)).

Bibliography

[1] J. C. Maxwell, *Theory of Heat* (Longmans, Green, and Co., London, 1871), Ch. 12.

[2] R. Landauer, IBM J. Res. Dev. **5**, 183 (1961).

[3] C. H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).

[4] W. K. Wooters and W. H. Zurek, Nature (London) 299, 802 (1982).

[5] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, R2629 (1999).

[6] Arun K. Pati, Phys. Rev. A **66**, 062319 (2002).

[7] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[8] E. Schrödinger, Naturwissenshaften **23**, 807, 823, and 844 (1935).

[9] J. S. Bell, Physics, **1**, 195-200 (1964).

[10] S. J Friedmann and J. F. Clauser, Phys. Rev. Lett **28**, 938 (1972).

[11] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).

[12] G. Weighs, T. Jennewein, Ch. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

[13] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895, (1993).

[14] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wooters, Phys. Rev. Lett. **70**, 661 (1991).

[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, Phys. Rev. A **54**, 3824 (1996).

[16] D. Deutsch, A. Ekert, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[17] N. Gisin, Phys. Lett. A **210**, 151 (1996).

[18] K Kraus, in *Foundations of Quantum Mechanics and Ordered Linear Spaces*, Vol. 29 of *Lecture Notes in Physics*, 206 (Springer-Verlag, 1973).

[19] M-D Choi, Lin. Alg. Appl. **10**, 285 (1975).

[20] F. Buscemi, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **68**, 042113 (2003).

[21] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[22] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).

[23] D. Salgado, J. L. Sanchez-Gomez, and M. Ferrero, math-ph/0406010.

[24] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. Smolin, and W. K. Wooters, Phys. Rev. A **59**, 1070 (1999).

[25] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[26] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).

[27] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York), 175-179 (1984).

[28] C. H. Bennett, Phys. Rev. Lett., **68**, 3121 (1992).

[29] A. K. Ekert, Phys. Rev. Lett., **67**, 661 (1991).

[30] N. Herbert, Found. Phys. **12**, 1171 (1982).

[31] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996); V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).

[32] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[33] C.-S. Niu and R. B. Griffiths, Phys. Rev. A58, 4377 (1998).

[34] R. Werner, Phys. Rev. A **58**, 1827 (1998).

[35] N. J. Cerf, Phys. Rev. Lett. 84, 4497 (2000).

[36] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000);

N. J. Cerf and S. Iblisdir, Phys. Rev A **62**, 040301 (2000);

S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, Phys. Rev. Lett. **86**, 4438 (2001);

N. J. Cerf and S. Iblisdur, Phys. Rev. Lett. **87**, 247903 (2001).

[37] S. L. Braunstein, V. Bužek, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).

[38] J. Fiurášek, S. Iblisdir, S. Massar, and N. J. Cerf, Phys. Rev. A **65**, 040302(R) (2002).

[39] L.-P. Lamoureux, P. Navez, J. Fiurášek, and N. J. Cerf, Phys. Rev. A **69**, 040301-1 (2004).

[40] P. Rungta, V. Bužek, C.M.Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315-1-13 (2001).

[41] F. Buscemi, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Lett. A **314**, 374 (2003).

[42] F. Sciarrino, C. Sias, M. Ricci, and F. De Martini, Phys. Rev. A **70**, 052305 (2004).

[43] F. Hansen, J. Pečarič, and I. Perič, math.OA/0606590 (2006).

[44] E. Schmidt, Math. Annalen **63**, 433 (1906).

[45] A. Ekert and P. L. Knight, Am. J. Phys. **63**, 415 (1995).

[46] R. E. Edwards, *Functional analysys, Theory and Application*, Holt, Rinehart and Winston, New York, (1965).

[47] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[48] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[49] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[50] M. Horodecki, and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[51] F. Buscemi, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **92**, 070403 (2004).

[52] P. R. Halmos, *A Hilbert Space Problem Book* (Springer-Verlag, 1982).

[53] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[54] M. A. Nielsen and J. Kempe, Phys. Rev. Lett., **86**, 5184-7 (2001).

[55] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[56] M. J. Donald, M. Horodecki, and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).

[57] O. Rudolph, J. Math. Phys. **42**, 2507 (2001).

[58] A. Uhlmann, Phys. Rev. A **62**, 032307 (2000).

[59] C. Bennett, H. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[60] K. Audenaert, F. Verstraete, and B. De Moor, Phys. Rev. A **64**, 052304 (2001).

[61] K. G. H. Vollbrecht and R. F. Werner, Phys. rev. A **64**, 062307 (2001).

[62] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens, Phys. Rev. Lett. **84**, 1611 (2000).

[63] B. Terhal and K. G. H. Vollbrecht, Phys. Rev. Lett. **85**, 2625 (2000).

[64] S. Hill, W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[65] W. K. Wooters, Phys. Rev. Lett. **80**, 2245 (1998).

[66] W. K. Wootters, Quant. Inf. Comp. **1**, 27 (2001).

[67] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **92**, 167902 (2004).

[68] S. J. Akhtarshenas, J. Phys. A Math. Gen. **38**, 6777 (2005).

[69] G. Vidal and R. F. Werner, Phys. Rev. A **65**, 032314 (2002).

[70] V. Vedral and M. Plenio, Phys. Rev. A **57**(3), 1619 (1998).

[71] G. Vidal and R. Tarrach, Phys. Rev. A **59**(1), 141 (1999).

[72] M. Christandl and A. Winter, J. Math. Phys. **45**(3), 829 (2004).

[73] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[74] A. Wong and N. Christensen, Phys. Rev. A **63**, 044301 (2001).

[75] Chang-shui Yu and He-shan Song, Phys. Rev. A **71**, 042331 (2005).

[76] F. Mintert, M. Kuś, and A. Buchleitner, Phys. Rev. Lett. **95**, 260502 (2005).

[77] Chang-shui Yu and He-shan Song, Phys. Rev. A **73**, 022325 (2006).

[78] T. J. Osborne and F. Verstraete, `quant-ph/0502176` (2006).

[79] W. K. Wootters, Contemporary Mathematics **305**, 299 (2002).

[80] K. M. O'Connor and W. K. Wootters, Phys. Rev. A **63**, 052302 (2001).

[81] M. Koashi, V. Bužek, and N. Imoto, Phys. Rev. A **62**, 050302 (2000).

[82] W. Dür, Phys. Rev. A **63**, 020303(R) (2001).

[83] M. Plesch and V. Bužek, Phys. Rev. A **67**, 012322 (2003).

[84] M. Plesch, J. Novotný, Z. Dzuráková, and V. Bužek, J. Phys.A **37**, 1843 (2004).

[85] P. Törma and I. Jex, J. Mod. Optics **44**, 875 (1997).

[86] P. Törma and I. Jex, J. Opt. B **1**, 8 (1999).

[87] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[88] P. Dita, J. Phys. A **37**, 5355 (2004).

[89] A. Vourdas and J. A. Dunningham, Phys. Rev. A **71**, 013809, (2005).

[90] Z. Ou, C. K. Hong, and L. Mandel, Optics Commun. **63**, 118 (1987).

[91] P. Törma, Phys. Rev. Lett. **81**, 2185 (1998).

[92] M. Toda, R. Kubo, and N. Saito, *Statistical physics I*, second edition, Springer, Berlin (1995).

[93] J. Kempe, Contemporary Physics, Vol. 44 (4) (2003).

[94] K. Blum, *Density Matrix Theory and Applications* (Plenum Press, New York, 1981).

[95] L. C. Biedenharn and J. D. Louck, *Angular Momentum in Quantum Physics* (Addison-Wesley Publishing Company, Massachusetts, 1981).

[96] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory*, Lecture Notes in Physics **190** (Springer, Berlin, 1983).

[97] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Pub., Dordrecht, 1995).

[98] R. Demkowicz-Dobrzański, M. Lewenstein, A. Sen(De), U. Sen, and D. Brus, Phys. Rev. A **73**, 032313 (2006).

[99] J. Schlienz and G. Mahler, Phys. Rev. A **52**, 4396 (1995).

[100] A. K. Pati, Phys. Rev. A **63**, 014302 (2001).

[101] H.-K. Lo, Phys. Rev. A **62**, 012313 (2000).

[102] Ch. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. Smolin, B. M. Terhal, and W. K. Wootters, Phys. Rev. Lett. **87** 077902 (2001).

[103] I. Devetak and T. Berger, Phys. Rev. Lett. **87**, 077906 (2001).

[104] B. Zeng and P. Zhang, Phys. Rev. **65**, 022316 (2002).

[105] D. W. Berry and B. C. Sanders, Phys. Rev. Lett. **90**, 057901 (2003).

[106] X. Peng, X. Zhu, X. Fang, M. Feng, M. Liu, and K. Gao, Phys. Lett. A **306**, 271 (2003).

[107] N. A. Peters, J. T. Barreiro, M. E. Goggin, T-Ch. Wei, and P. G. Kwiat, Phys. Rev. Lett. **94**, 150502 (2005).

[108] P. Kok, K. Nemoto, and W. J. Munro, qunt-ph/0201138.

[109] J. Novotný, G. Alber, and I. Jex, submitted to Phys. Rev. (2007).

[110] A. Barenco, Ch. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[111] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge UP, Cambridge, 2000).

[112] A. Uhlmann, Rep. Math. Phys., **9**, 273 (1976).

[113] A. O. Barut and R. Raczka, *Theory of Group Representation and Applications* (Warsaw: Polish Scientific Publishers, 1977).

[114] D. P. Zhelobenko, *Compact Lie Groups and Their Representations* (American Mathematical Society, 1973).

List of publications

- Martin Plesch, Jaroslav Novotný, Zuzana Dzuráková, Vladimír Bužek: *Controlling bipartite entanglement in multi qubit systems*, J. Phys.A **37**, 1843-1859 (2004).
- Jaroslav Novotný, Martin Štefaňák, Tamas Kiss, Igor Jex: *Control of entanglement in Ising-type networks with one and two excitations*, J. Phys. A **38**, 9087-9103 (2005).
- Jaroslav Novotný, Gernot Alber, Igor Jex: *Optimal copying of entangled two-qubit states*, Phys. Rev A **71**, 042332 (2005).
- Jaroslav Novotný, Gernot Alber, Igor Jex: *Completely positive covariant two-qubit quantum processes and optimal quantum NOT operations for entangled qubit pairs*, Phys. Rev A **73**, 062311 (2006).
- Jaroslav Novotný, Gernot Alber, Igor Jex: *Network implementation of covariant two-qubit quantum operations*, Phys. Rev. A **75**, 042309 (2007).

Czech summary

Disertační práce je věnována studiu sdílení kvantového provázání, jeho generace v pasivních sítích a jeho úloha v kvantově-informačních procesech: kopírování a NOT operace. Provázání lze charakterizovat jako neklasickou korelaci odpovědnou za nelokální povahu některých kvantových stavů. Jeho sdílení v mnohačásticových kvantových systémech však není libovolné ale podléhá určitým v současné době ne zcela známým pravidlům. Neznáme tedy úplnou odpověď na otázku, které struktury provázání odpovídají fyzikálním stavům. V této práci bylo k popisu sdílení dvoučásticového provázání v kvantových více-q-bitových stavech použito váhovaných grafů, kdy vrcholům odpovídají jednotlivé q-bity a hrany mezi vrcholy jsou ohodnoceny silou provázání (měřeno mírou zvaná concurrence) mezi q-bity odpovídající těmto vrcholům. Každému kvantovému stavu N q-bitů lze tedy jednoznačně připsat váhovaný graf. Řešení opačného problému, zda-li daný váhovaný graf odpovídá nějakému kvantovému stavu, je podstatně složitější. V této práci byla nalezena široká třída váhovaných grafů, pro které existují více-q-bitové stavy se strukturou provázání předepsanou grafy z této třídy. Důkaz existence těchto stavů je konstrukční a obsahuje iterační postup, jak hledaný kvantový stav k danému grafu z této množiny zkonstruovat.

Práce se dále věnuje možnosti generace provázaných stavů v pasivních sítích. Byly nalezeny vztahy pro "concurrence" vstupních stavů s jednou a dvěma excitacemi v libovolné pasivní síti. Byla analyzována obecná struktura provázání pro vstupní stavy s jednou excitací a navržena síť, která předepsanou strukturu provázání realizuje. Rovněž bylo analyzováno, jak silně provázané stavy lze v pasivních sítích s jednou a dvěma excitacemi vyrábět. Získané výsledky byli porovnány s výsledky numerických simulací Isingovských sítí. Simulace ukázaly, že v limitě neomezené Isingovské optické sítě se hodnoty celkového bipartitního provázání mezi jednotlivými mody sítě přibližují teoreticky odvozeným maximálním hodnotám.

Dalším studovaným problémem je kopírování entanglovaných stavů. Bylo analyzováno klonovací zařízení, jehož vstupem jsou dva q-bity a jež má produkovat dvě co nejlepší kopie těchto dvou vstupních q-bitů. Předpokládá se, že vstupní q-bity jsou v čistém stavu s předem daným stupněm provázání. Vyvstává základní otázka, jak síla provázání vstupních stavů ovlivňuje optimální kvalitu kopií. V rámci řešení tohoto problému byla studována speciální třída kovariantních kvantových operací. Byly nalezeny optimální klonovací transformace pro každou třídu dvou q-bitových čistých stavů s daným stupněm provázání a pro dvě různé míry kvality kopií.

Byla studována optimální NOT operace pro entanglované q-bity. Předpokládalo se, že dva vstupní q-bity jsou v čistém stavu a s předem daným stupněm provázání a je hledána kvantová operace, jejímž výstupem je stav z ortogonálního doplňku vstupních stavů nebo stav tomuto ortogonálnímu doplňku blízký. Bylo dokázáno, že pro maximálně provázané stavy existují nekovariantní ideální NOT operace. Byla nalezena úplná struktura těchto operací a navržen protokol pro vzdálenou přípravu maximálně provázaných stavů. Dále byla nalezena obecná konvexní struktura všech úplně positivních kvantových operací, transformující vstupní dvou-q-bitové stavy na dvou-q-bitové výstupní stavy kovariantním způsobem. V rámci této třídy kvantových procesů byly určeny kovariantní optimální NOT operace pro všechny třídy dvou-q-bitových stavů s daným stupněm provázání. Byla navržena posloupnost podmíněných kvantových bran, realizující pomocí nastavení pomocné ancily celou třídu kovariantních procesů.