Dissertation

submitted to the

Combined Faculties of the Natural Sciences and Mathematics

of the Ruperto-Carola-University of Heidelberg, Germany

for the degree of

Doctor of Natural Sciences

Put forward by

Michael Siomau

born in: Postavi, Belarus

Oral examination: 6^{th} July, 2011

Entanglement and optimal quantum information processing

Referees: Priv-Doz. Dr. Stephan Fritzsche

Priv-Doz. Dr. Jörg Evers

Zusammenfassung

Heute stehen wir am Anfang einer neuen Ära der Informationsverarbeitung, in der Quantentechnologien immer bedeutsamer werden. Ungeachtet bedeutender Fortschritte bei der experimentellen Erzeugung und Manipulation sowie der theoretischen Beschreibung von einfachen Quantensystemen, in den letzten drei Jahrzehnten, gibt es noch viele ungelöste Probleme im Verständnis des Verhaltens und der Eigenschaften von komplexen Vielteilchenquantensystemen. In dieser Dissertation wird eine theoretische Untersuchung einer Reihe von Problemen im Zusammenhang mit der Verschränkung — dem nichtlokalen Merkmal von komplexen Quantensystemen — in Vielteilchenzuständen endlichdimensionaler Quantensysteme durchgeführt. Wir betrachten zu-sätzlich optimale Möglichkeiten zur Manipulation solcher Systeme. Der Schwerpunkt der Arbeit liegt insbesondere auf optimalen Quantentransformationen die eine gewünschte Operation unabhängig von den Anfangszuständen des Systems erlauben. Der erste Teil dieser Arbeit widmet sich dabei einer detaillierten Analyse, wie sich die Verschränkung in Qubit-Systemen unter Einwirkung einer nichtunitären Dynamik (zeitlich) entwickelt. Im zweiten Teil der Arbeit konstruieren wir mehrere optimale zustandsunabhängige Transformationen, untersuchen ihre Eigenschaften und schlagen Anwendungen in der Quantenkommunikation und im Quantencomputing vor.

Abstract

Today we are standing on the verge of new enigmatic era of quantum technologies. In spite of the significant progress that has been achieved over the last three decades in experimental generation and manipulation as well as in theoretical description of evolution of single quantum systems, there are many open problems in understanding the behavior and properties of complex multiparticle quantum systems. In this thesis, we investigate theoretically a number of problems related to the description of entanglement — the nonlocal feature of complex quantum systems — of multiparticle states of finite-dimensional quantum systems. We also consider the optimal ways of manipulation of such systems. The focus is made, especially, on such optimal quantum transformations that provide a desired operation independently on the initial state of the given system. The first part of this thesis, in particular, is devoted to the detailed analysis of evolution of entanglement of complex quantum systems subjected to general non-unitary dynamics. In the second part of the thesis we construct several optimal state independent transformations, analyze their properties and suggest their applications in quantum communication and quantum computing.

During my PhD training the following papers were published:

- M. Siomau and S. Fritzsche, *Quantum computing with mixed states*, (accepted in European Physical Journal D).
- M. Siomau and S. Fritzsche, *Evolution equation for entanglement of multiqubit systems*, Physical Review A **82**, 062327 (2010).
- M. Siomau and S. Fritzsche, *Universal quantum Controlled-NOT gate*, European Physical Journal D **60**, 417 (2010).
- M. Siomau and S. Fritzsche, *Entanglement dynamics of three-qubit states in noisy channels*, European Physical Journal D **60**, 397 (2010).
- M. Siomau and S. Fritzsche, *High-fidelity copies from a symmetric* $1 \rightarrow 2$ *quantum cloning machine*, European Physical Journal D **57**, 293 (2010).
- M. Siomau and S. Fritzsche, *Efficiency of the eavesdropping in B92 QKD protocol with a QCM*, in *Proceeding of QuantComm 2009*, edited by A. Sergienko (LNICST **36**, 2010), p. 267.

Acknowledgements

I would like to take opportunity and thank those people who contributed to this work, helped and supported me during my study. First and foremost I want to thank my supervisor Stephan Fritzsche who gave me a job and guided me through my projects. Secondly, I wish to thank my co-advisors: Andrey Surzhykov for hospitality in his theory group and many discussions about science and far beyond and Jörg Evers for his genuine interest in my research projects. Thirdly, it is my great pleasure to thank my scientific collaborators and friends: Filippo Fratini, Anton Artemyev, Sean McConnell, Thorsten Jahrsetz, Lalita Sharma and Armen Hayrapetyan. It is hard to mention all the support I received from my colleagues. All these people created nice working atmosphere without which this work would not be possible.

I am grateful to Stephen M. Barnett, Andreas Osterloh and Markus Oberthaler for random scientific discussions which often became sources of scientific inspiration for me.

Also, I thank my friends Baybars Külebi, Ralph Matucci, Hector Cortes, Mari Chikvaidze for many enjoyable hours spend together and for their support when it was required. Due to these people my stay in HD, especially out of the office, was really enjoyable.

Additionally, I would like to thank Sandra Klevansky, the administrative director of Heidelberg Graduate School for Fundamental Physics, for her important support during a difficult period of my study. Without exaggeration I can say that without her help this work would never be finished.

Last, but not least, I wish to thank my parents, Mikalai and Sviatlana Siomau, for giving me birth and first life lessons that brought me to this day. Finally, I wish to thank my girlfriend, Natallia, for the essential role that she played and is still playing in my life.

April 2011, Heidelberg

Contents

Introduction

We may hope that machines will eventually compete with men in all purely intellectual fields.

Alan M. Turing

The fundamental problem of communication is that of reproducing at one point either exactly of approximately a message selected at another point.

Claude E. Shannon

The concept of information is shaping our world from everyday communication to sophisticated high technological devices, such as space satellites and supercomputers. The investigation of the basic laws of information processing attracted attention of many scientists in the past. The modern incarnation of information science was announced by two great mathematicians of the last century: Alan Turing and Claude Shannon. Turing developed in details an abstract notion of what we would now call a programmable computer [1]. Approximately at the same time, Shannon mathematically defined the concept of information which became the foundation for the modern theory of communication [2].

Not long after Turing's paper, the first computers constructed from electronic components were developed. Since then computer hardware has grown in power and minimized in size at an amazing pace. However, most observers expect that this run will end some time during the first two-three decades of the 21^{st} century. Conventional approaches to the fabrication of computers are beginning to suffer from fundamental difficulties of size: quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller. A possible way to overcome this difficulties is to move to a different computing paradigm. One such paradigm is provided by the theory of quantum computation which is based on the idea of using quantum mechanics to perform computations, instead of classical physics [3].

What do we expect from a quantum computer? While a classical computer can be used to simulate a quantum computer, it appears to be impossible to perform the simulation in an efficient fashion [3]. This implies that quantum computers offer an essential speed advantage over classical computers [4]. David Deutsch showed the first example, a black-box problem that requires two queries to solve on a classical

computer but that can be solved with single quantum query [5]. A series of related results [6, 7] gave increasingly dramatic separation between classical and quantum query complexities, culminating in the example from Simon [8] providing an exponential separation. Based on these works, Shor discovered that a quantum computer could efficiently factor integers and calculate discrete logarithms [9]. An algorithm achieving quadratic speed-up over the best possible classical algorithm for the unstructured search problem was suggested by Grover [10]. Concept of the quantum walk, developed by analogy to the classical random walk, has proven to be another useful tool for quantum algorithms [11, 12]. Finally, the performance of game strategies based on quantum principles superior the efficiencies of classical strategies [13].

What is the essential quantum effect that gives rise to increase in the computational power of a quantum computer? Although this question has not been answered so far on a fundamental level [14, 15], there are many evidences that certain correlated superpositions of multiparticle states, so-called entangled states, play the key role [16, 17, 18]. Several proposals for architecture of quantum computer based on using entangled states have been already suggested, such as linear optical quantum computing [19, 20], teleportation-based [21] and one-way quantum computing [22, 23]. Although all basic steps required for the realization of the mentioned schemes have been already experimentally demonstrated [24, 25, 26], it is still unclear whether it will be ever possible to run a quantum computer that exceeds the performance of a modern classical one.

In contrast to computation theory, there was no technological necessity to use quantum systems in communication. This situation dramatically changed with the discovery of the no-cloning principle [27, 28]. The direct consequence of this principle is unconditional security of communication with quantum systems [29, 30] – the most desirable goal of communication theory. Security of classical communication is conditional and is based on computational complexity of an encoding protocol. Under condition that the third (eavesdropping) person has limited computational resources, classical communication is secure. However, this is not longer true, if the eavesdropper possesses a classical supercomputer or a quantum computer. Quantum communication is secure independently on the eavesdropper's resources.

Up to now, a large number of quantum communication protocols have been suggested. In some of these protocols the information is encoded in superposition states of single quantum systems, for example, the BB84 [31], the B92 [32] and the six-state protocol [33]. Some (so-called teleportation-based) protocols, are based on utilizing entangled states of multiparticle systems [34, 35]. Many of the protocols for quantum communication have been experimentally tested. The longest distance over which quantum communication has been demonstrated using optic fibre is 148.7 km. This was achieved by Los Alamos National Laboratory using the BB84 protocol [36]. The highest bit rate system currently demonstrated exchanges quantum information at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre), achieved by a collaboration between the University of Cambridge and Toshiba using the BB84 protocol with decoy pulses [37]. There are currently four companies offering commercial quantum communication systems: id Quantique (Switzerland), MagiQ

Technologies (USA), SmartQuantum (France) and Quintessence Labs (Australia).

In both, quantum computation and quantum communication, entangled states of multiparticle quantum systems plays an important role. Although the notion of entanglement is known since the early days of quantum mechanics [38], it took almost 50 years of theoretical challenge until quantum entanglement was demonstrated experimentally [39] to be an element of physical reality.

Pure entangled states are best suited for technical applications because they bear only quantum correlations and do not show classical probabilistic correlations that are often detrimental to an application. However, there is no a quantum system that could be isolated perfectly from environmental influence. This unavoidable environmental coupling leads to non-unitary dynamics of initially pure states turning them to mixed states.

In practice, we of course need to know whether a given state is entangled and, if it is, how much entanglement is preserved in this quantum state. While entanglement of pure states can be easily quantified, the theoretical description of mixed states remains an open problem [40]. In general, amount of quantum correlation in a given (mixed) state can be quantified with a scalar quantity called entanglement measure. Although several such measures have been suggested, there is no a simple criteria to distinguish entanglement from classical correlations. Calculation of most of proposed entanglement measures that unambiguously discriminate classical against quantum correlations involve some sophisticated optimization procedures [41].

Quantification of entanglement is one of the main problems in quantum computation and quantum communication theories. There is, however, a number of other theoretical challenges. In quantum computation, for example, we need to read-out the result of computation encoded in a(n unknown for us) quantum state. This state is more likely given by a superposition of conventional basis states. According to quantum mechanics the coefficients of a quantum superposition have statistical meaning [42] and, therefore, can be experimentally identified only after a seria of measurements on a sufficiently large ensemble of identical particles. Of course, we are not supposed to run a quantum processor too many times in order to obtain a large ensemble of output states, rather, we are going to run it just a few times. But, if we have a finite and very limited ensemble of identical outputs[1], what is the best strategy to extract information about the superposition coefficients by a measurement. This problem is known as state estimation of an unknown quantum state [43, 44, 45].

Another practically important example comes from quantum communication. Although the no-cloning principle forbids exact replication of an unknown quantum state, it is still possible to make an approximate copy of a given state at cost of some perturbation [46]. This means that an eavesdropper can obtain some information about the transmitting message introducing some errors. In practice, errors in the transmission of a message can have very different reasons. Apart from the eavesdropper, the quantum control during the preparation or transmission of the quantum systems might be incomplete for a given realization of the quantum channel. For all practical realization of quantum communication protocols, therefore, a certain error

[1]We assume that the repeated computation did not cause any errors.

rate need to be accepted, and the eavesdropper might be successful in extracting some information about the message. That is why it is important to establish qualitative tradeoffs between the information acquired by an eavesdropper and the error rate. For the calculation of such tradeoffs, one should assume that the eavesdropper has applied the most powerful strategy consistent with quantum mechanics. The problem of estimating the maximum information for a given error rate is equivalent to the search for an optimal eavesdropping attack on the used protocol [47]. This is a very difficult problem and the complete solution is not known for any of the existing protocols[2].

In this thesis we shall explore in details several problems related to:

1. the description of entanglement and entanglement dynamics of multiparticle states of finite-dimensional quantum systems;

2. the optimal processing of information encoded in states of such systems.

The first part of this thesis, in particular, deals with the problem of quantifying entanglement. After a brief introduction of parametrization and properties of two- and multidimensional quantum systems in section 1.1, we shall present, in section 1.2, the entanglement theory (including the separability problem and constriction of entanglement monotones and entanglement measures) that has been developed over the past decade. The focus will be made especially on quantification of entanglement of general multiparticle states of two-dimensional quantum systems with certain entanglement measure – concurrence. In section 1.3, we shall analyze in details two essentially different ways of how this entanglement measure can be employed to characterize entanglement dynamics of a quantum system subjected to a general non-unitary evolution. The first part of this thesis ends with a summary on results of our analysis with some remarks.

The second part of this thesis is devoted to the optimal processing of information encoded in states of two-dimensional quantum systems. In section 2.1, in particular, we shall present the existing theory of quantum cloning, which is consistent with the no-cloning principle, and its application in eavesdropping of quantum communication. In section 2.2 we shall extend this theory to arbitrary quantum transformations. The focus will be made especially on transformations which do not depend on particular form of input states, i.e. are input state independent. We also suggest and discuss an application of these state independent transformations in quantum computing with initially mixed states. In section 2.3, in addition, we shall briefly discuss the problem of state estimation from a finite ensemble of identical particles and show an example of how the suggested state independent transformations may serve in estimating the fidelity between two finite ensembles of identical particles. We close the second part of this thesis with a discussion of our results.

[2]It is important to note that the eavesdropper's success does not dispute unconditional security of quantum communication. Intercepted information can be always reduced to zero, if the authorized users apply error correction and security amplification procedures [3] on their message. However, it is still necessary to know the maximum information that can be accessed by the eavesdropper in order to provide mentioned procedures in an optimal fashion.

Chapter 1

Quantifying quantum entanglement

[Entanglement] is not one, but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.

Erwin Schrödinger

1.1 Basic notations: qubit and qudit

The bit is the fundamental concept of classical computation and classical communication. Quantum computation and quantum communication are built upon an analogous concept, the q(uantum)bit. Just as a classical bit has a state – either 0 or 1 – a qubit also has two possible states $|0\rangle$ and $|1\rangle$. The difference between bits and qubits is that a qubit lives in a two-dimensional Hilbert space $\mathcal{H}$ and can be written as a complex linear combination of orthonormal basis states $|0\rangle$ and $|1\rangle$ as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\ , \tag{1.1}$$

where α and β are subordinated to the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. The qubit state (1.1) is called pure superposed state.

A pure qubit state can be visualized as a point on the unit three-dimensional (Bloch) sphere and can be also parameterized as

$$|\psi\rangle\ =\ \cos\frac{\theta}{2}\,|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}\,|1\rangle\ . \tag{1.2}$$

In this representation, the parameters θ and φ take values in the range $0 \leq \theta \leq \pi$ and $0 \leq \varphi < 2\pi$, respectively, and we shall later use the Bloch sphere in order to visualize the states of interest. From the context it will be always seen which parametrization of a qubit state between (1.1) and (1.2) we use at the moment.

More generally, a qubit may also exist as a statistical mixture of pure states $|\psi_i\rangle$. For example, a statistical mixture may represent an ensemble of states that is created

by a source that produces different states $|\psi_i\rangle$ with the according probabilities $p_i > 0$ (with $\sum_i p_i = 1$). This situation is described by a density matrix

$$\rho \equiv \sum_{ij} \rho_{ij} |i\rangle \langle j| = \sum_k p_k |\psi_k\rangle \langle \psi_k| \ . \tag{1.3}$$

This matrix is positive semidefinite and hermitian[1], since all the operators $|\psi_k\rangle \langle \psi_k|$ are positive semidefinite and hermitian. Conversely, any positive semidefinite matrix of trace one can be interpreted as a density matrix of some state. This leads to a geometrical picture of the set of all states as a convex set restricted by the Bloch sphere. A convex combination of two qubit states ρ_1 and ρ_2 is also a qubit state $\rho = \alpha\rho_1 + (1-\alpha)\rho_2$ with $\alpha \in [0,1]$.

The decomposition of a mixed state ρ into pure states $|\psi_k\rangle$ is not unique and depends on a chosen basis. If there exist a basis in which a qubit state ρ is given by a single term in the sum (1.3), the qubit is in a pure state, otherwise the qubit is in a mixed state. The simple criteria to distinguish between pure and mixed states is to calculate $\mathrm{Tr}\rho^2$ of a given state, where the trace operation

$$\mathrm{Tr}\, \rho = \sum_i \langle i| \rho |i\rangle = \rho_{ii} \tag{1.4}$$

takes the diagonal elements of a given state in some basis $\{|i\rangle\}$. Iff $\mathrm{Tr}\rho^2 = 1$, the qubit state ρ is pure. For $\mathrm{Tr}\rho^2 < 1$, the qubit state ρ is mixed.

Later we will be often interested in multiqubit systems. Such a system lives in a Hilbert space that is a tensor product of Hilbert spaces $\mathcal{H}$ which are associated with each individual qubit. The dimension of the N-qubit Hilbert space $\mathcal{H}^{\otimes N}$ is 2^N. Thus a pure state of a N-qubit system is given by a complex linear combination of 2^N mutually orthogonal basis vectors $|i\rangle$. It is convenient to write basis vectors of multiqubit systems in the binary (computational) form. For example, vectors $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ are the four computational basis vectors of a two-qubit system. A mixed state of a two-qubit system can be written as

$$\rho_{AB} = \sum_{ij,kl} \rho_{ij,kl} |i_A k_B\rangle \langle j_A l_B| = \sum_{ij,kl} \rho_{ij,kl} |i_A\rangle \langle j_A| \otimes |k_B\rangle \langle l_B| \ . \tag{1.5}$$

This definition generalizes straightforwardly to multiqubit systems.

Knowing the state of a multiqubit system, we may be interested to find out the state of some subsystem of this system. This task can be accomplished by taking partial trace. For example, for the two-qubit density matrix ρ^{AB}, the state of the qubit A is given by

$$\begin{aligned} \rho_A \equiv \mathrm{Tr}_B(\rho_{AB}) &= \mathrm{Tr}_B \left(\sum_{ij,kl} \rho_{ij,kl} |i_A\rangle \langle j_A| \otimes |k_B\rangle \langle l_B| \right) \\ &= \sum_{ij,kl} \rho_{ij,kl} |i_A\rangle \langle j_A| \ \langle k_B | \, l_B\rangle \ . \end{aligned} \tag{1.6}$$

[1] A hermitian matrix M is called positive semidefinite iff its eigenvalues are non-negative.

It is also useful to introduce a generalization of the qubit to higher dimensions, qudit, a d-dimensional $(d < \infty)$ quantum system. A pure state of qudit is defined by analogy with Eq. (1.1) and is given by a complex linear combination of d orthonormal basis states. A mixed state of qudit is then a statistical mixture of pure states (1.3). The definitions of trace (1.4) and partial trace (1.6) are straightforward. Later we will see that many results obtained for qubits can be extended to qudits.

Finally, after the mathematical introduction of the qubit concept, we would like to note that the qubit is not just a mathematical abstraction, it is a model for real physical systems. Electrons, nuclear or molecule spins, quantum dots or the polarization states of photons are physical representatives of qubit.

1.2 Entangled states

For a single qubit system (1.1), the statistics of measurements in the computational basis $\{|0\rangle, |1\rangle\}$ provides us with full knowledge about the coefficients α and β of the qubit state. The measurement data for a multiqubit system, however, may not be fully described by the collected statistics on the individual qubits, since there may exist correlations which cannot be deduced from observing the individual parts independently. For statistically independent quantum systems, say two qubits in pure states $|\psi_A\rangle$ and $|\psi_B\rangle$, the state of the system AB is simply formed by the tensor product of the states of its parts, i.e.

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = |\psi_A\rangle\, |\psi_B\rangle \,. \tag{1.7}$$

In this case, the statistics of measurements of the composite system AB is indeed given by the individual measurement data. Whenever a pure state of two (or more) qubits can be written as a tensor product of states of individual qubits, this state is called separable or a product state.

However, there are multiqubit states, so-called entangled states, which cannot be written as a tensor product of states of individual qubits. For such states the measurement results on different qubit subsystems are correlated. A (local) measurement of a single qubit causes a reduction of the multiqubit state and therefore changes the probabilities for potential measurements on the rest of the multiqubit system. The simplest example is a two-qubit system prepared in a pure (Bell) state

$$|\psi_{AB}\rangle = \frac{|0_A\rangle\, |1_B\rangle + |1_A\rangle\, |0_B\rangle}{\sqrt{2}} \,. \tag{1.8}$$

After a local measurement of qubit B the state of the qubit A is not a pure state, but is given by a statistical mixture of states, i.e. $\rho_A = \mathrm{Tr}_B\, |\psi_{AB}\rangle \langle\psi_{AB}| = (|0\rangle \langle 0| + |1\rangle \langle 1|)/2$.

By analogy with pure states, a general mixed state of N-qubit system is called separable iff it can be written as a convex combination of product states [48], i.e.

$$\rho_{\mathrm{sep}} = \sum_i p_i\, \rho_1^i \otimes \rho_2^i \otimes .. \otimes \rho_N^i \,, \tag{1.9}$$

where $\sum_i p_i = 1$ and $\rho_n^i = |\psi_n^i\rangle \langle\psi_n^i|$ for $n = 1..N$. If a mixed state cannot be written in the form (1.9) it is entangled.

1.2.1 Separability criteria

Having the simple definitions of entanglement and separability, it is very natural to verify whether a given multiqubit state is separable or entangled. In general, this is a very difficult (so-called separability) problem. Indeed, to check whether a given N-qubit density matrix admit decomposition (1.9) one should perform a search in 2^N-dimensional Hilbert space. Up to now, no general solution is known for the separability problem [40].

However, the separability problem can be unambiguously resolved for a number of special cases. For example, a simple criterion for separability of pure two-qubit states can be obtained with the help of Schmidt decomposition [3]. According to this decomposition any pure two-qubit state can be written in the form

$$|\psi_{AB}\rangle = \sum_i \sqrt{\lambda_i} \, |\psi_A\rangle_i \, |\psi_B\rangle_i \ , \tag{1.10}$$

where $\{|\psi_A\rangle\}$ and $\{|\psi_B\rangle\}$ are orthonormal bases for the qubit subsystems and $\sqrt{\lambda_i}$ are the real nonnegative (Schmidt) coefficients which fulfils $\sum_i \lambda_i = 1$. From Eq. (1.10), it follows immediately that the pure state $|\psi_{AB}\rangle$ is separable iff there is just one term in the Schmidt decomposition (1.10).

For a given pure two-qubit state, the decomposition (1.10) can be constructed as follows. We start from a representation of $|\psi_{AB}\rangle$ in some basis

$$|\psi_{AB}\rangle = \sum_{ij} a_{ij} \ |i_A\rangle \, |j_B\rangle \ , \tag{1.11}$$

so that the coefficients a_{ij} form a complex matrix A. Every complex matrix A can be diagonalized by two unitary transformations $U \equiv \{u_{ik}\}$ and $V \equiv \{v_{kj}\}$ such that

$$|\psi_{AB}\rangle = \sum_{ijk} u_{ik} d_{kk} v_{kj} \, |i_A\rangle \, |j_B\rangle \ , \tag{1.12}$$

with real and nonnegative diagonal elements d_k which provide the singular value decomposition of A [49]. Hence, any pure state $|\psi_{AB}\rangle$ can be represented in terms of its Schmidt coefficients $\lambda_k \equiv d_k^2$ and the associated Schmidt bases $|\psi_A\rangle_k = \sum_i u_{ik} \, |i_A\rangle$ and $|\psi_B\rangle_k = \sum_j v_{kj} \, |j_B\rangle$.

It is important to note that Schmidt decomposition can be constructed for an arbitrary pure two-qudit state $|\psi_{AB}\rangle$. The Schmidt coefficients in this case can be easily founded with the help of one of the reduced density matrices $\rho_A = \mathrm{Tr}_B \ |\psi_{AB} \langle\psi_{AB}|\rangle$ or $\rho_B = \mathrm{Tr}_A \ |\psi_{AB} \langle\psi_{AB}|\rangle$. Let us assume, without loss of generality, $d = \dim(\mathcal{H}_A) < \dim(\mathcal{H}_B)$. Using Eq. (1.10) it is easy to check that the spectrum of ρ_A is given by the Schmidt coefficients. The spectrum of ρ_B is the Schmidt coefficients and $\dim(\mathcal{H}_B) - \dim(\mathcal{H}_A)$ vanishing eigenvalues.

However, the Schmidt decomposition can not be constructed for a general pure state of a multiqubit (as well as a multiqudit) system with more than two subsystems. Even for a three-qubit system there are pure quantum states which can not be brought into the form [50]

$$|\psi_{ABC}\rangle = \sum_i \sqrt{\lambda_i}\, |i_A\rangle\, |i_B\rangle\, |i_C\rangle\ . \tag{1.13}$$

In absence of the high-order Schmidt decomposition , it is possible to use a legal trick – consider a N-qubit system as bipartite system of n_1 and n_2 qubits $(n_1 + n_2 = N)$ and construct a Schmidt decomposition for this bipartite system. This decomposition tells us whether the first n_1-qubit subsystem is separable from the second n_2-qubit subsystem.

The concept of Schmidt coefficients allows us to relate the degree of entanglement of pure states to the degree of mixing of the corresponding reduced density matrices. A pure reduced density matrix corresponds to a separable bipartite state. In the next section we will see how the degree of mixing of the reduced density matrices can be assign not only to distinguish between separable and entangled states, but also to quantify entanglement.

Apart of the case of pure bipartite (two-qubit and two-qudit) states discussed above, the separability problem can be unambiguously resolved for some two-partite mixed states. The standard approach to decide on the separability of a given mixed two-partite state relies on positive semidefinite map. A map $\Lambda : \mathcal{A}(\mathcal{H}) \to \mathcal{A}(\mathcal{H})$ is called positive semidefinite if it maps positive operators with nonnegative eigenvalues onto positive operators with nonnegative eigenvalues, i.e. $\Lambda(\rho) \geq 0$ for all $\rho \geq 0$. A crucial property of positive semidefinite maps is that an extension $\Lambda \otimes \mathbf{1}$ to higher dimensions is not positive, where $\mathbf{1}$ is the identity map. This property can be used to conclude on separability of a mixed state. Consider a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ of two d-dimensional systems $(d < \infty)$ and a positive semidefinite map on the Hilbert subspace $\mathcal{H}_A$, i.e. $\Lambda : \mathcal{A}(\mathcal{H}_\mathrm{A}) \to \mathcal{A}(\mathcal{H}_\mathrm{A})$. If map $\Lambda \otimes \mathbf{1}$ is applied on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, there are some states ρ for which this map is not positive, that is $(\Lambda \otimes \mathbf{1})\, \rho \ngeq 0$. However, if a state ρ is separable, its convex decomposition into product states (1.9) implies that

$$(\Lambda \otimes \mathbf{1})\, \rho = \sum_i p_i\, \Lambda(\rho_A^i) \otimes \rho_B^i\,, \tag{1.14}$$

i.e. $(\Lambda \otimes \mathbf{1})\, \rho \geq 0$. Thus, a state ρ is necessarily entangled if $(\Lambda \otimes \mathbf{1})\, \rho \ngeq 0$.

If, however, a given state ρ remains positive under the map $(\Lambda \otimes \mathbf{1})$, it does not guarantee that this state is separable. Only if $(\Lambda \otimes 1)\, \rho \geq 0$ for all positive maps Λ, it can be concluded that the state ρ is separable [51]. This statement does not allow to derive a sufficient separability criterion for a general case, since the classification of positive maps is a currently unsolved problem.

An example of separability criteria based on positive semidefinite maps is positive partial transpose (PPT) criterion [52]. According to it the matrix transposition operation $T(\rho) = T(\sum_{ij} \rho_{ij}\, |i\rangle\, \langle j|) \equiv \sum_{ij} \rho_{ij}\, |j\rangle\, \langle i|$ should be applied to one of the subsystems of a bipartite system. If the partial transpose $\rho^{pt} = (T \otimes \mathbf{1})\rho$ of a

bipartite state ρ has at least one negative eigenvalue, the state ρ is entangled. The PPT criterion unambiguously distinguishes separable and entangled states only for low-dimensional ($2 \otimes 2$ and $2 \otimes 3$) systems [51]. In higher dimensions there exist entangled states [53, 54] that are not detected by the PPT criterion.

To sum up, entangled and separable states can be unambiguously distinguished for: pure states of bipartite systems with arbitrary finite dimensions of the subsystems and mixed states of bipartite systems with low dimensions of the subsystems. Even in rather simple case of three qubits, there is no a simple (algebraic) criteria to distinguish separable and entangled states. There is a number of numerical approaches to resolve the separability problem [55]. However, for a N-qubit system a numerical solution of the separability problem require optimization over 4^N free real parameters.

1.2.2 Entanglement monotones and measures

The definition of separable states (1.9) is not constructive and, as we have just seen, does not provide us with an algorithm to distinguish between separable and entangled states. This definition, moreover, complicates finding a quantitative description of entanglement. Therefore, one should base on a completely different idea to quantify entanglement. Widely accepted strategy for a quantitative description of entanglement is to classify all kinds of operations that in principle can be applied to quantum systems. From all possible quantum operations we are interested in those which can change only classical correlations in quantum states leaving quantum correlations invariant. Any number assigned to a state that does not change under such operations can serve for a quantitative description of entanglement [56].

In general, a quantum operation describing evolution of a quantum system is given by a linear map $\mathcal{E} : \mathcal{B}(\mathcal{H}_\mathrm{i}) \to \mathcal{B}(\mathcal{H}_\mathrm{f})$,

$$\mathcal{E}(\alpha_1\rho_1 + \alpha_2\rho_2) = \alpha_1 \mathcal{E}(\rho_1) + \alpha_2 \mathcal{E}(\rho_2) , \tag{1.15}$$

according to the underlying linear Schrödinger equation. In order to ensure positivity of a quantum state ρ, the map $\mathcal{E}$ has to be positive. This requirement, however, is not strong enough. It is always possible to consider a quantum system as a subsystem of a larger one. In this case, the extended map $\mathcal{E} \otimes \mathbf{1}$ acts on the entire system so that the original map $\mathcal{E}$ affects the (sub)system of interest and the identity map $\mathbf{1}$ acts on the appended subsystem. As it was mentioned in the previous section, an extension $\mathcal{E} \otimes \mathbf{1}$ is not necessarily a positive map. In order to ensure that the map $\mathcal{E} \otimes \mathbf{1}$ is positive we have to require that any extension of the positive map $\mathcal{E}$ to identity maps in arbitrary dimensions is positive, i.e. the map $\mathcal{E}$ is completely positive. Accordingly, any operation consistent with quantum mechanics have to be described by a linear completely positive map. This implies, in particular, that separability criteria based on positive maps are not part of quantum dynamics, but just a mathematical tool to conclude on separability of a given quantum state.

The notion of quantum operation is a very general one that includes both unitary and non-unitary, *e.g.* due to environment coupling or measurements, evolution of a quantum system. A large class of quantum operations, such as

- unitary transformation, $\mathcal{E}_1(\rho) = U\rho U^\dagger$;
- addition to the original system ρ an auxiliary system σ, $\mathcal{E}_2(\rho) = \rho \otimes \sigma$;
- partial trace over a part p, $\mathcal{E}_3(\rho) = \mathrm{Tr}_p \rho$;
- projective measurement, $\mathcal{E}_4(\rho) = P_k \rho P_k / \mathrm{Tr}(P_k \rho)$, with $P_k^2 = P_k$;

can be expressed as an operator sum

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger , \tag{1.16}$$

where the linear operators E_i are subordinated to the condition $\sum_i E_i^\dagger E_i = \mathbf{1}$[2]. Using the operator sum representation (1.16) we can classify all quantum operations to three types [57]: local operations, global operations and local operations and classical communication (LOCC). What type of operations can assist in quantifying entanglement?

An operation is called local if under its action subsystems of a composite system evolve independently from each other. For a bipartite system, for example, the effect of a local operation can be described with the operator sum representation as

$$\mathcal{E}_{\mathrm{L}}(\rho) = \sum_{ij} E_i \otimes F_j \, \rho \, E_i^\dagger \otimes F_j^\dagger \quad \text{with} \quad \sum_{i,j} E_i^\dagger E_i \otimes F_j^\dagger F_j = \mathbf{1} . \tag{1.17}$$

Local operations do not change initial classical correlations in quantum states, e.g. a product state remains a product state under their action,

$$\mathcal{E}_{\mathrm{L}}(\rho_1 \otimes \rho_2) = \left(\sum_i E_i \rho_1 E_i^\dagger \right) \otimes \left(\sum_i F_i \rho_2 F_i^\dagger \right) . \tag{1.18}$$

Local operations also do not change quantum correlations,

$$\mathcal{E}_{\mathrm{L}} \left(\sum_i p_i \, \rho_1^i \otimes \rho_2^i \right) = \sum_i p_i \left(\sum_i E_i \rho_1^i E_i^\dagger \right) \otimes \left(\sum_i F_i \rho_2^i F_i^\dagger \right) . \tag{1.19}$$

Therefore, local operation can not serve in quantifying entanglement.

Any operation that is not local is called global. Under this type of operations both classical and quantum correlations may increase as well as decrease [57]. For example, the most prominent and natural way of creating entangled states is a global unitary evolution of a quantum system due to interaction between its subsystems [58, 59]. Therefore, global operations do not help to quantify entanglement.

LOCC is the third type of quantum operations. These operations comprise local operations and, in addition, allow exchange of classical information about locally performed operations and their results. In term of operator sums this is expressed as

$$\mathcal{E}_{\mathrm{LOCC}}(\rho) = \sum_i E_i \otimes F_i \, \rho \, E_i^\dagger \otimes F_i^\dagger \quad \text{with} \quad \sum_i E_i^\dagger E_i \otimes F_i^\dagger F_i = \mathbf{1} . \tag{1.20}$$

[2] For a restriction on the operator sum representation (1.16) see section (1.3).

In contrast to Eq. (1.17), only a single sum is involved in the description of LOCC. This implies the correlated application of the respective operations on the subsystems: if the operator E_i is applied to the first subsystem, the operator F_i is applied to the second subsystem.

LOCC can be used to create classical correlations between subsystems. In general, a product state does not remain a product one under the action of LOCC

$$\mathcal{E}_{\mathrm{LOCC}}\left(\rho_1 \otimes \rho_2\right) = \sum_i \left(E_i \rho_1 E_i^\dagger\right) \otimes \left(F_i \rho_2 F_i^\dagger\right) = \sum_i p_i \, \rho_1^i \otimes \rho_2^i \,, \tag{1.21}$$

where

$$\rho_1^i = \frac{E_i \rho_1 E_i^\dagger}{\mathrm{Tr}\left(E_i \rho_1 E_i^\dagger\right)} \,, \quad \rho_2^i = \frac{F_i \rho_2 F_i^\dagger}{\mathrm{Tr}\left(F_i \rho_2 F_i^\dagger\right)} \,, \tag{1.22}$$

and $p_i = \mathrm{Tr}\left(E_i \rho_1 E_i^\dagger\right) \mathrm{Tr}\left(F_i \rho_2 F_i^\dagger\right)$. Thus, classical probabilistic correlations can change under the action of LOCC. However, as it is seen from Eq. (1.21) separable states remain separable and, therefore, LOCC can not change entanglement[3].

Since it has been argued that entanglement can not be changed under LOCC, the discussion at the beginning of this section suggests to consider quantities that are invariant under LOCC. Any scalar valued function that satisfies this criterion is called an entanglement monotone [56] and can be used to quantify entanglement. For example, let us consider a bipartite system prepared in a pure state $|\psi_{AB}\rangle$. Taking partial trace over the subsystem B, we have a reduced density matrix $\rho_A = \mathrm{Tr}_B \, |\psi_{AB}\rangle \langle\psi_{AB}|$. As we mentioned in the previous section, the degree of mixing of the reduced density matrix can be assigned to the amount of entanglement of the pure state $|\psi_{AB}\rangle$. Therefore, any scalar function of the reduced density matrix $f\left(\rho_A\right)$ that is invariant under LOCC is an entanglement monotone. The simplest example of the entanglement monotone is $\mathrm{Tr}\rho_A^2$ [57].

Because of its invariance under LOCC, $f\left(\rho_A\right)$ can only be a function of unitary invariants, i.e. spectrum of ρ_A. Accordingly, it is not necessary to distinguish between ρ_A and ρ_B, since they have the same non-vanishing eigenvalues as we have seen during the discussion of the Schmidt coefficients. If the dimensions of ρ_A and ρ_B are not equal the reduced density matrix of the larger subsystem simply has some additional vanishing eigenvalues.

For pure bipartite states, it is rather simple to find an entanglement monotones due to the fact that there are no classical (probabilistic) correlations in these states. For mixed states, there are both classical and quantum correlations that should be discriminated against each other by the entanglement monotone. There are two general requirements to an entanglement monotone for a mixed state [57]. It must

[3]It is important to note that LOCC do not change entanglement on average. If we interpret a mixed state ρ as an ensemble of pure states, the non-increase of entanglement of ρ means that the ensemble average does not increase, whereas a single instance of the ensemble may show an increased amount of entanglement [60]. In section (1.3.2) a particular case of LOCC operation, so-called filtering operation, which can change entanglement with some probability will be shown.

be still invariant under LOCC and have to reduce to the original pure state definition when applied to a pure state.

On the first glance, it might be obvious that an entanglement monotone for a mixed state $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$ is a weighted by factors p_i linear combination of the monotones for pure states $|\psi_i\rangle$. However, the decomposition of a mixed state into pure states is not unique, therefore, different decompositions lead to different values for a chosen mixed state entanglement monotone. The unambiguous generalization of a pure state monotone to a mixed state monotone is the extremum over all possible decompositions into pure states – the so-called convex roof (extension) [41, 57]. Moreover, if a given mixed state is separable, the entanglement monotone should have the minimum value among all possible decompositions, therefore a mixed state monotone is the minimum over all possible decompositions

$$f(\rho) \equiv \min_{\{p_i,\psi_i\}} \sum_i p_i f(|\psi_i\rangle), \text{ with } \rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| . \tag{1.23}$$

Entanglement monotones that satisfy some additional axioms are called entanglement measures $\mathcal{EM}$. Although there are still some debates on the list of axioms that should be accepted [57, 60], there are three most frequently used requirements:

- $\mathcal{EM}(\rho)$ vanishes for a separable state ρ;
- $\mathcal{EM}(\rho)$ is a convex function, i.e.
  $\mathcal{EM}(\lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda\mathcal{EM}(\rho_1) + (1-\lambda)\mathcal{EM}(\rho_2)$, for $0 \leq \lambda \leq 1$;
- $\mathcal{EM}(\rho)$ is subadditive[4], the entanglement of a tensor product is not larger than the sum of the entanglement of both individual states, i.e.
  $\mathcal{EM}(\rho_1 \otimes \rho_2) \leq \mathcal{EM}(\rho_1) + \mathcal{EM}(\rho_2)$.

Up to now, a number of entanglement monotones and measures have been suggested [40]. In the next section we shall focus especially on, probably, the most powerful entanglement measure – concurrence.

1.2.3 Concurrence

Concurrence was originally introduced by Wootters to calculate entanglement of arbitrary states of two qubits [61]. Here, we shall first present the simple formula derived by Wootters to compute the concurrence. Next, we shall show how this simple formula can be derived from the optimization (1.23).

The formula for entanglement makes use a mathematical abstraction what can be called the 'spin flip' transformation. For a pure state of a single qubit, the spin flip, which is denoted by a tilde, is defined by

$$|\tilde{\psi}\rangle = \sigma_y |\psi^*\rangle , \tag{1.24}$$

[4] There is a much stronger requirement – additivity of an entanglement measure, $\mathcal{EM}(\rho_1 \otimes \rho_2) = \mathcal{EM}(\rho_1) + \mathcal{EM}(\rho_2)$. This requirement would significantly simplify quantifying entanglement. However, none of the existing entanglement measures is shown to be additive in general case [40].

where $|\psi^*\rangle$ is the complex conjugate of $|\psi\rangle$ when it is expressed in a chosen basis $\{|0\rangle, |1\rangle\}$ and σ_y is the matrix $\sigma_y = -i\,(|0\rangle\langle 1| - |1\rangle\langle 0|)$ in the same basis. To perform the spin flip on a general state of two qubits, one applies the above transformation to each individual qubit, i.e.

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)\,, \tag{1.25}$$

where again the complex conjugate is taken in the conventional basis. The concurrence for the mixed state ρ is given by

$$C(\rho) = \max\{0, \lambda^1 - \lambda^2 - \lambda^3 - \lambda^4\}\,, \tag{1.26}$$

where the λ^i, $i = 1..4$ are the square roots of the four nonvanishing eigenvalues of the non-hermitian matrix $\rho\,\tilde{\rho}$, if taken in decreasing order.

The Eq. (1.26) for the concurrence can be derived from the optimization of the convex roof (1.23) as follows. As it follows from Eqs. (1.25) and (1.26), the concurrence for a pure two-qubit state is given by

$$C(|\psi\rangle) = |\,\langle\psi^*|\,\sigma_y \otimes \sigma_y|\,\psi\rangle\,|\,. \tag{1.27}$$

It is easy to check by direct calculation that $C(|\psi\rangle) = \sqrt{2\,(1 - \mathrm{Tr}\rho_{\mathrm{red}}^2)}$, where ρ_{red} is a reduced single-qubit density matrix. Since the two-qubit concurrence (1.27) is a function of $\mathrm{Tr}\rho_{\mathrm{red}}^2$ it does not increase under LOCC. The concurrence of a pure two-qubit state also satisfies the three requirements at the end of the previous section to be an entanglement measure.

The concurrence of a mixed state is given by the corresponding convex roof, alike Eq. (1.23)

$$C(\rho) \equiv \min_{\{p_i,\psi_i\}} \sum_i p_i\, C(|\psi_i\rangle)\,,\ \text{with}\ \ \rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|\ . \tag{1.28}$$

To perform the optimization of this expression it is convenient to use the following characterization of ensembles of pure states. Using subnormalized states

$$|\Psi_i\rangle = \sqrt{p_i}\,|\psi_i\rangle \tag{1.29}$$

allows to reduce the number of involved quantities. Since the p_i are positive, one has $|\Psi_i\rangle\langle\Psi_i| = p_i\,|\psi_i\rangle\langle\psi_i|$. Assume one ensemble $\{|\Psi_i\rangle\}$ is known such that $\rho = \sum_i |\Psi_i\rangle\langle\Psi_i|$. A new ensemble can be defined as

$$|\Phi_i\rangle = \sum_j V_{ij}\,|\Psi_j\rangle\ , \quad \text{with} \sum_i V_{ki}^\dagger V_{ij} = \delta_{jk}\,, \tag{1.30}$$

which represents the same mixed state $\rho = \sum_i |\Psi_i\rangle\langle\Psi_i| = \sum_j |\Phi_j\rangle\langle\Phi_j|$. Moreover, any ensemble representing ρ can be constructed in this way.

Using the subnormalized states (1.29) and taking into account that the quantity $\langle\psi^*|\,\sigma_y \otimes \sigma_y|\,\psi\rangle$ in Eq. (1.27) can be understood as elements τ_{ij} of a complex symmetric matrix τ, the convex roof for the concurrence (1.28) can be written as

$$C(\rho) = \min_V \sum_i \left|\left[V\tau V^T\right]_{ii}\right|\ . \tag{1.31}$$

The minimum of this quantity is known [61] to be given by $C(\rho) = \max\{0, \lambda^1 - \lambda^2 - \lambda^3 - \lambda^4\}$ where λ^i are the square roots of the eigenvalues of the positive hermitian matrix $\tau\tau^\dagger$.

The concept of the concurrence can be extended to bipartite systems with arbitrary finite dimensions of the subsystems [62, 63]. The main ingredient to construct the (extended) concurrence is to define by analogy with Eq. (1.24) the 'spin flip' transformation for a pure qudit state. This task is, however, far from being trivial. The group of symmetry of a qubit, $SU(2)$, has only single generator σ_y which was used to construct the 'spin flip'. The group of symmetry of a d-dimensional $(d \geq 3)$ quantum system, $SO(d)$, has $n = d(d-1)/2$ generators. Each of this generators is a potential 'spin flip'. However, none of these generators by itself provide us with the desired state inversion (i.e. 'spin flip') operation [63]. The best approximation for the 'spin flip' transformation for a pure state $|\psi\rangle$ of a d-dimensional quantum system is given by a combination of $d(d-1)/2$ generators of the group $SO(d)$. Thus, the concurrence for a pure state of a bipartite $d_1 \otimes d_2$ system can be written as

$$C(|\psi\rangle) \equiv \sqrt{\sum_{i=1}^{\frac{d_1(d_1-1)}{2}} \sum_{j=1}^{\frac{d_2(d_2-1)}{2}} |C_{ij}|^2}\,, \tag{1.32}$$

where $C_{ij} = \langle\psi^*|\, L_i \otimes L_j |\,\psi\rangle$, L_i and L_j are the generators of the groups $SO(d_1)$ and $SO(d_2)$ respectively. In fact, the definition (1.32) is simply equivalent to $C(|\psi\rangle) = \sqrt{2\,(1 - \mathrm{Tr}\rho_{\mathrm{red}}^2)}$ [64, 65]. However, this definition (1.32) provides us with a constructive way to optimize the convex roof (1.28) for mixed bipartite states later. Indeed, each operator $L_i \otimes L_j$ describes a 'spin flip' transformation in just a $2 \otimes 2$-dimensional subspace of the original $d_1 \otimes d_2$-dimensional Hilbert state space of the bipartite system [66]. The concurrence $C(|\psi\rangle)$ is just the sum of all possible squared 'two-qubit' concurrences associated with the $2 \otimes 2$-dimensional subspaces. It is also notable that the concurrence (1.32) reduces to the definition (1.27) for two qubits.

Having the definition of the concurrence (1.32) for a pure state $|\psi\rangle$ of a bipartite system and taking into account the interpretation of this definition as given above, we can repeat the optimization of the convex roof (1.28) in order to obtain the expression for entanglement of a mixed state of a bipartite system. The concurrence for a mixed state ρ of a bipartite system is given by [66]

$$C(\rho) = \sqrt{\sum_{i=1}^{\frac{d_1(d_1-1)}{2}} \sum_{j=1}^{\frac{d_2(d_2-1)}{2}} |C_{ij}|^2}\,, \tag{1.33}$$

where $C_{ij} = \max\{0, \lambda_{ij}^1 - \lambda_{ij}^2 - \lambda_{ij}^3 - \lambda_{ij}^4\}$ and λ_{ij}^k, $k = 1..4$ are the square roots of the four nonzero eigenvalues, in decreasing order, of the non-Hermitian matrix $\rho\,\tilde{\rho}_{ij}$, where $\tilde{\rho}_{ij} = (L_i \otimes L_j)\rho^*(L_i \otimes L_j)$ and $i = 1..d_1(d_1-1)/2,\ j = 1..d_2(d_2-1)/2$.

Being an entanglement measure for an arbitrary mixed state of a bipartite system, the concurrence (1.33) should vanish for separable states and, therefore, may serve as a simple separability criteria. However, in section 1.2.1 we stated that there is no a

separability criteria for a general bipartite state. On the first glance, there is a contradiction until we remember that the 'spin flip' transformation used in Eqs. (1.32) and (1.33) is an approximation for the state inversion operation [63]. Thus, the bipartite concurrence (1.33) is also an approximation for the convex roof (1.28) for bipartite states and, therefore, can not be used for unambiguous discrimination between entangled and separable states. In spite of this the concurrence (1.33) detects most of mixed entangled states [66] what makes it quite a powerful entanglement measure.

1.2.4 A lower bound for concurrence

Unfortunately the concept of the concurrence cannot be straightforwardly extended to multipartite systems. The definitions for the concurrence for pure two-qubit (1.27) and two-qudit (1.32) states are based on our ability to distinguish between entangled and separable states assigning the degree of mixing of the reduced (over one subsystem) density matrix, i.e. $C(|\psi\rangle) = \sqrt{2\left(1 - \mathrm{Tr}\rho_{\mathrm{red}}^2\right)}$, to the entanglement of the given bipartite state. As we have seen in section 1.2.1, in the case of multipartite systems we are unable to say whether a given pure state is separable or entangled and, therefore, none value can be assigned to quantify entanglement of a pure state. The one way around is to consider a multipartite system as a bipartite system and quantify entanglement of this 'virtual' bipartite system. Although such bipartite split can not be unique we need to take into account all possible bipartite splits of a given multipartite system.

For example, for a given *pure* N-qubit state $|\psi\rangle$, the concurrence can be approximated by [64, 67]

$$C_N(|\psi\rangle) = \sqrt{1 - \frac{1}{N}\sum_{i=1}^{N} \mathrm{Tr}\,\rho_i^2}\,, \tag{1.34}$$

where the $\rho_i = \mathrm{Tr}\,|\psi\rangle\langle\psi|$ denotes the reduced density matrix of the i-th qubit which is obtained by tracing out the remaining $N-1$ qubits. This concurrence can be also expressed as a linear combination of N bipartite concurrences (1.32) for $(2 \otimes 2^{N-1})$-dimensional bipartite systems.

Having the definition (1.34) for the concurrence for a pure state of multiqubit system, we can formally define the concurrence for a mixed state through the convex roof (1.28). So far, however, there is no a general solution for the optimization problem (1.28) for multiqubit mixed states [40, 41]. Nevertheless, the convex roof can be estimated by a function that does not exceed the convex roof, a so-called lower bound for multiqubit concurrence. This function has a clear practical meaning: it defines the minimum (nontrivial) amount of entanglement which is preserved in a mixed state and can be further utilized [59].

So far, various numerically [41] and analytically [67] computable lower bounds have been suggested [40]. Here, I focus on an analytical lower bound for multiqubit

concurrence as suggested by Li *et al.* [67]. The lower bound $\tau_N(\rho)$ is given by

$$C_N(\rho) \geq \tau_N(\rho) \equiv \sqrt{\frac{1}{N}\sum_{n=1}^{N}\sum_{k=1}^{K}(C_k^n)^2}\,. \tag{1.35}$$

This bound is defined in terms of the N 'bipartite' concurrences C^n that correspond to the possible (bipartite) cuts of the multiqubit system in which just one of the qubits is discriminated from the other $N-1$ qubits. For the separation of the n-th qubit, the bipartite concurrence C^n is given by a sum of $K = 2^{N-2}\,(2^{N-1}-1)$ terms C_k which are expressed as

$$C_k^n = \max\{0, \lambda_k^1 - \lambda_k^2 - \lambda_k^3 - \lambda_k^4\}\,, \tag{1.36}$$

and where the λ_k^m, $m = 1..4$ are the square roots of the four nonvanishing eigenvalues of the matrix $\rho\,\tilde{\rho}_k^n$, if taken in decreasing order. These (non-hermitian) matrices $\rho\,\tilde{\rho}_k^n$ are formed by means of the density matrix ρ and its complex conjugate ρ^*, and are further transformed by the operators $\{S_k^n = L_k^n \otimes L_0,\ k = 1, ..., K\}$ as: $\tilde{\rho}_k^n = S_k^n \rho^* S_k^n$. In this notation, moreover, L_0 is the (single) generator of the group SO(2), while the $\{L_k^n\}$ are the $K = 2^{N-2}\,(2^{N-1}-1)$ generators of the group SO(2^{N-1}). In fact, the lower bound (1.35) is simply a linear combination of the squared bipartite concurrences (1.33) for mixed states.

Let us display this lower bound (1.35) especially for three-qubits, $\tau_3(\rho)$, for which the entanglement dynamics of entangled states will be discussed in the next section. For such states, the lower bound $\tau_3(\rho)$ can be written in terms of the three bipartite concurrences that correspond to possible cuts of the two qubits from the remaining one, i.e.

$$\tau_3(\rho) = \sqrt{\frac{1}{3}\sum_{k=1}^{6}(C_k^{12|3})^2 + (C_k^{13|2})^2 + (C_k^{23|1})^2}\,. \tag{1.37}$$

The bipartite concurrence $C_k^{ab|c}$ (for $a, b, c = 1..3$ and $a \neq b \neq c \neq a$) are obtained as described above with the help of the operators $\{S_k^{ab|c} = L_k^{ab} \otimes L_0^c,\ k = 1...6\}$, where L_0 is the generator of the group SO(2) which is given by the second Pauli matrix $\sigma_y = -i\,(|0\rangle\langle 1| - |1\rangle\langle 0|)$. The (six) generators L_k^{ab} of the group SO(4) can be expressed explicitly by means of the totally antisymmetric Levi-Cevita symbol in four dimensions as $(L_{kl})_{mn} = -i\,\varepsilon_{klmn};\ k, l, m, n = 1..4$ [68].

Of course, the lower bound (1.35) is only an approximation to the convex roof for the concurrence (1.28) as a measure of entanglement, therefore, it is useful to understand how well this measure is represented by the given bound. Unlike the analytical formula for the lower bound, the only way to compute the convex roof is to provide a numerical optimization. How demanding this numerical simulation for a given mixed state ρ of a multiqubit system is?

A given state ρ can be written using subnormalized states (1.29) as $\rho = \sum_i |\Psi_i\rangle\langle\Psi_i|$. The minimum number i of the ensemble members in this decomposition is given by the rank r, i.e. the number of nonvanishing eigenvalues, of the density matrix ρ.

According to the Caratheodory (convex hull) theorem, the maximum number of the ensemble members in the decomposition of the hermitian matrix ρ is r^2 [69]. Therefore, to find the optimal decomposition for ρ which minimize the convex roof (1.28) one should first define a $r^2 \times r$ matrix V_{ij} in Eq. (1.30). By varying the parameters of this matrix the optimal matrix V_{ij}^{opt} that transforms a given decomposition $\rho = |\Psi_i\rangle \langle\Psi_i|$ into the optimal one should be found. This implies an optimization procedure of dimensions r^3 for a given rank-r mixed state density matrix [57].

1.3 Entanglement dynamics

Having the tool, the lower bound for the concurrence (1.35), to quantify entanglement of general multiqubit states, we can describe entanglement dynamics of multiqubit systems. Typically, the evolution of entanglement of a system is deduced from studying its state evolution focusing especially on the most general nonunitary evolution [41, 75, 76].

The state dynamics of a closed quantum system which does not interact with the outside world is described by a unitary transform $|\phi\rangle = U|\psi\rangle$, where $U^\dagger U = \mathbf{1}$. In many cases, however, a physical system S cannot be considered as closed owing to its interaction with some environment E. Although the dynamics of the system S cannot be described by a unitary transformation any more, it is possible to consider a unitary evolution of a closed composite system SE. Assuming that the principal system S and the environment E are initially uncorrelated and that the environment was in some pure state $|e_0\rangle$, the general unitary evolution of the whole system SE can be written as

$$\rho_{SE} = U_{SE}\left(\rho_S \otimes |e_0\rangle \langle e_0|\right) U_{SE}^\dagger . \tag{1.38}$$

The evolution of the system S is obtained by tracing over the degrees of freedom of the environment, i.e.

$$\begin{aligned} \rho_S' &= \mathcal{E}(\rho) = \mathrm{Tr}_E\left[U_{SE}\left(\rho_S \otimes |e_0\rangle \langle e_0|\right) U_{SE}^\dagger\right] \\ &= \sum_i \left\langle e_i \mid U_{SE}\left(\rho_S \otimes |e_0\rangle \langle e_0|\right) U_{SE}^\dagger \mid e_i\right\rangle = \sum_i K_i \rho_S K_i^\dagger , \end{aligned} \tag{1.39}$$

where $\{|e_i\rangle\}$ denotes an orthonormal basis for the environment and $\sum_i K_i^\dagger K_i \leq \mathbf{1}$ [70, 71]. Essentially, Eq. (1.39) is an operator representation of a quantum operation, i.e. a completely positive map, $\mathcal{E}(\rho) = \sum_i K_i \rho_S K_i^\dagger$ which acts on the subsystem S. The corresponding operation elements K_i are sometimes called Kraus operators [72].

It is also important to note that, in this section, a slightly more general definition of quantum operation will be used in comparison to the definition (1.16) in section 1.2.1. While before we considered only trace-preserving quantum operations with $\sum_i K_i^\dagger K_i = \mathbf{1}$, here we include non-trace-preserving operations, i.e. with $\sum_i K_i^\dagger K_i \leq \mathbf{1}$, into consideration. These non-trace-preserving operations describe processes in which extra information about what occurred in the process is obtained by a measurement [3].

Operator representation (1.39) of quantum operation $\mathcal{E}$ is very simple and convenient tool to describe state dynamics of a system coupled to the environment. However, this representation was obtained under two assumptions that the principal system S and the environment E are initially uncorrelated and that the environment was in some pure state $|e_0\rangle$. Although there is no loss of generality in assuming that the environment starts in a pure state (since if it starts in a mixed state it is always possible to introduce an extra system purifying the environment), the first assumption is indeed crucial. If the system S and the environment E are initially entangled, the operator representation can not be given in the form $\mathcal{E}(\rho) = \sum_i K_i \rho_S K_i^\dagger$ [73]. Fortunately, in almost all cases in practice and as we shall always assume later, the system S and the environment E are initially uncorrelated.

Quantum operations formalism is not the only possible description of non-unitary behavior of a quantum system. The state dynamics of a quantum system can be provided by the master equation, which can be written most generally in the Lindblad form [74] as

$$\frac{\partial \rho}{\partial t} = -\frac{i}{\hbar}\left[H_S, \rho\right] + \sum_i \left(2L_i \rho L_i^\dagger - \{L_i^\dagger L_i, \rho\}\right). \tag{1.40}$$

where $\{a, b\} = ab + ba$ is an anticommutator, H_S is the system Hamiltonian that represents the coherent part of the dynamic and L_i are the Lindblad operators which are giving the coupling of the system to its environment. This master equation provides a valid description of the state dynamics iff the system and environment begins in product state [73] and the system-environment model Hamiltonian is consistent with Born and Markov approximations [70, 71].

The master equation approach (1.40) to describe state dynamics of a given system is less general than quantum operation formalism (1.39) [3]. Unlike the quantum operation formalism, however, the master equation provides continuous time description of state evolution and, therefore, it is used more often in quantum communication theory [70, 71]. Also, by analogy with classical communication theory, in quantum communication the environment $\mathcal{E}$ that acts on the system of interest $\mathcal{S}$ is usually called quantum noisy channel or simply quantum noise.

In the next section, we shall study entanglement dynamics of multiqubit states by example of three qubits. The entanglement evolution will be deduced from the state evolution of initially pure three-qubit states under the influence of environment. The examples of state evolution of the initially pure three-qubit states was worked out in [81] by solving analytically the master equation (1.40) for different models for the coupling of the system to its environment. Using these analytical expressions for the mixed-state density matrices, we shall quantify the (time-dependent) entanglement of these states by using the lower bound for three-qubit concurrence (1.37). We shall also discuss how the accuracy of the lower bound approximation for three-qubit concurrence depends on parameters of density matrices under consideration. As we have just seen at the end of the previous section, the numerical optimization for the convex roof depends on the matrix invariant – its rank. We shall show that the lower bound approximation also depends on this invariant. For density matrices with rank

$r \leq 4$, moreover, the comparison between the analytically computed lower bound and numerically optimized convex roof will be provided.

In section 1.3.2, a completely different approach for the description of entanglement dynamics, an evolution equation for entanglement [82, 83, 84], will be presented. An evolution equation for entanglement provides a direct relationship between the initial and the final entanglement of a quantum system without knowing underlying state dynamics.

1.3.1 Entanglement dynamics from state evolution

The best way to discuss entanglement dynamics of three-qubit states is to focus on some practical situations where such description is desired. At the beginning of the discussion it is useful to introduce the maximally entangled states of three qubits, the Greenberger-Horne-Zeilinger state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) , \tag{1.41}$$

and the W state

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right) . \tag{1.42}$$

These states are the typical members of the two inequivalent with regard to LOCC classes of three-qubit entangled states [77]. This implies that the GHZ state can not be transformed to the W state by means of local operations and classical communication and vice versa and, therefore, leads to completely different protocols for utilizing entanglement of the states (1.41)-(1.42). In particular, Karlsson and Bourennane [78] have suggested (teleportation-based) protocols for quantum communication between two and three partners based on the three-qubit GHZ state. Although the W can not be used to perform perfect teleportation [79], protocols for quantum teleportation between two partners and for superdense coding with an entangled state

$$|W'\rangle = \frac{1}{2}\left(\sqrt{2}\,|001\rangle + |010\rangle + |100\rangle\right) , \tag{1.43}$$

which belongs to the class of W states have been proposed by Agrawal and Pati [80].

Recently, Jung *et al.* [81] have analyzed the time evolution of the three-qubit GHZ (1.41) and W′ (1.43) states, if they are transmitted through noisy channels. As noise models for the influence of the environment the Pauli channels σ_z, σ_x and σ_y as well as the depolarizing channel were considered [3]. In this work, in more detail, an initially pure entangled state $\rho(0)$ was supposed to be transmitted through (one of) these channels for the time t, and its time evolution $\rho(t)$ obtained as solution of a (Lindblad-type) master equation (1.40). In this master equation, the (Lindblad) operators $L_{i,\alpha}$ were assumed to act independently upon the $i-$th qubit; for example, the operator $L_{1,z} \equiv \sqrt{k}\sigma_z \otimes \mathbf{1} \otimes \mathbf{1}$ describes the decoherence of the first qubit under a phase-flip σ_z, and where the coupling constant k is approximately inverse to the *decoherence time* with regard to such a phase-flip. Later we shall refer the Pauli channels σ_x and

σ_y to bit-flip and bit-phase-flip coupling of the three-qubit system to the environment, since this channels have the corresponding operational interpretation. For any given Pauli channel σ_α the master equation (1.40) only includes three Lindblad operators, $L_{1,\alpha}$, $L_{2,\alpha}$ and $L_{3,\alpha}$, while nine of these operators are needed for the depolarizing channel, $L_{i,\alpha}$, $(i = 1, 2, 3,\ \alpha = x, y, z)$. In the latter case, each of the qubits can be affected with equal coupling strength by all three Pauli channels simultaneously.

Knowing the time evolution of the three-qubit GHZ (1.41) and W′ (1.43) states in transmission through the Pauli and the depolarizing channels, we can employ the lower bound (1.37) to the concurrence $\tau_3(\rho(t))$ to analyze the decay of the entanglement for these states. Using the definition (1.34), we can easily calculate the concurrence $C_3(|\mathrm{GHZ}\rangle) = 1/\sqrt{2}$ and $C_3(|\mathrm{W}\rangle') = \sqrt{3/8}$ for pure GHZ (1.41) and pure W′ (1.43) states. The definition results in two different values; therefore, we shall re-normalize the expression (1.34) for each state in such a way, that we have $C_3(|\mathrm{GHZ}\rangle) = C_3(|\mathrm{W}\rangle') = 1$. This re-normalization is justified from an experimental viewpoint, since a three-qubit maximally entangled state can be viewed as a single unit of a quantum communication protocol.

If an initially pure GHZ state (1.41) is transmitted through the Pauli channel σ_z, its time evolution is obtained as solution of the master equation (1.40) with Lindblad operators $(L_{1,z}, L_{2,z}, L_{3,z})$ and can be expressed in terms of the rank-2 density matrix

$$\begin{aligned} \rho(t) &= \frac{1}{2}\left(|000\rangle\langle 000| + |111\rangle\langle 111|\right) \\ &+ \frac{1}{2}e^{-6kt}\left(|000\rangle\langle 111| + |111\rangle\langle 000|\right). \end{aligned} \tag{1.44}$$

For this mixed state, the lower bound (1.37) to the three-qubit concurrence is a monoexponential function of time,

$$\tau_3\left(\rho(t)\right) = e^{-6kt}. \tag{1.45}$$

Since the rank of the density matrix (1.44) is just two, the convex roof (1.28) for this density matrix can be even calculated analytically [75]. In this case, the convex roof is shown to follow the behavior of the nondiagonal elements (up to the normalization factor). In fact, the convex roof for the density matrix (1.44) coincides with the lower bound (1.45).

If the GHZ state (1.41) is instead transmitted through the Pauli channel σ_x, its time evolution is given by the rank-4 density matrix

$$\rho(t) = \frac{1}{8}\begin{pmatrix} \alpha_+ & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_+ \\ 0 & \alpha_- & 0 & 0 & 0 & 0 & \alpha_- & 0 \\ 0 & 0 & \alpha_- & 0 & 0 & \alpha_- & 0 & 0 \\ 0 & 0 & 0 & \alpha_- & \alpha_- & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha_- & \alpha_- & 0 & 0 & 0 \\ 0 & 0 & \alpha_- & 0 & 0 & \alpha_- & 0 & 0 \\ 0 & \alpha_- & 0 & 0 & 0 & 0 & \alpha_- & 0 \\ \alpha_+ & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_+ \end{pmatrix}, \tag{1.46}$$

with

$$\alpha_+ \;=\; 1+3e^{-4kt} \quad \text{and} \quad \alpha_- \;=\; 1-e^{-4kt}\,.$$

In this case, the lower bound (1.37) to the three-qubit concurrence becomes

$$\tau_3\left(\rho(t)\right) = e^{-4kt}\,. \tag{1.47}$$

For the rank-4 density matrix (1.46) we also calculated numerically the convex roof (1.28). The numerical simulation shows that the lower bound (1.47) coincides with the convex roof.

For a transmission of the GHZ (1.41) state through the Pauli channel σ_y, the density matrix

$$\rho(t) = \frac{1}{8}\begin{pmatrix} \alpha_+ & 0 & 0 & 0 & 0 & 0 & 0 & \beta_1 \\ 0 & \alpha_- & 0 & 0 & 0 & 0 & -\beta_2 & 0 \\ 0 & 0 & \alpha_- & 0 & 0 & -\beta_2 & 0 & 0 \\ 0 & 0 & 0 & \alpha_- & -\beta_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -\beta_2 & \alpha_- & 0 & 0 & 0 \\ 0 & 0 & -\beta_2 & 0 & 0 & \alpha_- & 0 & 0 \\ 0 & -\beta_2 & 0 & 0 & 0 & 0 & \alpha_- & 0 \\ \beta_1 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_+ \end{pmatrix}, \tag{1.48}$$

has full rank (i.e. rank 8), with the two functions

$$\beta_1 \;=\; 3e^{-2kt}+e^{-6kt} \quad \text{and} \quad \beta_2 \;=\; e^{-2kt}-e^{-6kt}\,,$$

respectively. For this matrix, the lower bound (1.37) to the concurrence gives rise to

$$\tau_3\left(\rho(t)\right) = \max\{0,\, \frac{1}{4}\left(3e^{-2kt}+e^{-4kt}+e^{-6kt}-1\right)\}\,, \tag{1.49}$$

or, in other words, this lower bound vanishes already after some finite time. Using the positive partial transpose separability criteria as it was discussed in section 1.2.1, we verified that the state (1.48) becomes separable only asymptotically for $t \to \infty$, which implies that the lower bound (1.49) does not describe the long-term behavior of the entanglement of an initial GHZ state if its is affected by bit-phase-flip noise.

For the rank-8 density matrix (1.48) the numerical calculation of the convex roof (1.28) requires optimization over $8^3 = 512$ free parameters. The numerical value of the convex roof (1.28) for the rank-8 density matrix (1.48) as well as for other rank-8 density matrices discussed below has not been obtained.

If the state (1.41) is transmitted through the depolarizing channel, its density

matrix has also rank-8 and takes the form

$$\rho(t) = \frac{1}{8}\begin{pmatrix} \tilde{\alpha}_+ & 0 & 0 & 0 & 0 & 0 & 0 & \gamma \\ 0 & \tilde{\alpha}_- & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}_- & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}_- & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_- & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_- & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_- & 0 \\ \gamma & 0 & 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_+ \end{pmatrix}, \tag{1.50}$$

with

$$\tilde{\alpha}_+ \;=\; 1+3e^{-8kt},\;\; \tilde{\alpha}_- \;=\; 1-e^{-8kt} \;\text{ and }\gamma = 4e^{-12kt}\,.$$

Here, again, the lower bound (1.37) to the entanglement vanishes already after some finite time due to the condition

$$\tau_3\left(\rho(t)\right) = \max\{0,\, \frac{1}{4}\left(4e^{-12kt}+e^{-8kt}-1\right)\}\,. \tag{1.51}$$

Fig. 1.1 displays the time-dependent lower bound (1.37) for initial GHZ state (1.41) if it's transmitted through the different channels. In all cases, this lower bound decays exponentially due to the noise of the channel; in transmission throw the Pauli channels σ_x and σ_y the entanglement of the GHZ state decreases slowly comparing to the Pauli channels σ_z. The depolarizing coupling of the three-qubit system to the channel is the most destructive for the entanglement. It is also remarkable that for density matrices with rank-2 and rank-4, the lower bound coincides with the convex roof and describes the entanglement evolution for all times, while this bound is not applicable for the long-time description of density matrices with rank-8 (the Pauli σ_y and the depolarizing channels) for which it vanishes at a finite time.

A similar analysis can be made if the system is initially prepared in the W′ state (1.43). If this state is transmitted through the channel σ_z, its time evolution is described by the rank-three density matrix

$$\rho(t) = \frac{1}{4}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & \sqrt{2}e^{-4kt} & 0 & \sqrt{2}e^{-4kt} & 0 & 0 & 0 \\ 0 & \sqrt{2}e^{-4kt} & 1 & 0 & e^{-4kt} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{2}e^{-4kt} & e^{-4kt} & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \tag{1.52}$$

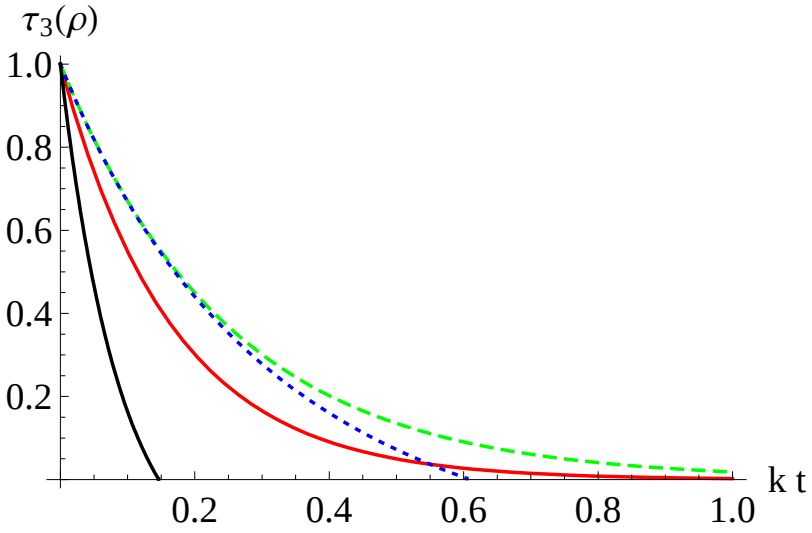

Figure 1.1: The lower bound (1.37) for the three-qubit concurrence τ_3 as function of time t for an initial GHZ state (1.41), if transmitted through various noisy channels: Pauli channels σ_z (solid red), σ_x (dashed green), σ_y (dotted blue) and the depolarizing channel (solid black).

and this gives rise to the lower bound

$$\tau_3\left(\rho(t)\right) = e^{-4kt} \tag{1.53}$$

for the evolution of the entanglement, which moreover coincides with the convex roof (1.37) as we verified numerically.

If the (initially prepared) W' state is transmitted through the Pauli channels σ_x or σ_y, a full rank-8 density matrix $\rho(t)_\pm$ is obtained for its time evolution

$$\frac{1}{16}\begin{pmatrix}
2\alpha_2 & 0 & 0 & \pm\sqrt{2}\alpha_2 & 0 & \pm\sqrt{2}\alpha_2 & \pm\alpha_2 & 0 \\
0 & 2\alpha_1 & \sqrt{2}\alpha_1 & 0 & \sqrt{2}\alpha_1 & 0 & 0 & \pm\alpha_3 \\
0 & \sqrt{2}\alpha_1 & 2\beta_+ & 0 & \alpha_1 & 0 & 0 & \pm\sqrt{2}\alpha_3 \\
\pm\sqrt{2}\alpha_2 & 0 & 0 & 2\beta_- & 0 & \alpha_4 & \sqrt{2}\alpha_4 & 0 \\
0 & \sqrt{2}\alpha_1 & \alpha_1 & 0 & 2\beta_+ & 0 & 0 & \pm\sqrt{2}\alpha_3 \\
\pm\sqrt{2}\alpha_2 & 0 & 0 & \alpha_4 & 0 & 2\beta_- & \sqrt{2}\alpha_4 & 0 \\
\pm\alpha_2 & 0 & 0 & \sqrt{2}\alpha_4 & 0 & \sqrt{2}\alpha_4 & 2\alpha_4 & 0 \\
0 & \pm\alpha_3 & \pm\sqrt{2}\alpha_3 & 0 & \pm\sqrt{2}\alpha_3 & 0 & 0 & 2\alpha_3
\end{pmatrix}, \tag{1.54}$$

and where the $+$ sign refers to the σ_x and $-$ to the σ_y channel, respectively. The

time-dependent parameters in expression (1.54) are given by

$$\begin{aligned}
\alpha_1 &= 1 + e^{-2kt} + e^{-4kt} + e^{-6kt} \\
\alpha_2 &= 1 + e^{-2kt} - e^{-4kt} - e^{-6kt} \\
\alpha_3 &= 1 - e^{-2kt} - e^{-4kt} + e^{-6kt} \\
\alpha_4 &= 1 - e^{-2kt} + e^{-4kt} - e^{-6kt} \quad \text{and} \quad \beta_\pm = 1 \pm e^{-6kt} .
\end{aligned}$$

Since two density matrices $\rho(t)_\pm$ have the same structure of matrix elements, the lower bounds for these density matrices coincide. Unfortunately, the analytical expression obtained for the lower bound for the density matrix (1.54) has no compact form and, thus, we do not show it here explicitly. At Fig. 1.2 the lower bound is shown with blue dashed line. As for all rank-8 density matrices above the lower bound for the density matrix (1.54) vanishes after finite time.

Finally, if the W' state (1.43) is transmitted through the depolarizing channel, the density matrix $\rho(t)$ has also rank-8 and is given by

$$\frac{1}{8}\begin{pmatrix}
\tilde{\alpha}_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \tilde{\alpha}_1 & \sqrt{2}\tilde{\gamma}_+ & 0 & \sqrt{2}\tilde{\gamma}_+ & 0 & 0 & 0 \\
0 & \sqrt{2}\tilde{\gamma}_+ & \tilde{\beta}_+ & 0 & \tilde{\gamma}_+ & 0 & 0 & 0 \\
0 & 0 & 0 & \tilde{\beta}_- & 0 & \tilde{\gamma}_- & \sqrt{2}\tilde{\gamma}_- & 0 \\
0 & \sqrt{2}\tilde{\gamma}_+ & \tilde{\gamma}_+ & 0 & \tilde{\beta}_+ & 0 & 0 & 0 \\
0 & 0 & 0 & \tilde{\gamma}_- & 0 & \tilde{\beta}_- & \sqrt{2}\tilde{\gamma}_- & 0 \\
0 & 0 & 0 & \sqrt{2}\tilde{\gamma}_- & 0 & \sqrt{2}\tilde{\gamma}_- & \tilde{\alpha}_4 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_3
\end{pmatrix}, \tag{1.55}$$

where

$$\begin{aligned}
\tilde{\alpha}_1 &= 1 + e^{-4kt} + e^{-8kt} + e^{-12kt} , \\
\tilde{\alpha}_2 &= 1 + e^{-4kt} - e^{-8kt} - e^{-12kt} , \\
\tilde{\alpha}_3 &= 1 - e^{-4kt} - e^{-8kt} + e^{-12kt} , \\
\tilde{\alpha}_4 &= 1 - e^{-4kt} + e^{-8kt} - e^{-12kt} , \\
\tilde{\beta}_\pm &= 1 \pm e^{-12kt} \quad \text{and} \quad \tilde{\gamma}_\pm = e^{-8kt} \pm e^{-12kt} .
\end{aligned}$$

The time-dependent lower bound (1.37) for initial W' state (1.43) transmitted through the different channels is shown in Fig. 1.2. As in the case of the GHZ state the lower bounds for the W' state decay exponentially due to the noise of the channels. In contrast to the GHZ state, the entanglement of the W' state decreases slowly in transmission throw the Pauli channel σ_z comparing to the Pauli channels σ_x and σ_y. However, the depolarizing coupling of the three-qubit system to the channel is again the most destructive for the entanglement. For the rank-3 density matrix, moreover, the lower bound coincides with the convex roof and describes the time evolution of the entanglement for all times, while this bound is not suitable for the

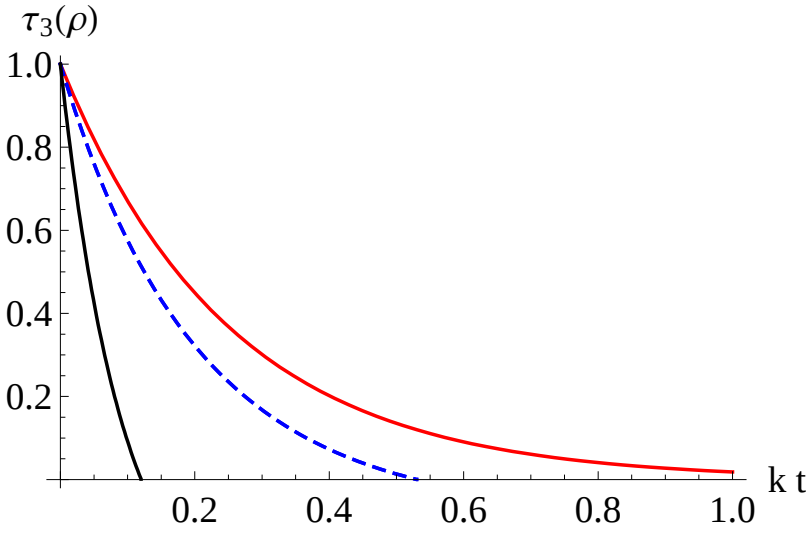

Figure 1.2: The same as in Fig. 1.1 but for an initial W' state (1.43); the lower bound (1.37) for the three-qubit concurrence τ_3 as function of time t is shown for noisy channels: Pauli channels σ_z (solid red), σ_x and σ_y (dashed blue) as well as the depolarizing channel (solid black)

long-time description of density matrices with rank eight, the Pauli σ_x and σ_y as well as depolarizing channels.

From the discussion above we have two important conclusions. First, the accuracy of the lower bound with regard to the convex roof depends on the rank of the density matrix under consideration. As we have shown on particular examples the lower bound coincides with the convex roof for density matrices with rank $r \leq 4$. For all rank-8 density matrices the lower bound vanishes after finite time making impossible long-time description of entanglement dynamics. In fact, this result can be easily understood if we look back to the structure of the lower bound (1.37) and bipartite concurrence (1.33). In both these formulas the concurrence is computed through equations alike Eq. (1.36), where only four eigenvalues of the matrix $\rho\,\tilde{\rho}_k^n$ are used independently on the rank of the given density matrix ρ. This is a drawback in the construction of the lower bound (1.37) and the bipartite concurrence (1.33) which has its roots in the approximate definition of the 'spin flip' operation (1.32).

Another practically important conclusion can be made based on the comparison of entanglement dynamics of pure GHZ (1.41) and W' (1.43) states under the influence of noisy channels. Similar question was earlier investigated by Carvalho *et al.* [75], who showed that an (initially pure) GHZ state is more fragile than the entanglement of a W state if affected by a thermal bath at zero or infinite temperatures, or by the so-called 'dephasing' (i.e. the Pauli σ_z) channel. Partially repeating this result we showed that an initially pure W' state preserves at all times t more entanglement than a GHZ state when passed through the Pauli σ_z, while, in contrast to [75], the GHZ state is doing better against decoherence for σ_x, σ_y, and the depolarizing channel.

1.3.2 Evolution equation for the entanglement

In the previous section we used the analytical solutions of the master equation (1.40) to describe entanglement dynamics of a three-qubit system. However, with increasing the dimension of the system, e.g. number of qubits, the analytical solution of the master equation dramatically complicates. For example, to describe state evolution of a N-qubit system one needs to solve in general 4^N differential equations for real functions. Thus, only for special cases the solution becomes feasible. This fundamental difficulty manifests the necessity to find a direct method to describe entanglement dynamics – an evolution equation for entanglement.

An evolution equation for quantum entanglement was originally suggested by Konrad *et al.* [82] to describe the time evolution of an entangled qubit pair without recourse to the time evolution of the underlying quantum state itself. Shortly, the concept of the evolution equation was extended to bipartite systems [83]. Here, we shall present the (extended) evolution equation for (finite-dimensional) bipartite systems as suggested in [83], focusing especially on the key ideas of how this equation can be derived. Next, we shall show how this evolution equation can be further extended to multiqubit systems.

Suppose, $|\chi\rangle$ is a pure state of a bipartite system $d_1 \otimes d_2$ with dimension d_1 and d_2 of the corresponding subsystems, and the second subsystem undergoes the action of a general noisy channel $\mathcal{S}$ which is given by a completely positive (non-)trace-preserving map. Then, the final state of the system is a mixed state in general and can be written in the symbolic form $\rho = (\mathbf{1} \otimes \mathcal{S}) |\chi\rangle \langle\chi|$. On the other hand, any pure state $|\chi\rangle$ can be obtained also from the maximally entangled state $|\phi\rangle = \sum_{i=1}^{d_2} |i\rangle \otimes |i\rangle / \sqrt{d_2}$ of the bipartite system by $|\chi\rangle = (M \otimes \mathbf{1}) |\phi\rangle$. In this notation, M denotes a local (filtering) operator that acts on the first subsystem of the maximally entangled state. Therefore, the final state ρ of the bipartite system can be expressed as

$$\rho = (\mathbf{1} \otimes \mathcal{S}) \ (M \otimes \mathbf{1}) \ |\phi\rangle \langle\phi| \ \left(M^\dagger \otimes \mathbf{1}\right) . \tag{1.56}$$

As we have discussed in section 1.2.2 local operations cannot change entanglement on average. There is a special case of LOCC, a filtering operator, which can increase (as well as decrease) entanglement probabilistically [85]. Let us show an example of filtering operation as it was given by Tiersch [60]. A filtering operation can be given in computational basis by a single (Kraus) operator

$$F = \sqrt{1-\kappa}\, |0\rangle \langle 0| + \sqrt{\kappa}\, |1\rangle \langle 1| \ , \quad 0 < \kappa < 1. \tag{1.57}$$

Since $F^\dagger F \neq \mathbf{1}$, the map associated with the filtering operation does not preserve the trace. If this filtering operation affects one qubit from an entangled pair initially prepared in state $|\psi\rangle = \sqrt{\lambda}\, |00\rangle + \sqrt{1-\lambda}\, |11\rangle$ with $0 < \lambda < 1$, the final two-qubit state is given by

$$\frac{|\psi'\rangle}{\| \, |\psi'\rangle \, \|} = \frac{(\mathbf{1} \otimes F) \, |\psi\rangle}{\| \, (\mathbf{1} \otimes F) \, |\psi\rangle \, \|} = \frac{\sqrt{\lambda(1-\kappa)}\, |00\rangle + \sqrt{\kappa(1-\lambda)}\, |11\rangle}{\lambda + \kappa - 2\lambda\kappa} . \tag{1.58}$$

The entanglement of the initial state $|\psi\rangle$ can be quantified by means of the concurrence (1.26) and equals $C(|\psi\rangle) = 2\sqrt{\lambda(1-\lambda)}$. The entanglement of the final state is given by

$$C\left(\frac{|\psi'\rangle}{\| \, |\psi'\rangle \, \|}\right) = \frac{2\sqrt{\lambda(1-\lambda)}\sqrt{\kappa(1-\kappa)}}{\lambda+\kappa-2\lambda\kappa}\,, \tag{1.59}$$

which becomes unity for $\lambda = \kappa$ and hence increase. However, this increase is probabilistic $p_F = \lambda+\kappa-2\lambda\kappa < 1$. A maximally entangled state $\lambda = 1/2$ undergoing the local filtering losses its entanglement from $C(|\psi\rangle) = 1$ to $C(|\psi'\rangle) = 2\sqrt{\kappa(1-\kappa)}$.

With this remark about the filtering operator, we now come back to the discussion of the bipartite system, i.e. to Eq. (1.56). Since the filtering operator M and the noise $\mathcal{S}$ act only on either the first or the second subsystems, the final state ρ can written in the form

$$\rho = (M \otimes \mathbf{1}) \; [(\mathbf{1} \otimes \mathcal{S}) \; |\phi\rangle \langle\phi|] \; \left(M^\dagger \otimes \mathbf{1}\right) \,, \tag{1.60}$$

which is equivalent to Eq. (1.56). The entanglement of the bipartite system under consideration can be quantified with the (bipartite) concurrence (1.33). Assume $(\mathbf{1} \otimes \mathcal{S}) \, |\phi\rangle \langle\phi| = \sum_i p_i \, |\varphi_i\rangle \langle\varphi_i|$ is the optimal decomposition of the state $(\mathbf{1} \otimes \mathcal{S}) \, |\phi\rangle \langle\phi|$ which minimize the convex roof (1.28). By convexity of the concurrence we have

$$\begin{aligned} C\left[\rho\right] \;&=\; C\left[\sum_i p_i \; (M \otimes \mathbf{1}) \; |\varphi_i\rangle \langle\varphi_i| \; \left(M^\dagger \otimes \mathbf{1}\right)\right] \\ &\leq \; \sum_i p_i \, C\left[(M \otimes \mathbf{1}) \; |\varphi_i\rangle \langle\varphi_i| \; \left(M^\dagger \otimes \mathbf{1}\right)\right] \\ &\leq \; \frac{d_2}{2} \, C\left[\chi\right] \, \sum_i p_i \, C\left[|\varphi_i\rangle\right] \equiv \frac{d_2}{2} \, C\left[\chi\right] \; C\left[(\mathbf{1} \otimes \mathcal{S}) \, |\phi\rangle \langle\phi|\right] \,, \end{aligned} \tag{1.61}$$

where the Cauchy inequity was used in order to come to the third line and d_2 denotes the dimension of the subsystem subjected to the noisy channel $\mathcal{S}$. Thus the evolution equation for entanglement of a bipartite system is given by

$$C[(\mathbf{1} \otimes \mathcal{S}) \; |\chi\rangle \langle\chi|] \; \leq \; \frac{d_2}{2} \, C[(\mathbf{1} \otimes \mathcal{S}) \; |\phi\rangle \langle\phi|] \; C[|\chi\rangle] \,, \tag{1.62}$$

i.e. the reduction of the entanglement of the system under the action of a noisy channel $\mathcal{S}$ is independent on the initial state $|\chi\rangle$, and is bounded from above by the channel's action upon the maximal entangled state $|\phi\rangle$. If, moreover, the bipartite system consists of a d_1-dimensional and a single-qubit subsystem, and just the qubit is affected by the noisy channel $\mathcal{S}$, the equal sign applies in inequality (1.62) and we obtain

$$C[(\mathbf{1} \otimes \mathcal{S}) \; |\chi\rangle \langle\chi|] \; = \; C[(\mathbf{1} \otimes \mathcal{S}) \; |\phi\rangle \langle\phi|] \; C[|\chi\rangle] \,. \tag{1.63}$$

That is, the entanglement dynamics of an arbitrary pure state of a $d_1 \otimes 2$ bipartite system is completely determined by the channel's action on the maximally entangled state $|\phi\rangle$ of the bipartite system if the single-qubit subsystem is affected by the noisy channel $\mathcal{S}$ [83] .

Based on Eq. (1.63) we can construct an evolution equation for the lower bound for three-qubit concurrence (1.37). Suppose $|\chi\rangle$ is a pure state of a three-qubit system and just one qubit undergoes the action of a channel $\mathcal{S}$. The final state of the three-qubit system takes the form $\rho = (\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,|\chi\rangle\,\langle\chi|$, which is equivalent to the final state of a bipartite $4\otimes 2$ system when the second subsystem is subjected to the channel $\mathcal{S}$. As we mentioned above, any pure state of a bipartite system can be obtained from the maximally entangled state of the bipartite system by means of a single local filtering operation M acting on the first subsystem as $|\chi\rangle = (M\otimes\mathbf{1})\,|\phi\rangle$.

In contrast, two local filters M and M' are in general required to obtain an arbitrary pure three-qubit state $|\chi\rangle$ from a maximally entangled state of three qubits $|\phi\rangle$ by $|\chi\rangle = (M\otimes M'\otimes\mathbf{1})\,|\phi\rangle$. For three-qubit systems, there are, moreover, two maximally entangled states (1.41) and (1.42) as we mentioned before. Although an arbitrary pure three-qubit state $|\chi\rangle$ can be generated from one of the maximally entangled states by means of local operations [77], we first need to identify the class of states either (1.41) and (1.42) to which it belongs to.

For an arbitrary (pure or mixed) three-qubit entangled state, fortunately, this is possible by following the procedure due to Dür *et al.* [77] which is simple and just includes the computation of the 3-tangle as described in [86]. It leads to the distinction that every entangled three-qubit state $|\chi\rangle$, for which the 3-tangle vanishes, belong to the W-class and can thus be obtained from the W state (1.42) by means of local unitary operations. In contrast, any entangled three-qubit state with nonvanishing 3-tangle is part of the GHZ-class. For a given pure three-qubit state $|\chi\rangle$, it is therefore always possible to find proper local (filtering) operations M and M' so that $|\chi\rangle$ is obtained from either (1.41) or (1.42) by $|\chi\rangle = (M\otimes M'\otimes\mathbf{1})\,|\phi\rangle$. Moreover, we have $|\phi\rangle \equiv |\mathrm{GHZ}\rangle$ if $|\chi\rangle$ belongs to the GHZ-class of entanglement, and $|\phi\rangle \equiv |W\rangle$ for $|\chi\rangle$ being part of the W-class.

To summarize our discussion here, the final state of the three-qubit system when one of its qubits undergoes the action of a noisy channel $\mathcal{S}$ is given by

$$\rho = (\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\times(M\otimes M'\otimes\mathbf{1})\;\;|\phi\rangle\,\langle\phi|\;\;\left(M^{\dagger}\otimes(M')^{\dagger}\otimes\mathbf{1}\right)\,. \tag{1.64}$$

where $|\phi\rangle$ is one of the maximally entangled states $\{|GHZ\rangle\,,\,|W\rangle\}$. In this equation (1.64), the filters M, M' and the noise $\mathcal{S}$ act on different subsystems. This allows us to apply the evolution equation for bipartite concurrence (1.63) to a 'bi-partite' split $12|3$ of the three-qubit system. We therefore obtain

$$C^{12|3}[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,|\chi\rangle\,\langle\chi|] \;=\; C^{12|3}[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,|\phi\rangle\,\langle\phi|]\;C^{12|3}[|\chi\rangle]\,, \tag{1.65}$$

while similar relations can be obtained for the 'bi-partite' concurrences $C^{13|2}$ and $C^{23|1}$ of the three-qubit system. Although the Eq. (1.65) has similar structure to the evolution equation for bipartite systems (1.63), they differ by the maximally entangled state $|\phi\rangle$ in their right-hand sides: the maximally entangled state $|\phi\rangle = \sum_{i=1}^{d_2}|i\rangle\otimes|i\rangle/\sqrt{d_2}$ of the bipartite system is to be substituted in Eq. (1.63), while one of the maximally entangled states (1.41)-(1.42) should be used in the right hand side of Eq. (1.65).

Because of the symmetry of the maximally entangled states (1.41)-(1.42) with regard to the qubits permutation we have a relation

$$\begin{aligned} C^{12|3}[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\left|\phi\right\rangle\left\langle\phi\right|] &= C^{13|2}[(\mathbf{1}\otimes\mathcal{S}\otimes\mathbf{1})\left|\phi\right\rangle\left\langle\phi\right|] \\ &= C^{23|1}[(\mathcal{S}\otimes\mathbf{1}\otimes\mathbf{1})\left|\phi\right\rangle\left\langle\phi\right|], \end{aligned} \tag{1.66}$$

where $|\phi\rangle = \{|GHZ\rangle, |W\rangle\}$. From Eqs. (1.65) and (1.66) it follows that for an arbitrary pure three-qubit state $|\chi\rangle$ the evolution of the bipartite concurrence is independent on a bipartite cut of the three-qubit system, i.e

$$\begin{aligned} C^{12|3}[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\left|\chi\right\rangle\left\langle\chi\right|] &= C^{13|2}[(\mathbf{1}\otimes\mathcal{S}\otimes\mathbf{1})\left|\chi\right\rangle\left\langle\chi\right|] \\ &= C^{23|1}[(\mathcal{S}\otimes\mathbf{1}\otimes\mathbf{1})\left|\chi\right\rangle\left\langle\chi\right|]. \end{aligned} \tag{1.67}$$

Substituting the evolution equation (1.65) into definition of the lower bound (1.37) and taking into account relation (1.66), we finally obtain an evolution equation of the lower bound for three-qubit concurrence

$$\tau_3[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\left|\chi\right\rangle\left\langle\chi\right|] = \tau_3[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\left|\phi\right\rangle\left\langle\phi\right|]\,\tau_3[|\chi\rangle], \tag{1.68}$$

where τ_3 [..] is defined in Eq. (1.37). The entanglement dynamics of an arbitrary pure state $|\chi\rangle$ of a three-qubit system, when one of its qubits undergoes the action of an arbitrary noisy channel $\mathcal{S}$, is subjected to the dynamics of one of the maximally entangled states $|\phi\rangle = \{|GHZ\rangle, |W\rangle\}$. The choice between the maximally entangled states should be done after determining the entanglement class of the given state $|\chi\rangle$ following the procedure in Ref. [77] and as briefly discussed above. We note, that due to Eq. (1.67) the entanglement dynamics of a pure three-qubit state $|\chi\rangle$ is independent on which of the qubits is affected by the noise. In fact, this equation (1.67) significantly simplifies the calculation of the lower bound (1.37). It is sufficient to compute just one bipartite concurrence in definition (1.37) of the lower bound, for example $C^{12|3}[|\chi\rangle]$, while the bipartite concurrences $C^{13|2}[|\chi\rangle]$ and $C^{23|1}[|\chi\rangle]$ are equal to it due to Eq. (1.67).

It is desirable, of course, to generalize the evolution equation (1.68) of the lower bound to the three-qubit concurrence also for N-qubit states, if just one of the qubits is affected by a noisy channel $\mathcal{S}$. In contrast to the classification of the three-qubit states, however, it is not known until now how many entanglement classes exist for qubit systems with $N > 4$, while some classification is available for $N = 4$ [87]. It is therefore not directly possible to generalize Eq. (1.68) to arbitrary pure states of N qubits. Nevertheless, some entanglement classes are known also for general pure N-qubit states, such as the GHZ- and W-class. If a given (pure) N-qubit state $|\chi\rangle$ belongs to the GHZ- or W-class, the evolution equation (1.68) of the lower bound can be extended to

$$\tau_N[(\mathbf{1}^{\otimes N-1}\otimes\mathcal{S})\left|\chi\right\rangle\left\langle\chi\right|] = \tau_N[(\mathbf{1}^{\otimes N-1}\otimes\mathcal{S})\left|\phi\right\rangle\left\langle\phi\right|]\,\tau_N[|\chi\rangle], \tag{1.69}$$

where $|\phi\rangle$ denotes the corresponding maximal entangled N-qubit state

$$|\mathrm{GHZ}\rangle_N = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right) , \tag{1.70}$$

$$|W\rangle_N = \frac{1}{\sqrt{N}}\left(|10,...,0\rangle + |01,...,0\rangle + |00,...,1\rangle\right) . \tag{1.71}$$

We can further analyze the lower bound (1.37) for the three-qubit concurrence in order to understand the entanglement evolution in those cases where one starts already with an initially mixed state ρ_0. If we make use of the convexity of the lower bound (1.68), we have $\tau_3[\,(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,\rho_0\,] = \tau_3[\sum_i p_i(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,|\psi\rangle_i\,\langle\psi|_i\,] \leq \sum_i p_i\tau_3[\,(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,|\psi\rangle_i\,\langle\psi|_i\,]$. Making use of this inequality in Eq. (1.68), we obtain

$$\tau_3[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\rho_0] \leq \tau_3[(\mathbf{1}\otimes\mathbf{1}\otimes\mathcal{S})\,|\phi\rangle\,\langle\phi|]\,\tau_3[\rho_0] \tag{1.72}$$

for the evolution of the lower bound and for an initially mixed state. As before, we assume here that just one of the qubits is affected by the noisy channel $\mathcal{S}$. Here, we like to underline that the inequality (1.72) holds for an arbitrary mixed state ρ_0, in spite of the fact that this inequality has been formulated for a lower bound τ_3. The generality of the inequality (1.72) build upon the convexity of the lower bound for the concurrence which is a valid entanglement measure.

The inequality (1.72) can be generalized for local two- and three-sided channels, i.e. to cases in which two or even all three qubits are affected by some local noise. For example, for a local two-sided channel $\mathcal{S}_1\otimes\mathcal{S}_2\otimes\mathbf{1} = (\mathcal{S}_1\otimes\mathbf{1}\otimes\mathbf{1})\,(\mathbf{1}\otimes\mathcal{S}_2\otimes\mathbf{1})$ we find

$$\begin{aligned}\tau_3[(\mathcal{S}_1\otimes\mathcal{S}_2\otimes\mathbf{1})\rho_0] \;\leq\; & \tau_3[(\mathcal{S}_1\otimes\mathbf{1}\otimes\mathbf{1})\,|\phi\rangle\,\langle\phi|] \\ & \times\tau_3[(\mathbf{1}\otimes\mathcal{S}_2\otimes\mathbf{1})\,|\phi\rangle\,\langle\phi|]\,\tau_3[\rho_0]\,.\end{aligned} \tag{1.73}$$

It is this particular form of Eq. (1.73) that gives rise to a sufficient criterion for finite-time disentanglement of arbitrary initial states being subjected to local multi-sided channels [82].

At the end of this section we would like to show three examples of the description of entanglement dynamics with the help of the evolution equation (1.72). We shall discuss the time evolution of entanglement of an initially mixed three-qubit state composed of GHZ (1.41) and W (1.42) state

$$\rho(p) = p\,|GHZ\rangle\,\langle GHZ| + (1-p)\,|W\rangle\,\langle W| \;, \tag{1.74}$$

if one of the qubits is affected by a phase, an amplitude or a generalized amplitude damping channel.

Indeed, there are several reasons for studying the entanglement evolution of the mixed state (1.74). For this state, first of all, an analytical expression is known for the convex roof to the concurrence [88]. This enables one to compare the time-dependent lower bound from the evolution equation (1.72) with the behavior of the convex roof as deduced from the state dynamics under the influence of a certain noise. Second,

the mixed state density matrix (1.74) has simply rank two. As we have seen earlier on particular examples, for rank-2 density matrices the lower bound (1.37) coincides with the convex roof. Third, it will be quite easy to compare also the speed of 'disentanglement' for an (initially) pure GHZ state $\rho(t, p = 1)$ and the pure W state $\rho(t, p = 0)$ under decoherence. We also note that the values for the lower bound for these pure states are related to each other through the ratio

$$\frac{\tau_3(\rho(t=0,p=1))}{\tau_3(\rho(t=0,p=0))} = \frac{\tau_3(|GHZ\rangle)}{\tau_3(|W\rangle)} = \frac{3}{2\sqrt{2}}\,, \tag{1.75}$$

a result that was obtained in [75] by means of a lower bound to the concurrence, different from definition (1.37).

Let us start with an example where a three-qubit system is prepared initially in the state (1.74) and just one qubit undergoes the action of the phase damping channel. A phase damping describes for instance a diffusive scattering interaction of the qubit with its environment and is known to result into a loss of phase coherence information. A possible representation of the phase damping in terms of time-dependent (Kraus) operators is given by [3]

$$K_1^{\rm pd} = \begin{pmatrix} e^{-\Gamma t} & 0 \\ 0 & 1 \end{pmatrix}, \quad K_2^{\rm pd} = \begin{pmatrix} \sqrt{1-e^{-2\Gamma t}} & 0 \\ 0 & 0 \end{pmatrix}. \tag{1.76}$$

where Γ denotes a coupling constant. For this noise model, Fig. 1.3 displays the time-dependent evolution of the lower bound τ_3 for the initially prepared state (1.74) for different parameters p of the mixed state and at different times of the system-channel coupling. In this figure, the blue surface displays the left-hand side (lhs) of the inequality (1.72), while the red lines shows the corresponding right-hand side. For all parameters $0 \leq p \leq 1$ of the mixed state, the lower bound τ_3 decays exponentially and vanishes only asymptotically for $t \to \infty$. For the phase damping channel, moreover, the lhs and rhs of (1.72) are always equal for an arbitrary parameter p and for all times t.

If the same system is affected by a (local) amplitude damping channel, which describes the dissipative coupling of a qubit to a thermal reservoir in the zero-temperature limit, the operator elements are given by [3]

$$K_1^{\rm ad} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\Gamma t} \end{pmatrix}, \quad K_2^{\rm ad} = \begin{pmatrix} 0 & \sqrt{1-e^{-2\Gamma t}} \\ 0 & 0 \end{pmatrix}. \tag{1.77}$$

For such an amplitude damping, the time evolution for the lower bound τ_3 shows completely different behavior in comparison to the corresponding dynamics in the phase damping channel as seen from Fig. 1.4. Although the lhs and the rhs of (1.72) differs significantly for some values of the parameter p, the rhs always exceeds the lhs as it is predicted by Eq. (1.72).

The third example shows entanglement sudden death [76] in the three-qubit system initially prepared in the state (1.74) and when just one qubits undergoes the

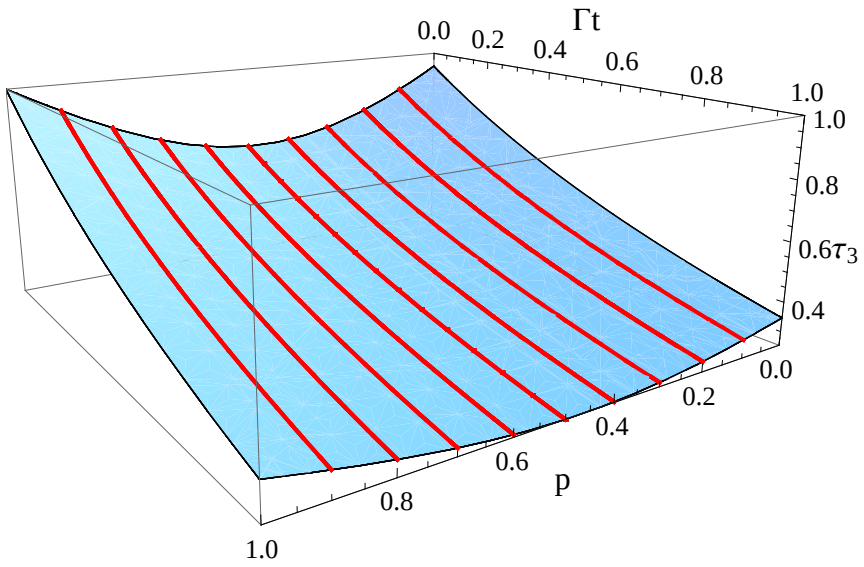

Figure 1.3: Evolution of the lower bound $\tau_3(\rho)$ for initially mixed state (1.74) if affected by the phase damping channel. While the blue surface shows the lhs of inequality (1.72), the red lines represents its rhs.

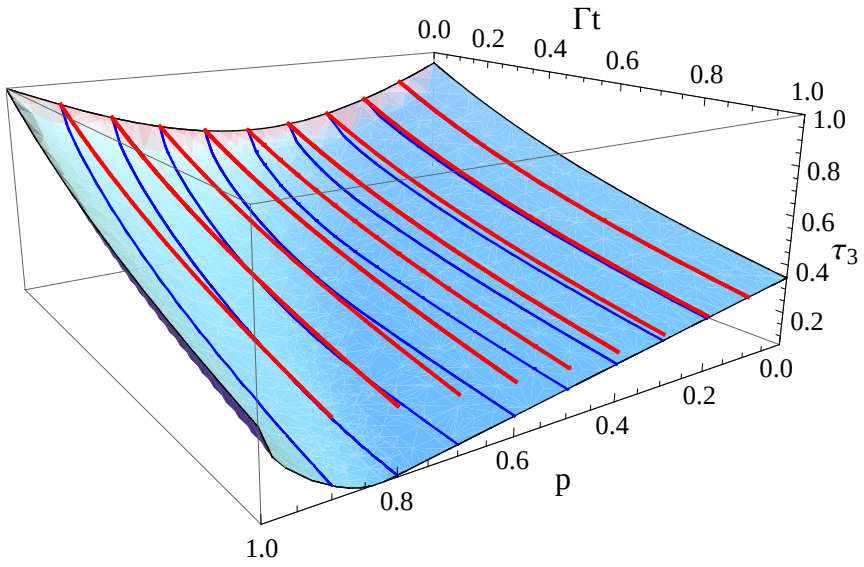

Figure 1.4: The same as in Fig. 1.3 but for the amplitude damping channel.

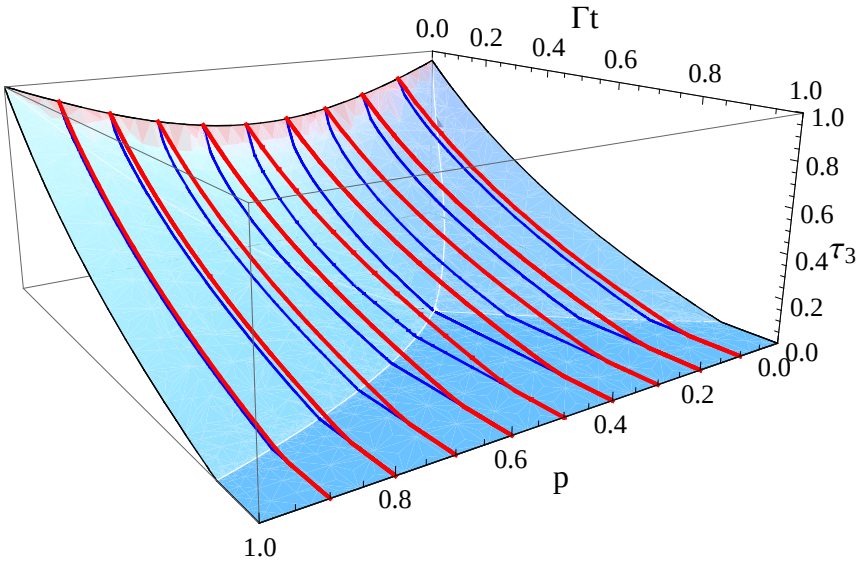

Figure 1.5: The same as in Fig. 1.3 but for the generalized amplitude damping channel. The sudden death of entanglement is clearly seen for all $0 \leq p \leq 1$.

action of the generalized amplitude damping channel. Based on the violation of additivity in the case of entanglement decay in a multi-qubit system coupled to two independent weak noises, entanglement sudden death reveals a practically important aspect of time-dependent entanglement evolution. It is important to verify whether such a phenomenon can be predicted with the suggested evolution equation of the lower bound (1.72). The generalized amplitude damping channel can be understood as a 'superposition' of two independent amplitude damping channels acting on a qubit and can be expressed by four Kraus operators $K_1^{\rm gad} = \frac{1}{2}K_1^{\rm ad}$, $K_2^{\rm gad} = \frac{1}{2}K_2^{\rm ad}$ and

$$K_3^{\rm gad} = \frac{1}{2}\begin{pmatrix} e^{-\Gamma t} & 0 \\ 0 & 1 \end{pmatrix}, \quad K_4^{\rm gad} = \frac{1}{2}\left(K_2^{\rm ad}\right)^{\dagger}, \tag{1.78}$$

where $K_1^{\rm ad}$ and $K_1^{\rm ad}$ are defined by Eq. (1.77). The evolution of the lower bound τ_3 for the three-qubit state (1.74) is shown in Fig. 1.5. Although the lhs and the rhs of the inequality (1.72) differ for some parameters p of the initial state $\rho(p)$, they both vanish in a finite time for all values p. Eq. (1.72), therefore, successfully describes the entanglement sudden death in this case.

1.4 Results and discussion

In this chapter, we have shown how entanglement and entanglement dynamics of an arbitrary state of a multiqubit system can be described with the help of the concurrence. While the computation of the (convex roof for the) concurrence for an arbitrary mixed state of a multiqubit system requires high-dimensional optimization

procedure, we have utilized a lower bound that can be computed analytically and showed by examples how accurate this bound is with respect to the convex roof for multiqubit concurrence.

In particular, based on the investigation of the entanglement dynamics of a three-qubit system coupled to environment in section 1.3.1, we have concluded that the accuracy of the lower bound depends on the rank of the density matrix under consideration. We have shown numerically that this bound coincides with the convex roof for density matrices with rank $r \leq 4$ as they appeared in section 1.3.1. Furthermore, with the help of the numerical algorithm which has been used to compute the convex roof for the concurrence for density matrices in section 1.3.1, we checked (by sampling 100 randomly generated density matrices) that the lower bound coincides with the convex roof for all (checked) density matrices with rank $r \leq 4$.

Also, using earlier suggested evolution equation for entanglement of bipartite quantum systems [83], we have proposed an evolution equation for entanglement of multiqubit systems in section 1.3.2 and showed three examples of the entanglement dynamics of a three-qubit system deduced from this new evolution equation.

Although much progress has been achieved during the last decade, the theory of quantifying entanglement is by no means complete and many problems remain unsolved [40]. The most fundamental problem is that it is still impossible to decide on separability of a given pure state of a multipartite system with more than two subsystems. As consequence none value can be assigned to describe 'true' entanglement of pure states of such systems and, therefore, any entanglement measure (or entanglement monotone) for multipartite systems is doomed to describe only entanglement of the system with regard to some bipartition or a combination of bipartitions.

It is also important to note that, in section 1.2.4, we used definition (1.34) for concurrence for a pure N-qubit state which was given by N bipartite concurrence where a single qubit was discriminated from $N-1$ qubits. There is, however, an alternative definition for concurrence for a pure N-qubit state $|\psi\rangle$ [75], i.e.

$$C_N(|\psi\rangle) = 2^{1-\frac{N}{2}} \sqrt{2^N - 2 - \sum_i \operatorname{Tr} \rho_i^2}\,, \tag{1.79}$$

where i runs over all possible $2^N - 2$ reduced density matrices which are obtained by tracing out not only a single qubit but also possible groups of $n = 1, 2, .., N-1$ qubits. However for this definition, the optimization of the convex roof becomes more complicated in comparison to the definition (1.34) because number of terms to be optimized growth. Moreover, the definition (1.79) does not give us any significant advantage in quantifying entanglement of three qubit systems , if compared to (1.34). In this particular case both definitions are equivalent. For a given pure three-qubit state $|\psi\rangle_{abc}$, the definition (1.79) requires computation of the traces of the six squared reduced density matrices ρ_i and ρ_{ij} for $i, j = a, b, c$ and $i \neq j$. However, the reduced density matrices ρ_a and ρ_{bc} have the same spectrum, and therefore there are only three matrices with different spectrum ρ_a, ρ_b and ρ_c. Thus the definitions (1.34) and (1.79) are equivalent indeed for an arbitrary pure three-qubit state.

There are many alternative to the concurrence proposals for entanglement measures, such as entanglement cost, entanglement of distillation, negativity and distance measures of entanglement [40, 59]. All these measures, except negativity, require some sort of optimization which often can not be done analytically and, therefore, do not have significant advantages over concurrence in entanglement description. In contrast, the computation of negativity does not require any optimization procedure. As discussed in section 1.2.1 in the context of the PPT separability criterion, the 'positivity' of the partial transpose of a density matrix is the necessary condition for separability. Therefore the amount of 'negativity' in the spectrum of the partial transpose gives rise to an entanglement measure. For a density matrix ρ of a bipartite system, for example, the negativity is defined as [89]

$$\mathcal{N}(\rho) = \frac{\mathrm{Tr}\sqrt{(\rho^T)^\dagger \rho^T} - 1}{d-1}, \tag{1.80}$$

where ρ^T denotes the partial transpose with respect to one subsystem and d is the dimension of smaller of the two subsystems. Of course, the negativity is incapable to describe entanglement of those entangled states which can not be detected by the PPT separability criterion. Moreover, it is unclear upon which of the given density matrix parameters the negativity depends. This makes negativity less competable to concurrence.

Finally, we would like to mention some approaches on quantification of entanglement in experiment. The most natural way to quantify entanglement of a given (unknown) state is to 'learn' the state first by means of the quantum state tomography [3] and quantify entanglement of this state thereafter. An alternative way is to construct a special observable – an entanglement witness [59]. By definition, this observable is a hermitian operator whose expectation value is positive for all separable states and negative for entangled states. Although the construction of an entanglement witness for an arbitrary multipartite state is a very complicated problem, an optimal witness has been recently constructed for unknown two-qubit entanglement [90]. Moreover, through the concept of entanglement witness a lower bound for concurrence can be directly measured [59].

In practice, it is often required to characterize entanglement dynamics of a quantum system that undergoes the action of some noisy channel. Usually, to estimate the robustness of the quantum system subjected to such process, one should accomplish quantum process tomography on certain types of initially prepares states [3]. However, the concept of the evolution equation as it is presented in section 1.3.2 simplifies the experimental characterization of entanglement dynamics under unknown channels dramatically: instead of exploring the time-dependent action of the channel on all initial states, it suffices to probe the entanglement evolution of the maximally entangled states alone. Moreover, the evolution equation for quantum entanglement has been recently successfully applied to characterize the entanglement dynamics of two-qubit systems coupled to some environments [91, 92].

Chapter 2

Optimal state independent quantum transformations

A quantum state is nothing more or less
than a prediction of the future.

Robin Blume-Kohout

Using quantum systems to encode and process information offers impressive technological advantages in communication and computing in comparison to classical information processing. Technological utilization of quantum systems necessarily requires clear understanding of the fundamental features of quantum information processing, such as the possibilities to copy, transform and read out the information. On the first glance, it may be obvious that these possibilities are essential features of any good encoding of information. This is, however, not the case: when information is encoded in quantum systems, in general it can not be replicated, transformed or read out without introducing errors. This limitation, however, does not make quantum information useless – quite the contrary, as we will see in this chapter.

In section 2.1 we shall discuss the essential features of copying of quantum information. In section 2.1.1, in more details, we shall formulate the no-cloning and the general impossibility theorems which postulate the fundamental restrictions on quantum copying process. Although the no-cloning theorem forbids exact copying of arbitrary states of quantum systems, we shall present, in section 2.1.2, a theory of physical device (so-called quantum cloning machine – QCM) that may support imperfect cloning of unknown qubits. We shall show, moreover, how such a QCM can be constructed from certain requirements. In section 2.1.3 we shall analyze how QCM may assist in the eavesdropping in quantum communication by example of incoherent attack on B92 protocol [32] for quantum key distribution.

In section 2.2 we shall move beyond quantum cloning and consider a general class of unitary quantum transformations that do not depend on input states. We shall start, in section 2.2.1, with single-qubit transformations that provide a desired operation on unknown input states. In section 2.2.2, we shall construct an optimal

approximation for the two-qubit state independent C-NOT operation — the operation that can not be constructed to be exact due to the general impossibility theorem. Based on this construction we shall demonstrate a deep analogy between cloning and state independent transformations. This analogy is extended to the case of multi-qubit controlled unitary transformations in section 2.2.3. Section 2.2.4 is devoted to a discussion of a possible application of state independent transformations in quantum computing with initially mixed states. In contrast to standard input state dependent transformations, we show that state independent transformations can be utilized efficiently to construct a quantum circuit for computation when the initial states are mixed.

Finally, we shall briefly discuss, in section 2.3, the optimal way of extracting information from finite ensembles of identically prepared particles. In particular, we shall discuss state estimation from a finite ensemble of unknown (equatorial) qubit states and suggest the best way of estimating fidelity between two ensembles of such states. In the latter case we show that the best strategy for the fidelity estimation includes two stages: a specific unitary state independent transformation on two ensembles and state estimation of the output states of this transformation.

2.1 Quantum cloning

2.1.1 No-cloning theorem

It is well known that the state of a single quantum system can not be perfectly reconstructed: the result of any single measurement of an observable O is one of its eigenstates, bearing only very poor information about the state before the measurement, namely, that is not orthogonal to the measured eigenstate. The only way to achieve a perfect reconstruction of the state of quantum system is to compute the statistical averages of different observables measured on a large ensemble of identically prepared systems. However, one can imagine how to overcome the impossibility to reconstruct the state of a single quanta in the following way: take the system in the unknown state $|\psi\rangle$ and let it interact (in some way consistent with quantum mechanics) with N other systems previously prepared in some reference (blank) state $|R\rangle$ in order to obtain $N+1$ copies of the initial state:

$$|\psi\rangle \otimes |R\rangle^{\otimes N} \longrightarrow |\psi\rangle^{\otimes N+1} . \tag{2.1}$$

Such a procedure would allow one to determine the quantum state of a single system without even measuring it because one could measure the N new copies and leave the original state untouched. The no-cloning theorem of quantum information formalizes impossibility of such a procedure: *No quantum operation exists that can duplicate perfectly an arbitrary quantum state*.

The theorem was originally formulated and proven by Wootters and Zurek [27] and independently by Dieks [28]. To understand the basic idea it is sufficient to prove the theorem for the simplest case of $1 \rightarrow 2$ cloning of a qubit, i.e. when two copies are

obtained from a single input qubit state. As we discussed already at the beginning of section 1.3, the most general quantum operation can be given by a unitary evolution of the principal system with some environment. In quantum information processing the environment is usually called an auxiliary system or simply ancilla. So let us suppose that perfect cloning of a quantum system initially prepared in a pure qubit state $|\psi\rangle$ can be realized as a unitary evolution involving an ancilla, i.e.

$$|\psi\rangle \otimes |R\rangle \otimes |A\rangle \longrightarrow |\psi\rangle \otimes |\psi\rangle \otimes |A_\psi\rangle \ . \tag{2.2}$$

Since a qubit state $|\psi\rangle$ is just a superposition of the basis states $|0\rangle$ and $|1\rangle$, the transformation (2.2) can be also written for the basis states as

$$\begin{aligned} |0\rangle \otimes |R\rangle \otimes |A\rangle &\longrightarrow |0\rangle \otimes |0\rangle \otimes |A_0\rangle \ , \\ |1\rangle \otimes |R\rangle \otimes |A\rangle &\longrightarrow |1\rangle \otimes |1\rangle \otimes |A_1\rangle \ . \end{aligned} \tag{2.3}$$

Making a linear combination of these transformations we obtain

$$(|0\rangle + |1\rangle) \otimes |R\rangle \otimes |A\rangle \longrightarrow |0\rangle \otimes |0\rangle \otimes |A_0\rangle + |1\rangle \otimes |1\rangle \otimes |A_1\rangle \ . \tag{2.4}$$

But, from the other hand, the cloning of the state $(|0\rangle + |1\rangle)$ should result to

$$(|0\rangle + |1\rangle)\ (|0\rangle + |1\rangle)\ \left|A_{(0+1)}\right\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)\ \left|A_{(0+1)}\right\rangle \tag{2.5}$$

where we omitted the tensor product for simplicity. The right hand side of the Eq. (2.4) can not be equal to Eq. (2.5). Since we used only linearity of quantum mechanics to come to this contradiction, our initial assumption, that the perfect cloning of a qubit can be realized, is wrong. This concludes the proof of the no-cloning theorem.

Shortly after its discovery, the no-cloning theorem was extended to arbitrary (pure and mixed) states of both finite- and infinite-dimensional quantum systems [46]. Moreover, it was shown by Pati [93] that no quantum operation exists that can provide perfectly the controlled unitary transformation

$$|\psi\rangle \otimes |R\rangle \otimes |A\rangle \longrightarrow |\psi\rangle \otimes |U(\psi)R\rangle \otimes |A_\psi\rangle \ , \tag{2.6}$$

on an arbitrary pure qubit state $|\psi\rangle$. This statement is known today as the general impossibility theorem. The proof of this theorem is very similar to the proof of the no-cloning theorem as it is given above and, therefore, we skip it here. The general impossibility theorem can be interpreted as follows. To perform a unitary transformation $U(\psi)$ on the blank state $|R\rangle$, it is necessary to obtain some information about the unknown input state $|\psi\rangle$ without changing this state. This would be in conflict with the no-cloning principle which implies that no information can be obtained about the quantum state without changing it.

2.1.2 Quantum cloning machine

The first step beyond the no-cloning theorem was done by Bužek and Hillery [94], who considered the possibility of imperfect cloning. Specifically, they considered ancilla assisted $1 \rightarrow 2$ cloning of an unknown qubit state and found a unitary transformation which provides this copying at cost of some perturbation of both original state and the copy. They called the device that provides this transformation a quantum cloning machine (QCM).

The discovery of the first QCM by Bužek and Hillery triggered an explosion in the number of investigations on quantum cloning. Formally, any quantum operation acting on M quantum systems, possibly mediated by an ancilla, which share the information between all the systems is a QCM. Thus for N replicas of an unknown qubit state $|\psi\rangle$ and $M-N$ blank states $|R\rangle$ a unitary transformation

$$|\psi\rangle^{\otimes N} \otimes |R\rangle^{\otimes (M-N)} \otimes |A\rangle \longrightarrow |\Psi\rangle \tag{2.7}$$

represents a $N \rightarrow M$ QCM and where $|\Psi\rangle$ gives the final state of the M copies with the ancilla. Since, in general, the copies are entangled with the ancilla, the state of each single copy is mixed and can be obtained by tracing out the auxiliary degrees of freedom and remaining $M-1$ copies.

To talk about efficiency of a QCM we need to have a quantitative characterization of how good the copies are in comparison to the input state. The commonly used quantity to characterize quality of the copies is *fidelity* which is defined for the original state $|\psi\rangle$ and the approximate copy ρ as

$$F = \langle\psi|\rho\,|\,\psi\rangle \ . \tag{2.8}$$

All QCMs can be classified by their properties [46]:

- A QCM is called optimal if the fidelities of the clones are the maximal allowed by quantum mechanics.
- A QCM is called universal if it copies equally well all the states of a given quantum system, i.e. if the fidelity of the copy is independent on the input state. Nonuniversal QCMs are called state dependent.
- A QCM is called symmetric if all the clones have the same fidelity in comparison to the input, otherwise a QCM is called asymmetric.
- If the cloning process is supported by an auxiliary system, a QCM is called ancilla assisted. There are several examples of QCM's which do not require ancilla [95, 96].
- Finally, QCMs can be split on deterministic and probabilistic. While in the spirit of Bužek and Hillery a determined imperfect cloning is allowed, in probabilistic cloning perfect copies are required [97, 98], but the price is that the QCM works only with some probability.

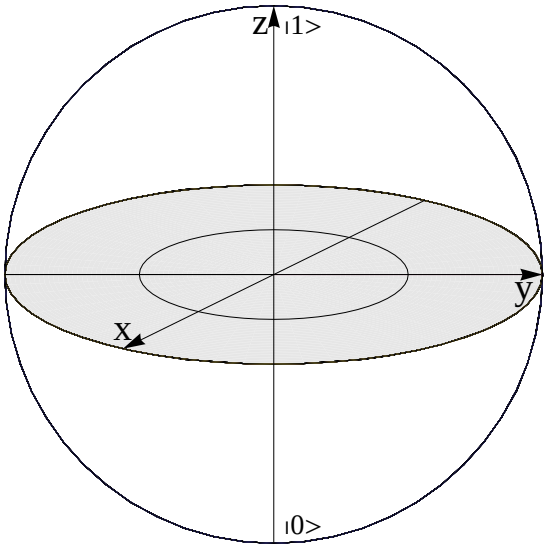

Figure 2.1: Bloch sphere representation of a qubit state.

Within this classification, only optimal deterministic symmetric and ancilla assisted QCMs will be considered in this thesis.

To simplify our discussion of universal and states dependent QCMs, it is convenient to introduce some additional notations. As we indicated in section 1.1, a pure qubit state can be visualized with the help of the Bloch sphere as it is displayed in Fig. 2.1 and parameterized as $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$, where $|0\rangle$ and $|1\rangle$ are the chosen (computational) basis states. Moreover, let us refer to the intersection of the Bloch sphere with the *z-y* plane as the main circle, so that all states from this intersection can be parameterized by means of just the (single) parameter θ as

$$|\psi_{\rm mc}\rangle = \cos\frac{\theta}{2}|0\rangle \pm \sin\frac{\theta}{2}|1\rangle \ . \tag{2.9}$$

These states are often called real states of qubit. While, in this expression, the '$+$' sign refers to the right (Eastern) meridian of the main circle passing through the positive direction of the *y* axis and includes for $\theta = \pi/2$ also the diagonal state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The '–' sign is associated with left (Western) meridian and includes the state $|-\rangle$.

The intersection of the sphere with the *x-y* plane is called equator of the Bloch sphere. All states from the equator can be parameterized with single parameter ϕ as

$$|\psi_{\rm e}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right) \ , \tag{2.10}$$

and are called equatorial. For the sake of simplicity in visualizing the different states on the Bloch sphere, we shall use this 'geographical' notation in our discussion below.

Let us show how an optimal quantum cloning transformation can be constructed by example of $1 \to 2$ cloning of a qubit. Although the state $|\psi\rangle$ of a given qubit is

typically in a superposition of the two basis states $|0\rangle$ and $|1\rangle$, it is of course sufficient to know the transformation of just the basis in order to obtain a proper copying of states. Therefore, the most general $(1 \rightarrow 2)$ quantum cloning transformation for the qubit state $|\psi\rangle$ upon the blank state $|0\rangle$ can be cast into the form

$$\begin{aligned} |0\rangle\,|0\rangle\,|A\rangle \;&\longrightarrow\; \sum_{i,j=0}^{1} |i\rangle\,|j\rangle\,|A_{ij}\rangle\;, \\ |1\rangle\,|0\rangle\,|A\rangle \;&\longrightarrow\; \sum_{i,j=0}^{1} |i\rangle\,|j\rangle\,\left|A'_{ij}\right\rangle\;, \end{aligned} \tag{2.11}$$

where $|A\rangle$ denotes the initial state of the ancilla, and where we have assumed — without loss of generality — that the blank qubit was prepared initially in the basis state $|0\rangle$. Once, the transformation has been performed, $|i\rangle$ and $|j\rangle$ denote the output basis states of the two copies, while $|A_{ij}\rangle$ and $\left|A'_{ij}\right\rangle$ are the corresponding states of the apparatus. As seen from the transformation (2.11), here we do not assume any additional condition for the final states of the cloning apparatus. However, in order to ensure that the transformation (2.11) is unitary,

$$\sum_{k} c_k\,|k\rangle\,|A\rangle \longrightarrow \sum_{k,\lambda} c_k U_{k\lambda}\,|\lambda\rangle\;, \tag{2.12}$$

for all possible input states, i.e. for $|k\rangle = \{|0\rangle\,|0\rangle\,,\,|1\rangle\,|0\rangle\}$, the final states of the apparatus must fulfill certain requirements [99]. In Eq. (2.12), the three-partite basis $\{|\lambda\rangle\}$ refers to a complete and orthonormal basis for the overall system 'the two qubits + apparatus'. Thus, the requested unitarity $U^{\dagger}U = \mathbf{1}$ of the transformation (2.11) implies the conditions

$$\begin{aligned} \sum_{i,j=0}^{1} \langle A_{ij}\,|\,A_{ij}\rangle \;&=\; \sum_{i,j=0}^{1} \left\langle A'_{ij}\,\middle|\,A'_{ij}\right\rangle \;=\; 1\,, \\ \sum_{i,j=0}^{1} \left\langle A_{ij}\,\middle|\,A'_{ij}\right\rangle \;&=\; 0\,. \end{aligned} \tag{2.13}$$

For any explicit construction of a $(1 \rightarrow 2)$ quantum cloning transformation, we must therefore 'determine' the final states $|A_{ij}\rangle$ and $\left|A'_{ij}\right\rangle$ of the apparatus in line with the conditions (2.13). These state vectors then define the cloning transformation uniquely.

For a general pure input qubit state, the cloning transformation (2.11) leads to the two-qubit output density matrix which is obtained by making a superposition of the first and the second lines of this transformation for an input qubit state and after the tracing over the auxiliary degrees of freedom. The two-qubit density matrix contains 16 scalar products between different final state vectors $|A_{ij}\rangle$ and $\left|A'_{ij}\right\rangle$ of the apparatus. Each scalar product introduces a (complex) parameter of the cloning transformation. This gives rise to the 16 optimization parameters for the cloning

transformation, while only the 3 conditions (2.13) need to be fulfilled due to the unitarity of the transformation.

Further conditions must therefore be formulated in order to define the QCM properly. For example, Bužek and Hillery have analyzed the three-term transformation

$$\begin{aligned} |0\rangle|0\rangle|A\rangle &\longrightarrow |0\rangle|0\rangle|A_{00}\rangle + (|0\rangle|1\rangle + |1\rangle|0\rangle)|A_{01}\rangle\,, \\ |1\rangle|0\rangle|A\rangle &\longrightarrow |1\rangle|1\rangle|A_{11}\rangle + (|0\rangle|1\rangle + |1\rangle|0\rangle)|A_{10}\rangle\,, \end{aligned} \tag{2.14}$$

with conditions

$$\langle A_{01}\,|\,A_{01}\rangle = \langle A_{10}\,|\,A_{10}\rangle \equiv \zeta\,, \tag{2.15}$$

$$\langle A_{01}\,|\,A_{11}\rangle = \langle A_{10}\,|\,A_{00}\rangle \equiv \eta/2\,, \tag{2.16}$$

$$\langle A_{11}\,|\,A_{10}\rangle = \langle A_{00}\,|\,A_{01}\rangle \equiv \kappa/2\,. \tag{2.17}$$

Under these conditions, it follows from Eqs. (2.13) that $\langle A_{00}\,|\,A_{00}\rangle = \langle A_{11}\,|\,A_{11}\rangle = 1-2\zeta$.

With these additional conditions, we have arrived at the final-state two-qubit density matrix $\rho^{\rm out}$ of the transformation (2.14) that now depends only on three parameters ζ, η and κ. We note that in the original work of Bužek and Hillery [94] the parameter κ was assumed to be zero. Thus the discussion below is slightly more general. While the condition (2.17) introduces a nonorthogonality between the final states of the apparatus, three parameters ζ, η and κ will eventually enable us to provide high-fidelity copies for a region of input states from the Bloch sphere. However, the three parameters ζ, η and κ are not completely independent of each other but must fulfill the three inequalities

$$\begin{aligned} 0 \;&\le\; \zeta \;\le\; \frac{1}{2}\,, \\ 0 \;&\le\; \eta \;\le\; 2\sqrt{\zeta(1-2\zeta)}\,, \\ 0 \;&\le\; \kappa \;\le\; 2\sqrt{\zeta(1-2\zeta)}\,. \end{aligned} \tag{2.18}$$

due to Schwarz' inequality for the state vectors of the cloning apparatus.

The quantum cloning transformation (2.14) can be further defined, in particular, to copy real qubit states (2.9) with high fidelity. Making a superposition of the first and the second lines of this transformation for an input qubit state and after the tracing over the auxiliary degrees of freedom and one of the copies we obtain a single-qubit density matrix

$$\begin{aligned} \rho^{\rm out} = \left(\cos^2\frac{\theta}{2} - \zeta\cos\theta\right)|0\rangle\langle 0| \;&+\; \frac{1}{2}\left(\kappa \pm \eta\sin\theta\right)\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) \\ &+\; \left(\sin^2\frac{\theta}{2} + \zeta\cos\theta\right)|1\rangle\langle 1|\,, \end{aligned} \tag{2.19}$$

which is the same for both copies. We can utilize this expression (2.19) to calculate the fidelity between the input and output for all states (2.9) along the main circle

$$F(\theta) \equiv \langle\psi_{\rm mc}|\rho^{\rm out}\,|\,\psi_{\rm mc}\rangle = (1-\zeta) - \frac{1}{2}(1-\eta-2\zeta)\sin^2\theta \pm \frac{\kappa}{2}\sin\theta\,. \tag{2.20}$$

Although the parameters ζ, η and κ are restricted by the inequalities (2.18), it is this freedom in choosing these parameters that enables us to optimize the fidelity $F(\theta)$ for certain (regions of) states. A general method for numerical optimization of parameters of an unitary transformation was developed by Audenaert and De Moor [100] and was successfully applied to show optimality of some cloning transformations [101]. Within this method, the optimal cloning transformation maximizes average single-clone fidelity

$$\overline{F} = \int_{\Omega} \frac{d\theta}{N} F(\theta) \tag{2.21}$$

for chosen region of states Ω on the Bloch sphere, where N is the normalization factor. Since the integral (2.21) depends on parameters of the given fidelity function $F(\theta)$, the maximum average fidelity can be obtained by varying numerically these parameters. Sometimes, however, the maximization of the average fidelity can be done even analytically.

If we require that the cloning transformation (2.14) copies an arbitrary real qubit state with maximal and constant fidelity, by optimizing (2.21) we obtain the parameters

$$\kappa = 0, \qquad \zeta = \frac{1}{6}, \qquad \eta = \frac{2}{3}, \tag{2.22}$$

which correspond to the average fidelity $\overline{F} = 5/6 \approx 0.83$. Through these parameters, using their definitions (2.15)-(2.17), the final states $|A_{ij}\rangle$ and $|A'_{ij}\rangle$ of the ancilla can be defined as

$$\begin{aligned} |A_{01}\rangle &= \left\{\frac{1}{\sqrt{6}}, 0\right\}, \quad |A_{10}\rangle = \left\{0, \frac{1}{\sqrt{6}}\right\}, \\ |A_{00}\rangle &= \left\{0, \sqrt{\frac{2}{3}}\right\}, \quad |A_{11}\rangle = \left\{\sqrt{\frac{2}{3}}, 0\right\}, \end{aligned} \tag{2.23}$$

It is quite interesting to admit that these four vectors span only a two-dimensional subspace within the (four-dimensional) space of the general copying machine (2.11). This implies that, in practice, a single qubit may play a role of the ancilla.

With the help of the final states (2.27) the quantum cloning transformation (2.14) can be written explicitly as

$$\begin{aligned} |0\rangle|0\rangle|A\rangle &\longrightarrow \sqrt{\frac{2}{3}}|00\rangle|0\rangle + \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle)|1\rangle, \\ |1\rangle|0\rangle|A\rangle &\longrightarrow \sqrt{\frac{2}{3}}|11\rangle|1\rangle + \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle)|0\rangle. \end{aligned} \tag{2.24}$$

This is the original quantum cloning transformation constructed by Bužek and Hillery. Although we constructed this transformation by optimization of the fidelity (2.8) only for real qubit states, this transformation was shown to be universal [95], i.e. it provides two copies of an arbitrary pure qubit state with maximal possible fidelity $F = 5/6$. The QCM that corresponds to the transformation (2.24) is called universal.

The fidelity of the copies from the universal QCM can be exceeded for some restricted set of input states. Since the parameter κ in the expression (2.20) for the fidelity of the transformation (2.14) has a different sign for the two parts of the main circle, a nonzero value of this parameter leads to a quite different behavior of the fidelity along Western and Eastern meridians: the high fidelity along Eastern meridian correspond to positive parameter κ, while the high fidelity along Western meridian is achieved for negative κ. So, for proper values of ζ, η and κ we can obtain a high fidelity for one meridian. In particular, let us require that the cloning transformation (2.14) copies states from the Easter meridian with maximal average fidelity. Substituting in the expression (2.21) the fidelity function (2.20) and integrating over all states from Eastern meridian of the Bloch sphere, we obtain average fidelity as function of the parameters ζ, η and κ, i.e.

$$\overline{F} = \int_0^\pi \frac{d\theta}{\pi} F(\theta) = \frac{1}{4}\left(3 - 2\zeta + \eta + \frac{4\kappa}{\pi}\right) . \tag{2.25}$$

Following numerical optimization procedure over the three parameters, which are restricted with inequalities (2.18), gives values

$$\kappa = \frac{2}{5}, \qquad \zeta = \frac{1}{10}, \qquad \eta = \frac{2}{5}, \tag{2.26}$$

approximately, that correspond to the maximal average fidelity $\overline{F} \approx 0.927$ which is better that the fidelity of the universal QCM.

There is, however, another quite an elegant way to perform optimization of the fidelity function (2.20) that does not require numerical calculations. It is known that parameters of the universal QCM can be found from the requirement of optimal copying of just the discrete set of six states that lie on x, y and z axis of the Bloch sphere [46]. We may, for example, request an equal and maximum fidelity for just three selected states from the meridian in order to determine optimal parameters of the cloning transformation (2.14). If the input $|\psi\rangle$ is taken from the set of the three states $|0\rangle$, $|1\rangle$ and $|+\rangle$ and we request an equal-fidelity cloning of them, the maximum fidelity $F = 0.90$ is obtained for the parameters (2.26). This result is not surprising since the fidelity has local minima for the states $|0\rangle$, $|1\rangle$ and $|+\rangle$; that is the main reason for optimization with this three states. In fact, in this optimization procedure we restricted the fidelity function (2.20) downwards.

To complete the construction of the state dependent QCM for states from the Eastern meridian we need to define the final-state vectors $|A_{ij}\rangle$ of the ancilla. With the help of the parameters (2.26) the final-state vectors can be defined as

$$\begin{aligned} |A_{01}\rangle &= \left\{\frac{1}{\sqrt{10}}, 0\right\}, \quad |A_{10}\rangle = \left\{0, \frac{1}{\sqrt{10}}\right\}, \\ |A_{00}\rangle &= \left\{\sqrt{\frac{2}{5}}, \sqrt{\frac{2}{5}}\right\}, \quad |A_{11}\rangle = \left\{\sqrt{\frac{2}{5}}, \sqrt{\frac{2}{5}}\right\}, \end{aligned} \tag{2.27}$$

in line with the conditions (2.15)-(2.17) from above. As in the case of universal QCM, these four vectors span only a two-dimensional subspace within the (four-dimensional)

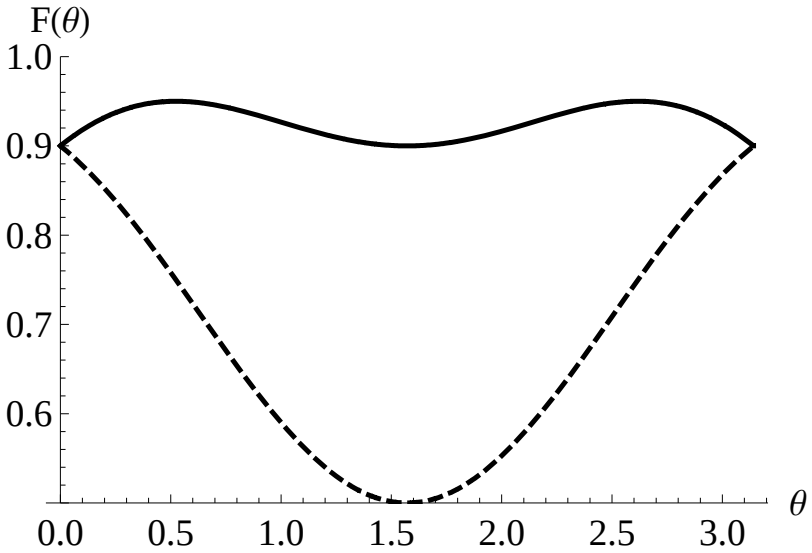

Figure 2.2: Fidelity (2.29) of the quantum cloning transformation (2.28) as function of the angle θ. The fidelity between the input and output states are shown for the states (2.9) from the main circle; Eastern meridian (solid line) and Western meridian (dashed line).

space of the general copying machine (2.11). If we introduce the orthogonal basis $|0\rangle$ and $|1\rangle$ for this subspace, the transformation (2.14) can be brought into the form

$$\begin{aligned} |0\rangle\,|0\rangle\,|A\rangle &\longrightarrow \sqrt{\frac{2}{5}}\,|00\rangle\,(|0\rangle+|1\rangle)+\frac{1}{\sqrt{10}}\,(|01\rangle+|10\rangle)\,|0\rangle\;, \\ |1\rangle\,|0\rangle\,|A\rangle &\longrightarrow \sqrt{\frac{2}{5}}\,|11\rangle\,(|0\rangle+|1\rangle)+\frac{1}{\sqrt{10}}\,(|01\rangle+|10\rangle)\,|1\rangle\;, \end{aligned} \tag{2.28}$$

if the vectors (2.27) are substituted into the transformation (2.14). This makes our suggested QCM now explicit. The QCM (2.28) is optimal for a symmetric cloning of the states from the Eastern meridian by construction.

Substituting the parameters (2.26) into the formula for the input-output fidelity (2.20) for the states from the main circle, we obtain

$$F(\theta)=\;\frac{9}{10}-\frac{1}{5}\sin^2\theta\pm\frac{1}{5}\sin\theta\,. \tag{2.29}$$

Figure 2.2 displays the behavior of this fidelity for the two meridians of the main circle. While the fidelity is $F\geq 0.9$ for all states along Eastern meridian (associated with the $+$ sign in Eq. (2.29)), it drops quickly down up to $F=1/2$ for the $|-\rangle$ state along Western meridian. Along the Eastern part, that includes the three states $\{|0\rangle\,,|1\rangle\,,|+\rangle\}$ from above, however, a remarkably small variation of the fidelity with $0.9\leq F\leq 0.95$ occurs and may favor this region to produce quantum copies with high fidelity.

So far, we have considered input states from the main circle for the transformation (2.28). If we apply this transformation to other (pure) states from the Bloch sphere $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$ with $\phi \neq 0$, the fidelity

$$F(\theta,\phi) = \frac{9}{10} - \frac{1}{5}\sin\theta\,(\sin\theta - \cos\phi)\,, \tag{2.30}$$

becomes dependent on the angle ϕ also and makes the behavior slightly more complex. Although this particular dependence (2.30) of the fidelity was obtained from the request that the states from Eastern meridian can be copied in optimal way, a high-fidelity cloning is possible also for other regions on the Bloch sphere by making similar requirements for other meridians.

Of course, the meridional QCM given by the transformation (2.28) is not the one state dependent QCM. There is also another well known state dependent QCM which was originally proposed by Bruß *et al.* [102] and is known today as equatorial QCM. This QCM provides two copies of an equatorial pure qubit state (2.10) with maximal possible fidelity $F = 1/2 + \sqrt{1/8}$ and is given by the transformation

$$\begin{aligned}
|0\rangle|0\rangle|A\rangle &\longrightarrow a|0\rangle|0\rangle|0\rangle + \sqrt{\frac{1}{8}}\,(|0\rangle|1\rangle + |1\rangle|0\rangle)\,|1\rangle + b|1\rangle|1\rangle|0\rangle\,,\\
|1\rangle|0\rangle|A\rangle &\longrightarrow a|1\rangle|1\rangle|1\rangle + \sqrt{\frac{1}{8}}\,(|0\rangle|1\rangle + |1\rangle|0\rangle)\,|0\rangle + b|0\rangle|0\rangle|1\rangle\,,
\end{aligned} \tag{2.31}$$

where $a = 1/2 + \sqrt{1/8}$ and $b = 1/2 - \sqrt{1/8}$. In comparison to the universal (2.24) and meridional QCMs, this cloning transformation includes four terms in the right hand side. In spite of this, the four final-state vectors of the ancilla still span a two-dimensional subspace. It is also important to note that although transformation (2.31) was constructed for optimal copying of equatorial states, it remains the optimal cloning transformation for states from an arbitrary big circle of the Bloch sphere as it is follows from the symmetry of the sphere.

The concepts of universal and equatorial quantum coping have been already extended to $N \to M$ cloning transformations, i.e. when M copies are created from N input replicas of a pure qubit state. Explicit formulas for such universal and equatorial QCMs are rather complicated and, therefore, we do not show them here. For future discussion in sections 2.2 and 2.3, it is important to note that the copies from the universal $N \to M$ QCM have the fidelity

$$F^{u}_{N\to M} = \frac{N}{M} + \frac{(M-N)(N+1)}{M(N+2)} \tag{2.32}$$

in comparison to the input state [103]. Each copy, moreover, is in a mixed (so-called pseudo-pure) state of the form

$$\rho = \eta(N,M)\;|\psi\rangle\langle\psi| \;+\; \frac{1}{2}\,[1-\eta(N,M)]\,\mathbf{1}\,, \tag{2.33}$$

where $|\psi\rangle$ is the input state and where the shrinking factor is found to be $\eta(N,M) = (NM+2N)/(NM+2M)$.

Each copy from the equatorial $N \to M$ QCM is given again by the mixed pseudo-pure state (2.33), but with the shrinking factor

$$\eta(N,M) = 2^{M-N} \frac{\sum_{l=0}^{N-1} \sqrt{C_l^N C_{l+1}^N}}{\sum_{j=0}^{M-1} \sqrt{C_j^M C_{j+1}^M}}, \tag{2.34}$$

which is given in terms of the binomial coefficients C_α^β [102]. The fidelity of each copy is given by $F_{N\to M}^e = [1+\eta(N,M)]/2$.

Motivated by practical necessities, most cloning transformations were developed for input pure states. Recently, however, optimal universal $N \to M$ quantum cloning transformations for initially mixed states were suggested by Dang and Fan [104]. They showed, in particular, that pseudo-pure mixed qubit states can be copied equally as well as pure states in the sense that the shrinking factor is the same for both cases. This result allows us do not distinguish between pure and pseudo-pure mixed states in construction of optimal cloning transformations.

2.1.3 Application of quantum cloning machines in the eavesdropping of quantum communication

As we have already stated in the introduction, the no-cloning principle is the cornerstone of unconditional security of quantum communication. Although an eavesdropping of quantum communication between two partners, say Alice and Bob, is seriously restricted by the impossibility to copy exactly quantum information, the generation of approximate copies with a QCM gives opportunity to an eavesdropper, usually called Eve, to intercept some information about the secret message. It is therefore worth to know for both, the two partners who wish to communicate as well as for a potential eavesdropper, how much information can be extracted about the message within an attack with a QCM and what is the price (in terms of errors in the original message) of such extraction. The eavesdropping attack that maximize Eve's knowledge about the Alice-Bob message under a given error rate is called optimal.

The simplest strategy for eavesdropping is to intercept each qubit from the Alice-Bob communication channel independently from other transmitting qubits, provide two copies from the intercepted qubit, send one of the copies back in the communication channel and measure the remaining copy following the same procedure as Bob. Such an eavesdropping attack is called incoherent. In contrast, an attack, in which Eve interacts individually with the states sent by Alice but delay her measurement until the end of the transmission and then perform a collective measurements on the intercepted data, is called coherent.

Optimal incoherent attacks with QCM's have been found for several protocols for quantum communication. In particular, for BB84 protocol [31], in which only four states lying on $\pm x$ and $\pm y$ directions of the Bloch sphere are used for communication between Alice and Bob, the attack with an equatorial QCM was proven to be optimal [105]. Also, a universal QCM is optimal in the eavesdropping of the six-state protocol

[33], where states $\pm z$, $\pm x$ and $\pm y$ are used to encrypt the data. Although it has not been proven in general case, there are several evidences that coherent attack has a negligible advantage over incoherent strategy for protocols utilizing single-qubit states [46], such as BB84, B92 and the six-state protocol.

To provide an explicit example of an eavesdropping attack on a communication protocol, let us analyze with which success Eve may attack Bennett's B92 protocol [32] for quantum key distribution. In our analysis, moreover, we shall only focus on incoherent strategy. In the B92 protocol, only two nonorthogonal quantum states are utilized in order to encode and transmit the information about the cryptographic key. As usual, we suppose that the information is sent from Alice to Bob by means of a quantum communication channel. At the beginning of the protocol, Alice encodes each logical bit, 0 or 1, into two nonorthogonal states, that can be parameterized in a computational basis with a single real parameter ϑ [106] as

$$\begin{aligned} |u\rangle &= \cos\frac{\vartheta}{2}\,|0\rangle + \sin\frac{\vartheta}{2}\,|1\rangle\ , \\ |v\rangle &= \sin\frac{\vartheta}{2}\,|0\rangle + \cos\frac{\vartheta}{2}\,|1\rangle\ . \end{aligned} \tag{2.35}$$

The overlap of the states $O(\vartheta) \equiv |\,\langle u\,|\,v\rangle\,|^2 = \sin^2\vartheta$ gives the distance between states $|u\rangle$ and $|v\rangle$ in geometric sense. These qubits are then sent to Bob who performs a positive operator-valued measurement (POVM), and the best operators for that are

$$\begin{aligned} G_1 &= \frac{1}{1+\langle u\,|\,v\rangle}\ (\mathbf{1} - |u\rangle\,\langle u|)\ , \\ G_2 &= \frac{1}{1+\langle u\,|\,v\rangle}\ (\mathbf{1} - |v\rangle\,\langle v|)\ , \\ G_3 &= \mathbf{1} - G_1 - G_2\,. \end{aligned} \tag{2.36}$$

Only measurements with POVM elements G_1 and G_2 are conclusive, because certain decision about the received state $|u\rangle$ or $|v\rangle$ can be made after the measurement. After all the qubits have been sent (and measured), Bob tells to Alice numbers of conclusive measurements via a public channel, which can be monitored but not modified by Eve. Only those bits (obtained in Bob's conclusive measurements) can be used to construct the key, while all the rest need to be discarded because no definite conclusion can be drawn from the outcome of Bob's measurement. To test and recognize a (possible) eavesdropper, Alice and Bob compare the values of some of their bits via the public channel in order to get an estimate how likely their communication was disturbed.

To quantify the disturbance in the transmission of a single qubit, a convenient measure is the probability that Alice and Bob detect an error. If Bob would know a state $|\psi\rangle$ of one or several qubits in advance, that were sent to him by Alice, he could easily test for a possible eavesdropping attack. In this case, he will receive in general the qubits no longer in a pure but a mixed state that has to be described in terms of its density matrix ρ. The *discrepancy* that is detected by Bob is given by

$$D \;=\; 1 \;-\; \langle\psi\,|\,\rho|\psi\rangle\ . \tag{2.37}$$

Since Bob knows the maximal discrepancy D_{max} for the given channel (due to the incomplete quantum control of the given transmission), he could recognize an eavesdropping attack for $D > D_{max}$ and discard the key accordingly.

A central question for Eve is of how much information can be extracted from the transmission of the key if the disturbance due to the attack is $D < D_{max}$. From the initial agreement between Alice and Bob about the basis states which are to be chosen randomly, Eve knows that Alice prepares the qubits in one of the two states (2.35) with probability $p_i = 1/2$ $(i = 0, 1)$. Before Eve has measured a given qubit, her (degree of) ignorance is given by Shannon's entropy $H = -\sum p_i \log_2 p_i = -\log_2(1/2)$ [3]. After the measurement, the knowledge about the system increases by decreasing this entropy, a measure that is called the mutual information that Eve has acquired due to the measurement. Of course, Eve will try to obtain as much information as possible keeping the discrepancy $D < D_{max}$.

Let us suppose that Eve performs incoherent attack on the communication channel with a QCM. Here, we shall not yet specify the QCM explicitly in order to enable us to compare different QCM's below. As output of the cloning transformation, Eve obtains two copies of one of the two possible states $\rho_{|u\rangle}$ and $\rho_{|v\rangle}$ which just correspond to the two input states (2.35) with a fidelity as defined by the given QCM. To calculate the mutual information between Alice and Eve that is to be extracted from the eavesdropping, we can follow the procedure as described by Peres [107]. Using the POVM elements (2.36), the probability for Eve to obtain the outcome μ is

$$P_{\mu i} = \mathrm{Tr}(G_\mu \rho_i)\,, \tag{2.38}$$

and where the operators ρ_i refer to the two possible states $\{\rho_{|u\rangle}, \rho_{|v\rangle}\}$ of her copy. After the measurement, when she has obtained a particular outcome μ, the posterior probability $Q_{i\mu}$ that ρ_i was prepared by Alice is

$$Q_{i\mu} = \frac{P_{\mu i} p_i}{q_\mu}\,, \tag{2.39}$$

where $q_\mu = \sum_j P_{\mu j} p_j$, and $p_j = 1/2$ is the probability for sending the states $|u\rangle$ and $|v\rangle$ within the B92 protocol. With these probabilities, the Shannon entropy (which was $H = -\log_2(1/2) = 1$ initially), becomes

$$H_\mu = -\sum_i Q_{i\mu} \log Q_{i\mu}\,, \tag{2.40}$$

once the result μ was obtained, and hence the mutual information is

$$I = H - \sum_\mu q_\mu H_\mu\,. \tag{2.41}$$

To determine the possible success of an eavesdropper, we only need to analyze the explicit form of the output states $\rho_{|u\rangle}$ and $\rho_{|v\rangle}$ for a particular QCM. By substituting the output states into Eqs. (2.41) and (2.37) we may then calculate the mutual information and discrepancy in case of an eavesdropping with the QCM. Since we

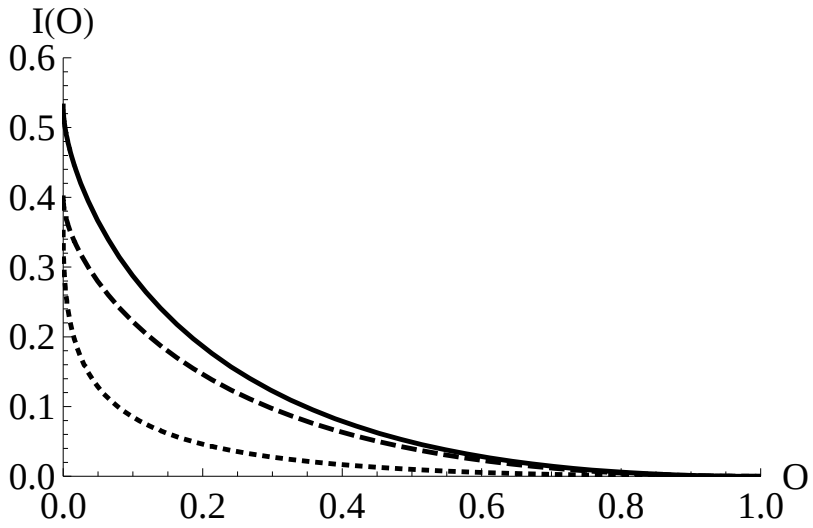

Figure 2.3: The mutual information between Alice and Eve $I(O)$ as function of the overlap O of the states (2.35) for eavesdropping with meridional (solid), equatorial (dashed) and universal (dotted) QCM's.

assumed that the copies from the QCM are identical (i.e symmetric), the mutual information extracted by Eve I_{AE} equals to the mutual information obtained by Bob in his measurements $I_{AB} = I_{AE} \equiv I$. As it is seen from Eqs. (2.38)-(2.40), moreover, this information depends on the overlap of the states (2.35).

If Eve applies universal QCM (2.24), which provides copies with fidelity $F = 5/6$, she causes discrepancy $D = 1/6 \approx 0.17$ independently from the choice of the states (2.35). The mutual information extracted by Eve is given in Fig. 2.3 with dotted line. For equatorial QCM (2.31) with the fidelity $F = 1/2 + \sqrt{1/8}$ of the copies, discrepancy equals $D = 1/2 - \sqrt{1/8} \approx 0.15$ for arbitrary states (2.35) and the mutual information is shown in Fig. 2.3 with dashed line. For the eavesdropping with meridional QCM discrepancy depends on particular choice of the states (2.35) and is given by $0.05 \leq D \leq 0.10$. The mutual information in this case is shown in Fig. 2.3 with solid line. Consequently, our suggested QCM introduces a lower disturbance into the data transmission between Alice and Bob than it is caused by universal or equatorial QCM's. It also enables Eve to extract in course of her eavesdropping more information than obtained by means of these two QCM's. Thus, the incoherent eavesdropping attack on B92 protocol with meridional QCM is optimal.

As the final remark, we like to note that modern channels for quantum communication have discrepancy less than $D < 0.03$. This implies that even an eavesdropping with meridional QCM would be easily found out by the legitime users. To remain undetected Eve may, for example, intercept just a part of the transmitted message, acquiring nevertheless some information. However, even if the eavesdropping was not detected directly by observing discrepancy, Eve's information about the message can be always reduced to zero by the legitime users. This can be done with the help

of security amplification protocols [3], which require additional comparison of Alice's and Bob's bits through the public channel, i.e. waste of transmitted data. The estimation of Eve's information, that can be intercepted by an optimal eavesdropping attack remaining below the detection value for discrepancy, allows the legitime users to spend minimal amount of data to ensure security of their communication.

2.2 State independent transformations

Having established the fundamental features of quantum copying, we eventually come to a more general problem: 'what is the optimal way to perform a quantum transformation with given properties on unknown quantum states?' Here we like to underline that we are only interested in those quantum transformations which do not depend on input states, i.e. are input state independent. In order to explain the notion of state independent transformation it is useful to consider a particular example.

Suppose, we are given a single qubit in an unknown state $|\psi\rangle$. We desire to find a quantum transformation that generates from the input state $|\psi\rangle$ the orthogonal state $\left|\psi^{\perp}\right\rangle$ independently on the input state, so that $\left\langle\psi \mid \psi^{\perp}\right\rangle \equiv 0$. A possible candidate for such an 'inversion' transformation is the Pauli matrix σ_x which can be written in a computational basis as $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. Indeed, applying the σ_x to basis states $|0\rangle$ and $|1\rangle$ of the qubit, we obtain the desired inversion, i.e. $\sigma_x|0\rangle = |1\rangle$ and $\sigma_x|1\rangle = |0\rangle$. However, if σ_x is applied to a superposed state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the output state $|\psi'\rangle = \beta|0\rangle + \alpha|1\rangle$ is not orthogonal to the input state in general case, i.e $\langle\psi \mid \psi'\rangle = \beta\alpha^* + \alpha\beta^* \neq 0$. Therefore the σ_x does not provide us with the desired state inversion transformation for an arbitrary input state of qubit. In fact, as we will see in the next section, the exact inversion transformation can not be constructed for an arbitrary state of qubit.

Independence of a quantum transformation from input states implies that this transformation is basis independent, i.e. it remains invariant with regard to a basis change. Indeed, if an operation given by quantum transformation does not depend on input states, a basis transformation, which simply maps all qubit states to themselves, do not act on this operation. In fact, it is very convenient to use the requirement of basis invariance to construct state independent transformations with given properties.

2.2.1 Single-qubit transformations

The simplest case of state independent transformation is, of course, single-qubit transformation. Let us consider in more details the state inversion transformation or, as it is called sometimes, universal NOT operation [108, 109]. As we have already mentioned, this operation generates the orthogonal state $\left|\psi^{\perp}\right\rangle$ at the output from a given unknown input state $|\psi\rangle$. Since the input state is, in general, a superposition of basis states $|0\rangle$ and $|1\rangle$, the universal NOT operation should generate the state

$$\left|\psi^{\perp}\right\rangle = \mathrm{NOT}\left(\alpha|0\rangle + \beta|1\rangle\right) = \beta^*|0\rangle - \alpha^*|1\rangle \ , \tag{2.42}$$

in order to ensure that $\langle\psi\,|\,\psi^{\perp}\rangle \equiv 0$ for an arbitrary input state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ as it is required. This operation, however, can not be implemented exactly on real quantum systems, since it is not a completely positive map. Nevertheless, the universal NOT operation can be provided approximately as it was shown by Bužek *et al.* [108] and is given by the unitary transformation

$$|\psi\rangle\,|A\rangle \longrightarrow \sqrt{\frac{2}{3}}\,|\psi^{\perp}\rangle\,|A_{\psi^{\perp}}\rangle \;+\; \sqrt{\frac{1}{3}}\,|\psi\rangle\,|A_{\psi}\rangle\;, \tag{2.43}$$

where $|A\rangle\,, |A_{\psi^{\perp}}\rangle$ and $|A_{\psi}\rangle$ are the state vectors of a four-dimensional auxiliary system. The fidelity between the approximate output of the transformation (2.43) and the ideal output $|\psi^{\perp}\rangle$ equals $F_{\mathrm{NOT}} = 2/3$. More generally, a universal NOT operation can be constructed for an ensemble of N input qubits that are prepared in an unknown qubit state $|\psi\rangle$ [108]. This operation can be performed approximately on the ensemble with fidelity $F = \langle\psi^{\perp}\,|\,\rho|\psi^{\perp}\rangle = (N+1)/(N+2)$ between the approximate output ρ of the transformation and the ideal output $|\psi^{\perp}\rangle$.

Interestingly enough the exact state inversion transformation exists for an arbitrary qubit state taken from a chosen one-dimensional subspace of the original two-dimensional qubit state space [110]. Using the Bloch sphere representation of the qubit state, a one-dimensional subspace can be visualized with a big circle which is given by the intersection of the sphere with a plane. For an arbitrary qubit state from the main circle (2.9), for example, the state inversion operation is given by

$$\mathrm{NOT}_{\mathrm{mc}} = -i\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\,. \tag{2.44}$$

Knowing the state inversion operations for an arbitrary state of qubit (2.43) and for (real) states from the main circle (2.44), we can in principle construct an arbitrary single-qubit state independent transformation for qubit. For real qubit states, for instance, any state independent transformation can be expressed as

$$U(\xi) \equiv \cos\frac{\xi}{2}\,I + \sin\frac{\xi}{2}\,\mathrm{NOT}_{\mathrm{mc}}\,, \tag{2.45}$$

where I is the identity matrix and ξ is a real free parameter $0 \le \xi \le \pi$. This gate (2.45) performs a rotation of the input qubit state (vector) on the angle ξ in the main circle independently on the input state. An input state independent Hadamard gate [93], that creates an equal superposition of a real qubit and its orthogonal, corresponds to the rotation $U(\pi/2)$.

2.2.2 Two-qubit Controlled-NOT transformation

In quantum information processing we are not restricted by single-qubit operations, but interested mostly in optimal state independent transformations of multiqubit systems. In fact, we have already seen the trivial examples of two-qubit state independent transformations: the $(1 \to 2)$ universal (2.24), meridional (2.28) and equatorial

(2.31) QCM's. Indeed, these transformations enables one to distribute information about an input qubit state between two qubits. The straightforward generalization of cloning transformation is state independent controlled unitary operation (2.6) that transmits information about the state $|\psi\rangle$ of the input qubit to the reference qubit state $|R\rangle$ by means of a conditional unitary transformation $|U(\psi)R\rangle$.

Although, due to the general impossibility theorem, the transformation (2.6) can not be perfectly realized, it is possible to construct an optimal approximation for this transformation. Let us construct a particular example of state independent controlled unitary transformation – Controlled-NOT operation. By analogy with classical information processing, the quantum C-NOT operation is defined to act on two qubits, one of which is called control and the other target. By definition, the quantum C-NOT operation leaves the meaning of the target qubit unchanged, if the control qubit is given in the state $|0\rangle$; if the control qubit is in the state $|1\rangle$, the NOT operation is to be performed on the target qubit, i.e.

$$\begin{aligned} |0\rangle_c \otimes |R\rangle_t \otimes |A\rangle &\longrightarrow |0\rangle_c \otimes |R\rangle_t \otimes |A_0\rangle \ , \\ |1\rangle_c \otimes |R\rangle_t \otimes |A\rangle &\longrightarrow |1\rangle_c \otimes (\mathrm{NOT}\,|R\rangle_t) \otimes |A_1\rangle \ . \end{aligned} \tag{2.46}$$

where we introduced an auxiliary system to keep the discussion as general as possible.

Based on the definition (2.46), the C-NOT operation is usually defined in a computational basis as [3]

$$U_{\mathrm{C-NOT}} = |0\rangle\langle 0|_c \otimes I_t + |1\rangle\langle 1|_c \otimes (\sigma_x)_t \, , \tag{2.47}$$

where $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. However, this operation is not input state independent. If the state of the control qubit is in one of the basis states $|0\rangle$ or $|1\rangle$, the C-NOT operation (2.47) satisfies indeed the definition (2.46) leaving the states of the control and the target qubit separable. If, in contrast, the control qubit is in a superposed state, this operation (2.47) acts to the input qubit differently creating entanglement between the control and the target qubits.

In contrast to the definition (2.47), the input state independent C-NOT operation should act alike on the basis and superposed states of input qubit, always leaving the states of the control and the target qubits separable. Indeed, a superposed state of the control qubit in a given basis can be always transformed in one of the basis states into a new basis by means of a basis transformation. In this new basis the output states of the control and the target qubits are separable according to the definition (2.46). On the other hand, the state independent C-NOT operation should be invariant with regard to a basis transformation as we required earlier. Therefore, for a given superposed input state of the control qubit, the output states of the control and the target qubits should be separable.

The state independent single-qubit NOT operation is an essential part of the state independent C-NOT operation, as it is seen from the definition (2.46). The approximate character of the universal NOT operation (2.43), however, complicates construction and interpretation of the universal C-NOT operation. In order to simplify our discussion, let us focus on construction of the input state independent C-NOT

operation, when input states of both the control and the target qubits belong to a one-dimensional subspace of the two-dimensional qubit state space. As we have seen in the previous section, for qubit states from the one-dimensional subspace the exact state independent NOT operation is available. Suppose, for instance, that the input states of the control and the target qubits belong to the main circle of the Bloch sphere. Let us introduce the following notations for these qubits

$$|\psi_{\pm}\rangle_c = \cos\frac{\theta}{2}\,|0\rangle_c \pm \sin\frac{\theta}{2}\,|1\rangle_c\,, \tag{2.48}$$

$$|\chi_{\pm}\rangle_t = \cos\frac{\phi}{2}\,|0\rangle_t \pm \sin\frac{\phi}{2}\,|1\rangle_t\,, \tag{2.49}$$

where $|\psi_{\pm}\rangle_c$ and $|\chi_{\pm}\rangle_t$ denote the states of the control and the target qubits respectively. According to the definition (2.46), for the input states $|0\rangle_c$ and $|1\rangle_c$ of the control qubit, the state independent C-NOT operation should perform the unitary transformation

$$\begin{aligned} |0\rangle_c \otimes |\chi_{\pm}\rangle_t \otimes |A\rangle &\longrightarrow |0\rangle_c \otimes |\chi_{\pm}\rangle_t \otimes |A_0\rangle\,, \\ |1\rangle_c \otimes |\chi_{\pm}\rangle_t \otimes |A\rangle &\longrightarrow |1\rangle_c \otimes \left|\chi_{\pm}^{\perp}\right\rangle_t \otimes |A_1\rangle\,. \end{aligned} \tag{2.50}$$

As before, the state vectors $|A\rangle$, $|A_0\rangle$ and $|A_1\rangle$ denote the initial and the final states of the auxiliary system. The output state $\left|\chi_{\pm}^{\perp}\right\rangle_t$ is orthogonal to the input target qubit state $|\chi_{\pm}\rangle_t$ and is obtained by applying the NOT operation (2.44) to the input state (2.49), i.e. $\left|\chi_{\pm}^{\perp}\right\rangle_t = \mathrm{NOT}_{\mathrm{mc}}\,|\chi_{\pm}\rangle_t$. If the state of the control qubit is given in the superposed state (2.48), the universal unitary C-NOT transformation should leave the states of the control and the target qubits separable while performing some transformation $f(\psi,\chi)$ on the target qubit, i.e.

$$|\psi\rangle_c \otimes |\chi\rangle_t \otimes |A\rangle \longrightarrow |\psi\rangle_c \otimes |f(\psi,\chi)\rangle_t \otimes |A_{\psi}\rangle\,, \tag{2.51}$$

where the function $f(\psi,\chi)$ is related to the original state $|\chi\rangle_t$ by a unitary transformation $|f(\psi,\chi)\rangle_t = U(\psi)\;|\chi\rangle_t$. On the other hand, making a superposition of Eqs. (2.50) we obtain

$$\begin{aligned} &\left(\cos\frac{\theta}{2}\,|0\rangle_c + \sin\frac{\theta}{2}\,|1\rangle_c\right) \otimes |\chi_{\pm}\rangle_t \otimes |A\rangle \longrightarrow \\ &\cos\frac{\theta}{2}\;|0\rangle_c \otimes |\chi_{\pm}\rangle_t \otimes |A_0\rangle \;+\; \sin\frac{\theta}{2}\;|1\rangle_c \otimes \left|\chi_{\pm}^{\perp}\right\rangle_t \otimes |A_1\rangle\,. \end{aligned} \tag{2.52}$$

Let us analyze this superposition (2.52) in order to specify the function $f(\psi,\chi)$ in the transformation (2.51). Suppose one has two qubits prepared in the states $|\psi_0\rangle_c = \cos\frac{\theta_0}{2}\,|0\rangle_c + \sin\frac{\theta_0}{2}\,|1\rangle_c$ and $|\chi_0\rangle_t$ respectively. If one performs the transformation (2.52) on them, so that the qubit $|\psi_0\rangle_c$ is the control and the qubit $|\chi_0\rangle_t$ – the target, the two-qubit state

$$\cos\frac{\theta_0}{2}\;|0\rangle_c \otimes |\chi_0\rangle_t \;+\; \sin\frac{\theta_0}{2}\;|1\rangle_c \otimes \left|\chi_0^{\perp}\right\rangle_t\,, \tag{2.53}$$

is obtained at the output, as it follows from Eqs. (2.50) and (2.52). Making a projective measurement on the target qubit in the $\{|\chi_0\rangle_t, |\chi_0^{\perp}\rangle_t\}$ basis, one obtains the outcomes $|\chi_0\rangle_t$ and $|\chi_0^{\perp}\rangle_t$ with probabilities $\cos^2\frac{\theta_0}{2}$ and $\sin^2\frac{\theta_0}{2}$ respectively. Therefore, we conclude that the universal C-NOT operation (2.51) is to have the following structure

$$|\psi_+\rangle_c \otimes |\chi_\pm\rangle_t \otimes |A\rangle \longrightarrow |\psi_+\rangle_c \otimes \left(\cos\frac{\theta}{2}|\chi_\pm\rangle_t + \sin\frac{\theta}{2}|\chi_\pm^{\perp}\rangle_t\right) \otimes |A_\psi\rangle \ , \quad (2.54)$$

On the right hand side of this transformation (2.54), the control qubit is left without changes as is required by Eq. (2.51) while the unitary transformation

$$U(\psi) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad (2.55)$$

is to be performed on the target qubit $|\chi\rangle_t$. After simple algebraic manipulation we find that the state independent C-NOT operation can be written as

$$\begin{aligned} &|\psi_+\rangle_c \otimes (\cos\frac{\phi}{2}|0\rangle_t \pm \sin\frac{\phi}{2}|1\rangle_t) \otimes |A\rangle \longrightarrow \\ &|\psi_+\rangle_c \otimes (\cos\frac{\phi-\theta}{2}|0\rangle_t \pm \sin\frac{\phi-\theta}{2}|1\rangle_t) \otimes |A_\psi\rangle \ , \end{aligned} \quad (2.56)$$

where we have shown the states of the target qubit before and after the transformation explicitly. The transformation (2.56) leaves the control qubit without changes and rotates the target qubit on the angle θ clockwise. We note that if the state of the control qubit is given in the state $|\psi_-\rangle_c$, the transformation (2.56) rotates the target qubit counterclockwise to the angle θ. It is also remarkable that the state of the output target qubit depends only on the difference $\phi - \theta$ and does not depend on a particular basis (as it should be for a basis/state independent transformation).

The transformation (2.56) introduces the 'idealized' state independent C-NOT operation which can not be perfectly realized due to the general impossibility theorem (2.6). As in the case of quantum cloning transformations considered in section 2.1.2, it is, however, possible to construct an optimal approximation for the C-NOT operation. Formally, the procedure of such a construction is identical to the construction of optimal cloning transformations: one should consider again the most general unitary transformation of two qubits (2.11) subordinated to the conditions (2.13), introduce free parameters of this transformation, define single copy fidelity (2.8) as function of the parameters and optimize the fidelity function using, for example, the numerical method (2.21). Since the procedure of construction of an optimal cloning transformation has been discussed in details in section 2.1.2, we skip here the derivation of the approximate C-NOT operation and focus on the discussion of the result.

The optimal approximation for the state independent C-NOT operation for real

input states (2.51) is given by the transformation

$$|0\rangle_c|\chi_\pm\rangle_t|A\rangle \longrightarrow \left(\frac{1}{2}+\sqrt{\frac{1}{8}}\right)|0\rangle_c|\chi_\pm\rangle_t|0\rangle$$
$$+\sqrt{\frac{1}{8}}\left(|0\rangle_c|\chi_\pm^\perp\rangle_t+|1\rangle_c|\chi_\pm\rangle_t\right)|1\rangle + \left(\frac{1}{2}-\sqrt{\frac{1}{8}}\right)|1\rangle_c|\chi_\pm^\perp\rangle_t|0\rangle\,,$$
$$|1\rangle_c|\chi_\pm\rangle_t|A\rangle \longrightarrow \left(\frac{1}{2}+\sqrt{\frac{1}{8}}\right)|1\rangle_c|\chi_\pm^\perp\rangle_t|1\rangle$$
$$+\sqrt{\frac{1}{8}}\left(|0\rangle_c|\chi_\pm^\perp\rangle_t+|1\rangle_c|\chi_\pm\rangle_t\right)|0\rangle + \left(\frac{1}{2}-\sqrt{\frac{1}{8}}\right)|0\rangle_c|\chi_\pm\rangle_t|1\rangle\,. \quad (2.57)$$

For this transformation, the fidelity between the ideal output and the actual output for the states of the control as well as the target qubits equals $F=1/2+\sqrt{1/8}$ and is constant for arbitrary input states of the control and target qubits taken from the main circle of the Bloch sphere.

The transformation (2.57) has similar structure to the equatorial QCM (2.31). This similarity has an important implication. The 'idealized' C-NOT transformation (2.56) can be formally treated as a two-stage transformation. The first stage of the device provides the cloning transformation on the input control qubit, the second stage rotates the state vector of the copy in the main circle over the angle ϕ which describes the state of the target qubit. While the first stage (cloning) transformation is strongly restricted by the no-cloning principle, there are no limitations on the second stage transformation. Thereby the problem to find an optimal C-NOT transformation for the input states of the qubits taken from the main circle reduces to a search for the optimal cloning transformation for such input states. Since equatorial QCM is the optimal cloning transformation for the input states from equator and from any big circle on the Bloch sphere, it is not surprising that the optimal state independent C-NOT transformation (2.57) has structure similar to equatorial QCM.

2.2.3 Multiqubit Controlled-U transformations

Having discussed in details the particular example of state independent controlled unitary transformation, the Controlled-NOT operation for real qubit states, we can now analyze the general case of such transformation. Let us construct the optimal approximation for two-qubit controlled unitary transformation

$$|\psi\rangle_c\otimes|\chi\rangle_t\otimes|A\rangle \longrightarrow |\psi\rangle_c\otimes U(\psi)|\chi\rangle_t\otimes|A_\psi\rangle\,. \quad (2.58)$$

without making any initial assumptions about the input states and the unitary that is to be applied to the target qubit. As we mentioned before, the trivial controlled unitary transformation is the $(1\rightarrow 2)$ cloning transformation

$$|\psi\rangle_c\otimes|0\rangle_t\otimes|A\rangle \longrightarrow |\psi\rangle_c\otimes|\psi\rangle_t\otimes|A_\psi\rangle\,. \quad (2.59)$$

This transformation can be realized approximately with the help of the universal QCM (2.24) with optimal fidelity $F = 5/6$ between the input state and each copy. In fact, not only transformation (2.59) but also an arbitrary transformation

$$|\psi\rangle_c \otimes |0\rangle_t \otimes |A\rangle \quad \longrightarrow \quad |\psi\rangle_c \otimes U(\psi)\,|0\rangle_t \otimes |A_\psi\rangle \tag{2.60}$$

can be performed approximately with the optimal fidelity $F = 5/6$ between each of the ideal outputs $|\psi\rangle_c$ and $U(\psi)\,|0\rangle_t$ in right hand side and the corresponding actual results of the transformation. Indeed, any transformation $U(\psi)\,|0\rangle_t$ can be obtained as a sequence of copying $|0\rangle_t \to |\psi\rangle_t$ (2.59) and a unitary transformation of the copy $U\,|\psi\rangle_t$. While the transformation of the copy $U\,|\psi\rangle_t$ is not restricted by the laws of quantum mechanics, the efficiency of the optimal transformation (2.60) is completely defined by the efficiency of the optimal cloning. Moreover, there is a freedom in choice of the initial 'blank' state of the target qubit. Consequently, any two-qubit Controlled-U transformation (2.58) on arbitrary input qubit states can be provided approximately with the optimal fidelity $F = 5/6$ between the ideal outputs and the corresponding actual outputs of the transformation.

This result can be further extended to the case of input qubit states taken from some restricted set of states. As we have seen in the previous section, the efficiency of the optimal C-NOT transformation for input real qubit states is defined by the efficiency of the corresponding cloning transformation for these states. This statement remains true for an arbitrary Controlled-U transformation for input states taken from a restricted set: the efficiency of this transformation is defined by the corresponding optimal cloning transformation.

By analogy with two-qubit Controlled-U transformation (2.58), we may consider a multiqubit transformation

$$|\psi\rangle_c^{\otimes N} \otimes |\chi\rangle_t^{\otimes K} \otimes |A\rangle \longrightarrow |\psi\rangle_c^{\otimes N} \otimes \left(U(\psi)\,|\chi\rangle_t\right)^{\otimes K} \otimes |A_\psi\rangle\ , \tag{2.61}$$

where a unitary is to be applied to K target qubits in presence of N control qubits. Following the same logic as in case of two-qubit transformation (2.58), we obtain that the efficiency of this multiqubit transformation (2.70) is completely defined by efficiency of $N \to N + K$ quantum cloning transformation. In particular, the fidelity between the ideal and the approximate outputs of the transformation (2.70) for an arbitrary input states is given by Eq. (2.32). For input real qubit states, in contrast, the fidelity of state independent multiqubit controlled-U transformation equals $F^e_{N\to N+K} = [1 + \eta(N, N + K)]/2$, where $\eta(N, N + K)$ is given by Eq. (2.34).

2.2.4 Application of state independent transformations in quantum computing

Apart of academic interest, single- and multiqubit state independent transformations may have applications in quantum communication and quantum computing. Leaving aside speculations about usefulness of state independent transformations in quantum communication, we like to analyze especially how these transformations can be used

in quantum computing. On the first glance the answer is evident: using state independent transformations we can construct a quantum circuit [3] to realize quantum computation. But, whether such a quantum circuit has any advantages comparing to a circuit constructed from usual basis dependent operations? Yes indeed, as we will see.

In general, a quantum computer is a device that runs a program through a carefully controlled sequence of unitary operations (and/or measurements) applied to initially prepared states of quantum systems. The answer is stored as classical information that can be read out with high probability by a measurement. To be more specific in definition of quantum computer, DiVincenzo formulated the five requirements for the architecture and physical implementation of a quantum computer [111], such as:

- *Scalability.* A scalable physical system with well characterized parts, usually qubits – two-level quantum systems, is available.
- *Initialization.* It is possible to prepare the system in a simple state, such as $|00...0\rangle$.
- *Control.* Control of a quantum computation is accomplished via some universal set of elementary unitary operations.
- *Stability.* The system has long relevant decoherence time, much longer than times of elementary transformations.
- *Measurement.* It is possible to read out the state of the computer in a convenient product basis.

If a quantum computer satisfies the five requirements above, it is called a scalable quantum computer (SQC). For such a computer, moreover, the entanglement of pure multiqubit states is proven to be necessary to support computational advantages of the quantum computer comparing to the classical one [14, 18].

However, first experiments on realization of SQC [112, 113, 114] faced many difficulties mostly connected to the control and the stability of the quantum systems. Indeed, real quantum systems are rarely in pure states and continuously interact with their environments which lead to non-unitary (uncontrolled and unstable) evolution. Furthermore, the proposals and experiments using nuclear magnetic resonance (NMR) at high temperature to study quantum computation [114] involve manipulations with initially mixed states giving rise to the problem of the initialization of the system. Since fully controllable, scalable and "initializable" quantum computers are still quite a way in the future, a less ambitious quantum processor, that may fail to satisfy one or more of the five criteria above but can nonetheless carry out interesting computations, is of great interest.

A particular paradigm for quantum computation which is different from SQC is quantum computation with initially mixed states. Quantum computer that breaks the second (initialization) requirement and operates with mixed states is recognized to

be an intermediate model for quantum computation that lies somewhere in between classical computers and SQCs [18]. The first investigation of the power of such a quantum computer was presented by Knill and Laflamme [115], who discussed deterministic quantum computation with just one qubit in an initially mixed state. The computation with the mixed state was shown to be less powerful than SQC. However, it was shown that some problems related to physical simulations, for which no efficient classical algorithms are known, can be solved with its help.

The analysis of efficiency of quantum computation with initially mixed states was performed for standard quantum algorithms. In particular, it was shown by Palma with co-authors [116] that mixedness of the initial states decreases the probability of successful computation of Shor's algorithm exponentially with the length of input data. This result implies that the computation of Shor's algorithm with initially mixed states has an exponentially small advantage over classical computation. Similar result was obtained by Braunstein and Pati for Grovers algorithm: the computational speed-up using mixed states is not possible except, however, for the special case of the search space of size four [17].

Quite recently, nevertheless, Biham *et al.* [15] analyzed how fast the Deutsch-Jozsa and the Simon problems can be implemented with a quantum computer operating with initially mixed states. It was found that these quantum algorithms can be implemented more reliably by means of quantum computing with mixed states then by the best possible classical algorithm. For an arbitrary pure N-qubit state $|\psi\rangle$ and real (purity) parameter $0 \leq \epsilon \leq 1$, it was proven that quantum computation with the *pseudo-pure* state

$$\rho = \epsilon \left|\psi\right\rangle \left\langle\psi\right| + (1-\epsilon) I^{\otimes N}\,, \tag{2.62}$$

where I denotes the identity operator, guarantees a speed-up over classical algorithms even when the purity parameter ϵ is arbitrarily close to zero. However, the speed-up of the quantum algorithms rapidly decrease with the number of qubits involved in the computation. Although the question of the existence of a non-vanishing advantage of quantum computing with mixed states is still open [14, 15], there is no doubt that this type of quantum computing may support classically unavailable information processing.

Keeping in mind quantum algorithms for which quantum computation with initially mixed states have advantages compared to classical computation, let us analyze how these algorithms can be implemented, at least in principle, using quantum circuits constructed from single- and multiqubit transformations. To be more precise, let us assume that the given input states are pseudo-pure. The well-known property of single-qubit unitary transformations is that they do not change the purity parameter of the input mixed state (2.62), if applied to a single qubit state [15], i.e.

$$U\rho U^{\dagger} = U\left(\epsilon \left|\phi\right\rangle \left\langle\phi\right| + (1-\epsilon) I\right) U^{\dagger} = \epsilon\, U \left|\phi\right\rangle \left\langle\phi\right| U^{\dagger} + (1-\epsilon) I\,. \tag{2.63}$$

As it is seen from Eq. (2.63), there is no loss of information, if a single qubit transformation is applied to an input pseudo-pure state. This statement is completely general and covers both cases of basis dependent and basis independent transformations.

Therefore, from the viewpoint of their efficiency, basis independent transformations do not differ from basis dependent transformations, if applied to a single qubit.

For multiqubit systems, however, there is a crucial difference in resulting states from basis dependent and basis independent transformations if they are applied to pseudo-pure input states. The simplest example is the two-qubit Controlled-NOT transformation. As we mentioned before the standard basis dependent C-NOT transformation is given by Eq. (2.47). This transformation creates entanglement between initially separable input (pure) states of control and target qubits, if the control qubit is given in a superposed state of the basis states $|0\rangle_c$ and $|1\rangle_c$. For instance, if the input control and target qubits are given in the states $|+\rangle_c = \sqrt{1/2}(|0\rangle + |1\rangle)$ and $|0\rangle_t$ respectively, the output state is the maximally entangled (Bell) state $|\phi\rangle = \sqrt{1/2}(|00\rangle + |11\rangle)$ of two qubits.

Suppose, the input states of the control and the target qubits are not pure anymore but pseudo-pure. Assume, for simplicity, that the input state of the control qubit is given by $\rho_c = \epsilon\,|+\rangle\langle+| + (1-\epsilon)I$ while the input state of the target qubit is $\rho_t = \epsilon\,|0\rangle\langle 0| + (1-\epsilon)I$ with an equal purity parameter ϵ. Applying the C-NOT gate (2.47) to the input qubits in the mixed states, let us analyze how rapid the entanglement of the output two-qubit state decreases with regard to the purity ϵ of the input states. To quantify entanglement of the output two-qubit state we use an entanglement measure, concurrence, as it was presented in section 1.2.3. Using Eq. (1.26), we found that the concurrence for the output two-qubit state decreases with the purity parameter as $C = \max\{0,\, 1/2(\epsilon^2+2\epsilon-1)\}$. While it is often required to apply the C-NOT gate (2.47) many times during a computation, the significant loss of entanglement of the output state after a single C-NOT operation makes impossible an effective quantum computation with input mixed states and with basis dependent transformations. Moreover, the computation with pseudo-pure states is not possible at all for the input states with the purity $\epsilon < 0.414$, since the concurrence for the output two-qubit state from the C-NOT gate vanishes.

A completely different situation appear, if we apply state independent C-NOT transformation (2.57) to input pseudo-pure states. As we have proven in section 2.2.3, efficiency of this state independent transformation is completely defined by the efficiency of the corresponding cloning transformation. Each copy from the cloning transformation is in pseudo-pure state (2.33), if the input states are pure. It is easy to check that for input mixed states (2.62), the copies are also in pseudo-pure states (2.33) but with the shrinking factor $\epsilon\,\eta(1,2)$. This implies that applying the state independent transformations to initially mixed states is equivalent to the shrinking of the Bloch sphere representing these states by factor $\eta(1,2)$. The shrinking, moreover, does not depend on the initial purity ϵ of the input states. This indifference in action with regard to the purity of the input mixed states is the advantage of state independent transformations in comparison to state dependent transformations.

Unfortunately, it is not possible to use the state independent C-NOT transformation (2.57) in realistic quantum computation. The reason for that is significant shrinking of the Bloch sphere representing the input states and, as consequence, low input-output fidelity $F = 1/2 + \sqrt{1/8}$ of this transformation. There is, however, a

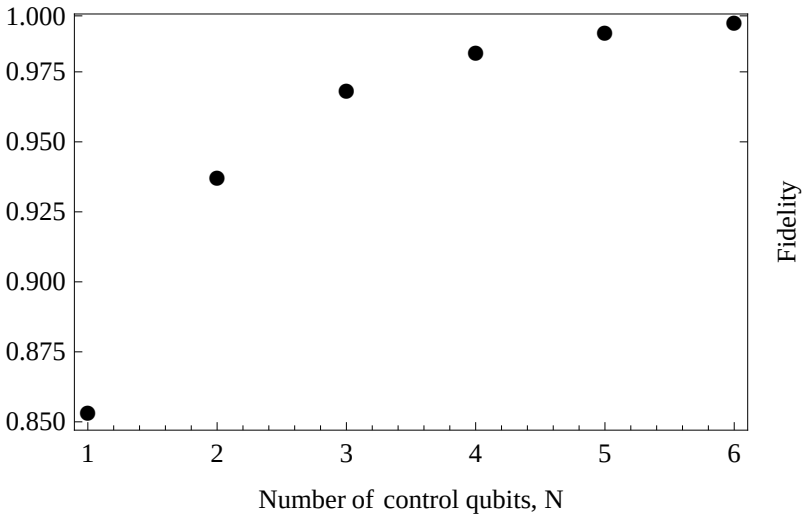

Figure 2.4: Fidelity of the state independent Toffoli operation (2.64) as a function of the number N of control qubits.

native way to improve the fidelity of the state independent C-NOT transformation. The approximate transformation (2.57) includes one control and one target qubit and is based on the equatorial $1 \rightarrow 2$ cloning transformation. In classical information processing there is a transformation, so-called Toffoli gate, that includes a few control qubits and just one target qubit [3]. By analogy with the classical Toffoli gate, we propose the quantum state independent Toffoli operation to have the following structure

$$|\psi\rangle_c^{\otimes N} \otimes |\chi\rangle_t \otimes |A\rangle_d \longrightarrow |\psi\rangle_c^{\otimes N} \otimes |f(\psi,\chi)\rangle_t \otimes |B\rangle_d \ . \tag{2.64}$$

This operation provides a specific transformation $|f(\psi,\chi)\rangle_t = U(\psi)\ |\chi\rangle_t$ on a single target qubit in the presence of N control qubits. This transformation is a particular case of the Controlled-U transformation (2.70) considered in section 2.2.3. Therefore, the fidelity between the idealized and actual outputs of such state independent Toffoli operation is given by $F^e_{N\rightarrow N+1} = [1+\eta(N,N+1)]/2$, where $\eta(N,N+1)$ is defined by Eq. (2.34). This fidelity growth with number of control qubits and achieves the unit asymptotically as it is displayed in Fig.2.4.

Up to now, we have not pay attention to the fact, that the state independent C-NOT (2.57) and Toffoli (2.64) transformations are constructed to be optimal for real input qubit states and, by implication, for pseudo-pure states (2.62) with real states $|\psi\rangle$ as a part. This restriction is not, however, crucial. First of all, it is possible to define the state independent C-NOT and Toffoli transformations for arbitrary input pure or mixed states following the procedure in section 2.2.2. Second, in many quantum algorithms, the utilization of real states is already sufficient to achieve computational advantages over classical computing [3].

Moreover, the construction of the multiqubit state independent transformations for real input qubit states provides us with a constructive way to improve further the

input-output fidelities of these transformations. As we have already see in section 2.1.2 by examples of universal, equatorial and meridional QCM's, the optimal fidelity of a cloning transformation increases for a small (in geometrical sense) set of input states. It is possible, therefore, to adopt the state independent two-qubit C-NOT and multiqubit Toffoli transformations for input states from a small circle on the Bloch sphere that is formed by a plane that crosses the sphere away from its center. It is known that for input states from a small circle, a much higher fidelity of the cloning transformation can be achieved in comparison to input states from the main circle [101].

Although during the realization of the single Toffoli transformation there is a loss of information $1-F$, it is always possible (by adding control qubits and/or by making a proper choice of set of input qubits) to make this loss $1-F$ less then a given value δ. In a particular algorithm, the overall fidelity between the ideal output and the actual read-out of the algorithm can be estimated as F^{ζ}, where F is the fidelity of a single N-qubit Toffoli transformation and ζ is the average number of the Toffoli transformations acting on an input qubit.

In fact, our suggestion to use basis independent transformations to perform quantum computation opens more questions than gives answers. The most important question to be answered: 'what is the role of entanglement in implementation of the presented basis independent operations?' So far we are unable to answer this question, since the role of entanglement is not clear in the cloning process in general. The presence of entanglement in the cloning process is widely confirmed [46]. For example, one may check that the copies from the universal QCM (2.24) are entangled with concurrence $C = 1/3$. From the other hand, It is also known that no entanglement is required for optimal cloning in the limit of large number of identical inputs [46].

Of course, the final decision on usefulness of the suggested implementation of state independent transformations in quantum computing can be done only after a detailed analysis of the efficiency of particular quantum algorithms realized with these transformations. At the moment the suggested implementation of basis independent transformations in quantum computing should be considered just as an alternative way of thinking about quantum computing with initially mixed states that, hopefully, may be useful in the development of new algorithms and in future experiments.

2.3 State and fidelity estimation

Any quantum information processing, be it cloning, basis dependent or basis independent unitary or non-unitary transformation, ends up with a measurement, the process that allows us to access the result of the performed on the quantum system actions. Although, the theory of quantum measurement has been known from the early days of quantum mechanics, recent experiments and achievements induced discussions of new earlier untouched problems such as state estimation [117], state discrimination [118, 119] and state comparison [120]. All these problems lie in the very foundation of quantum mechanics and, by implication, whole quantum information theory.

In the state estimation problem, we are given a finite ensemble of N independent

identical quantum systems initially prepared in some pure or mixed state. Our task is to find a measurement that provides us with the best possible estimation of the unknown state. Of course, having an unlimited supply of identical particles, we can estimate the state of interest with an arbitrary precision. In practice, however, only finite and usually small ensembles of identically prepared quantum systems are available. This leads to the problem of the optimal state estimation with limited physical resources.

The first profound result concerning the state estimation problem was obtained by Massar and Popescu [43], who showed that optimal measurement procedures must necessarily view the ensemble of particles as a single composite system rather than as a sum of its components. Soon after, a universal algorithm to construct an optimal measurement for state estimation from a finite ensemble of pure states was suggested by Derka *et al.* [45]. In the line of this algorithm a positive operator valued measurement (POVM), which is characterized by a set of orthogonal projectors, need to be performed on the composite system of all N particles.

Let us display explicitly the optimal POVM for the state estimation of a pure qubit state $|\psi\rangle$ being given N copies of this state. Let us also focus on the case when the state $|\psi\rangle$ is known to belong to the equator of the Bloch sphere. Later it will become clear why this particular example is important for our discussion. Since the state of the N-qubit system always remains within the totally symmetric subspace of $\mathcal{H}_2^{\otimes N}$ where $\mathcal{H}_2$ is the two-dimensional qubit state space, the dimensionality of the space in which the POVM need to be defined is $N+1$. If $|n\rangle\,,\, n=0,...,N$ is an orthonormal basis in this $N+1$-dimensional space, the optimal POVM for the state estimation of the equatorial qubit is given by the set of $k=1,...,N$ orthogonal projectors $P_k = |\Psi_k\rangle\langle\Psi_k|$ where

$$|\Psi_k\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} e^{i\frac{2\pi}{N+1}kn} |n\rangle \ . \tag{2.65}$$

A convenient value that characterize the efficiency of the measurement procedure is the mean fidelity between the original and the estimated states. For an ensemble of N pure equatorial qubit states, the POVM defined through Eq. (2.65) is shown [45] to maximize the mean fidelity between the original equatorial state $|\psi\rangle$ and the reconstructed state $|\psi'\rangle$. The maximal mean fidelity is given by

$$\overline{f}(|\psi_a\rangle\,,|\psi'_a\rangle) = \frac{1}{2} + \frac{1}{2^{N+1}} \sum_{i=0}^{N-1} \sqrt{C_i^N\, C_{i+1}^N}\,, \tag{2.66}$$

where C_i^N and C_{i+1}^N denote the binomial coefficients.

State estimation of an equatorial qubit state from a finite number of copies is a practically important task. Equatorial qubit states may represent, for instance, polarization states of photons. Therefore, any protocol for quantum communication and computation based on implementation of photons requires the optimal measurement procedure that is given by the optimal state estimation of equatorial qubits.

We may also make a step beyond simple state estimation and consider a more sophisticated problem of fidelity estimation. Suppose, we are given two finite ensembles of unknown equatorial qubit states. Each ensemble, moreover, contains N separable particles initially prepared in pure states $|\psi_a\rangle$ and $|\psi_b\rangle$. As we mentioned before, a pure equatorial qubit state can be parameterized with a single parameter as (2.10) and can be visualized as a point lying on a big circle which is formed by the intersection of the Bloch sphere in Fig. 2.1 with $x-y$ plane. We may ask what is the best strategy to estimate the fidelity

$$F_{a,b} \equiv |\langle\psi_a|\psi_b\rangle|^2 = \frac{1}{4}|1+e^{i(\phi_b-\phi_a)}|^2 \tag{2.67}$$

between the finite ensembles of equatorial qubit states $|\psi_a\rangle$ and $|\psi_b\rangle$?

Apart of academic interest the fidelity estimation problem may be relevant in implementation of schemes for quantum communication with linearly polarized photons and for linear optics quantum computation [20]. For example, we are given with a finite ensemble of $2N$ identical linearly polarized photons in some quantum state $|\psi_a\rangle$. A half of the photons from the ensemble are subjected independently to some unitary evolution so that the outputs are in the state $|\psi_b\rangle$. We like to know the effect (2.67) of the unitary evolution by comparing the phases of the states $|\psi_a\rangle$ and $|\psi_b\rangle$.

The simplest (measurement-based) strategy to estimate the fidelity between the ensembles of states $|\psi_a\rangle$ and $|\psi_b\rangle$ is to perform state estimation of each of these states independently and compute the fidelity (2.67) between the estimated states $|\psi'_a\rangle$ and $|\psi'_b\rangle$. Following this strategy, the maximal mean fidelity between each of the original equatorial states $|\psi_i\rangle$ and the corresponding reconstructed states $|\psi'_i\rangle$ where $i=\{a,\,b\}$ is given by (2.66). Since the states of interest are estimated independently, the probability to reconstruct fidelity (2.67) correctly is given by $\overline{f}^2(|\psi_a\rangle, |\psi'_a\rangle)$ and displayed in Fig. 2.5 by dots. Here and later we use term "probability" in order to avoid any confusion. This term is used in the sense of mean fidelity between estimated and actual values of (2.67).

An alternative (cloning-based) strategy for the fidelity estimation can be viewed to include two stages. At the first stage we provide infinite many copies from available replicas of the unknown states $|\psi_a\rangle$ and $|\psi_b\rangle$. This task can be realized with equatorial $N\longrightarrow\infty$ QCM [102]. Each copy from this QCM is given by the mixed state

$$\rho_k^{\rm out} \;=\; \eta(N,\infty)\,|\psi_k\rangle\langle\psi_k| + \frac{1}{2}\left[1-\eta(N,\infty)\right] I\,, \tag{2.68}$$

where the shrinking factor $\eta(N,M)$ is defined in Eq. (2.34). Having two infinite ensembles of states $\rho_a^{\rm out}$ and $\rho_b^{\rm out}$ we can perform measurements in some chosen basis and estimate these states by computing statistical averages. The measurement procedure gives the second stage of the fidelity estimation. Knowing the estimated states we can calculate the fidelity (2.67). In the line of this strategy, the fidelity between each of the original states $|\psi_k\rangle$ and their estimations $\rho_k^{\rm out}$ is given by $F_e = \langle\psi_k|\rho_k^{\rm out}|\psi_k\rangle = \left[1+\eta(N,\infty)\right]/2$. Therefore, the probability to reconstruct the fidelity (2.67) correctly equals F_e^2.

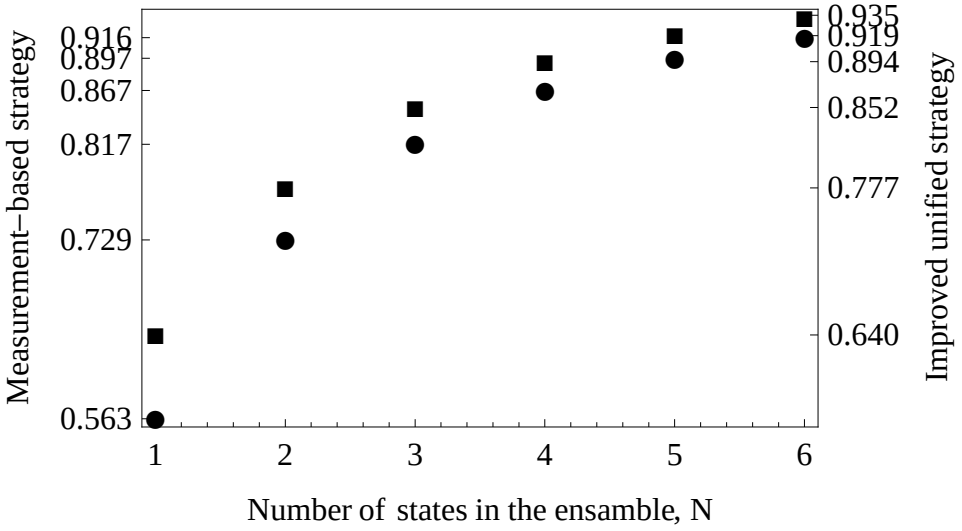

Figure 2.5: The probabilities to reconstruct fidelity (2.67) by the first measurement-based strategy (dots) and the third improved unified strategy (squares).

Surprisingly enough, the two discussed strategies for the fidelity estimation are equivalent in the sense that the probabilities $\overline{f}^2(|\psi_a\rangle, |\psi'_a\rangle)$ and F_e^2 are equal. This demonstrates the fundamental link between quantum cloning and state estimation established by Bae and Acin [121] who showed that asymptotic quantum cloning is equivalent to the state estimation.

The two strategies above are based on independent estimation of quantum states and computation of the fidelity using the estimated states. However, to estimate the fidelity (2.67) we do not need to know phases ϕ_a and ϕ_b of the unknown states, rather, the difference between them. Based on this simple observation we now introduce the third two-stage strategy for the fidelity estimation which unifies previous two strategies in some sense. At the first stage we take a pair of qubits $|\psi(\phi_a)\rangle$ and $|\psi(\phi_b)\rangle$ from different ensembles and perform a unitary transformation

$$|\psi(\phi_a)\rangle\,|\psi(\phi_b)\rangle\,|A\rangle \longrightarrow |\psi(\phi_a)\rangle\,|\psi(\phi_b-\phi_a)\rangle\,|A_\psi\rangle \tag{2.69}$$

on these unknown input qubits. The matter of the first stage is to obtain a qubit in the state $|\psi(\phi_b-\phi_a)\rangle$ at the output of this transformation. At the second stage, the state estimation of the state $|\psi(\phi_b-\phi_a)\rangle$ is to be performed what allows us eventually to access the fidelity (2.67).

Of course, the transformation (2.69) can not be performed exactly on unknown quantum states due to the general impossibility theorem. However, we have already constructed the optimal approximation for this transformation — the state independent C-NOT transformation (2.57)[1]. As we know, the output states of the

[1]Although the state independent C-NOT transformation in section 2.2.2 was originally constructed for real qubit states, it remains optimal for input states taken from an arbitrary one-dimensional subspace of the two-dimensional qubit state space. This follows from the symmetry of the Bloch sphere. The equatorial qubits is just a particular choice of the one-dimensional subspace.

C-NOT transformation are in the mixed states of the form (2.68) with $\eta(1,2)$ and $|\psi_k\rangle = \{|\psi(\phi_a)\rangle\,,\,|\psi(\phi_b-\phi_a)\rangle\}$. The fidelity between the actual output states and the idealized outputs of the transformation (2.57) equals $F_{C-NOT} = 1/2 + 1/\sqrt{8}$.

Coming back to the original problem of the fidelity estimation and repeating the C-NOT transformation N times on available copies of the states $|\psi(\phi_a)\rangle$ and $|\psi(\phi_b)\rangle$ we have an ensemble of N particles in the mixed state (2.68) with $\eta(1,2)$ and $|\psi_k\rangle \equiv |\psi(\phi_b-\phi_a)\rangle$ at the output. Having this ensemble we can start the second stage – the state estimation. Here we note that, in general, state estimation of mixed states with unknown shrinking factor and phase require construction of a specific POVM [122]. However, in our case the shrinking factor is known and, therefore, state estimation of the mixed state reduces to the estimation of the phase of the pure state $|\psi(\phi_b-\phi_a)\rangle$. As we discussed earlier, this task can be accomplished with the POVM (2.65). Thus the probability to reconstruct fidelity (2.67) is given by $\overline{f}(|\psi\rangle\,,|\psi'\rangle)\times F_{C-NOT}$. This probability is better than the probability to reconstruct fidelity by independent state estimation only for ensembles consisting of single particle. For ensembles of several particles the first (measurement-based) strategy becomes more efficient.

The reason for the very limited advantage of the third (unified) strategy over the measurement-based strategy is clear: we applied the universal transformation (2.69) only on pairs of qubits from different ensembles. An improved unified strategy is to apply a more general controlled unitary transformation to *all* states in two ensembles at the first stage, i.e.

$$|\psi(\phi_a)\rangle^{\otimes N}|\psi(\phi_b)\rangle^{\otimes N}|A\rangle \longrightarrow |\psi(\phi_a)\rangle^{\otimes N}|\psi(\phi_b-\phi_b)\rangle^{\otimes N}|A_\psi\rangle\,. \qquad (2.70)$$

The optimal approximation for this transformation has been already constructed in section 2.2.3. By our construction, the approximate transformation has similar structure to $N\longrightarrow 2N$ equatorial QCM. The output states of the transformation (2.70) are in the mixed states of the form (2.68) with $\eta(N,2N)$. The fidelity between the actual output states and the idealized outputs is given by $F^{\rm gen}_{C-NOT} = [1+\eta(N,2N)]/2$. Coming to the second stage of the fidelity estimation, i.e. performing the state estimation on the ensemble of N output qubits $\rho^{out}(\phi_b-\phi_a)$ with POVM (2.36), we obtain that the probability to reconstruct fidelity (2.67) equals $\overline{f}(|\psi\rangle\,,|\psi'\rangle)\times F^{\rm gen}_{C-NOT}$. As displayed in Fig. 2.5, this probability always superior the probability of the fidelity reconstruction by the measurement-based strategy. Therefore, the third improved unified strategy for the fidelity estimation is the best among the three.

At the beginning of the discussion of the fidelity estimation problem we assumed that both ensembles contain equal number of particles in separable and pure states. In fact, the first assumption can be easily remover. It is easy to define the three strategy for two ensembles with unequal number of particles N and K. By analogy with transformation (2.70), a generalized $N\longrightarrow N+K$ transformation can be defined similar to Eq. (2.70). We checked that the third strategy remains the best among the three in the case of unequal number of particles in the ensembles.

However, the other two assumptions, namely that the initial states in the ensembles are separable and pure, are indeed crucial for present discussion. Being given two

ensembles of correlated qubits or qubits in mixed states, one should accordingly revise all three strategies. For example, without any knowledge about the shrinking factor of given mixed states, one should use an optimal set of POVM for state estimation of unknown mixed states as it was derived by Bagan *et al.* [122]. Moreover, in order to apply the third strategy on two ensembles of correlated qubits or qubits in mixed states one should find an optimal approximation for the transformation (2.70) for these ensembles. It remains an open problem for us whether the third strategy is still the best in the cases of two finite ensembles of unknown equatorial correlated qubits or qubits in mixed states.

2.4 Results and discussion

In this chapter, we analyzed the fundamental features of optimal quantum information processing and suggested several optimal quantum transformations. In particular, unlike the well-known universal [94] and equatorial [102] quantum cloning, we presented a QCM that provides high-fidelity copies for all states from a selected meridian (i.e. half-circle) of the Bloch sphere. This (so-called) meridional QCM was constructed to provide hight-fidelity copies with $0.95 \geq F \geq 0.90$ for all states along the Eastern meridian. Although this QCM provides high-fidelity copies for the Eastern meridian, it can be applied with little adaptations also to other meridians. All what is needed to follow the optimization procedures as described, in section 2.1.2. In addition, the suggested QCM was applied to analyze a possible eavesdropping attack in the data transmission between Alice and Bob, within Bennett's B92 QKD protocol [32], in section 2.1.3. From this analysis, it was shown that Eve, the eavesdropper, can obtain more information from the meridional than from the universal or equatorial QCM's.

We also defined and constructed the optimal approximation for state independent C-NOT transformation (2.57) for two unknown input qubits taken form the main circle of the Bloch sphere, in section 2.2.2. The C-NOT transformation, moreover, was shown to have similar structure to equatorial QCM. Using obtained analogy between this state independent controlled unitary transformation and cloning, we conjectured in section 2.2.3, that the efficiency of an arbitrary $N \rightarrow N + K$ controlled unitary transformation is defined by the efficiency of the corresponding optimal cloning.

In section 2.2.4, we suggested an implementation of the derived state independent transformations in quantum computing. In spite of the approximate character of these transformations, we argued that a quantum circuit constructed from state independent transformations can be efficiently used for quantum computation when initially mixed qubit states are available. We also discussed how the efficiency of such a quantum circuit can be estimated and how this efficiency can be improved by increasing the number of qubits involved in a state independent transformation and by decreasing (in geometric sense) the set of input states. However, we did not analyze the efficiency of quantum circuits constructed from basis independent transformations for particular quantum algorithms. This analysis is necessarily to be made in the future to conclude on usefulness of the suggested implementation.

Finally, we briefly discussed the state and the fidelity estimation problems, in

section 2.3. While for the state estimation we just called existing results, we suggested and analyzed the three possible strategies for the fidelity estimation between two finite ensembles of unknown pure equatorial qubit states. We showed that the best strategy for the fidelity estimation includes an optimal state independent transformation (2.70) of *all* qubits and the state estimation of the output of this transformation by the optimal POVM (2.65).

We also would like to admit that many physical realizations of QCM's has been demonstrated recently. An optical implementation of the universal $1 \rightarrow 2$ QCM (2.24) for an arbitrary input qubit state based on parametric down-conversion has been demonstrated to have fidelity 0.810 ± 0.008 [123] which is in a good agreement with the theoretical prediction $5/6 = 0.833$. Another physical realization of the universal QCM was achieved by using optical fibers doped with erbium ions. The universal cloning transformation based on this technique was shown to have fidelity $F \approx 0.82$ which is again in good agreement with the theoretical prediction [46]. Also, several realistic theoretical schemes for the physical realization of a QCM on atoms in a cavity have been recently proposed [46]. However, to our knowledge no experimental results are available at the moment. Also, some physical realizations of universal and equatorial $1 \rightarrow N$ QCMs where $N = 2, 3...$ has been already reported.

Apart of the optimal cloning transformations, a single-qubit state independent transformation — universal NOT operation (2.43) — has been experimentally demonstrated with an optical setup to have fidelity 0.630 ± 0.008 which is in a good agreement with the theoretical prediction $2/3 \approx 0.666$ [123]. However, it is worth noticing that while most of efforts has been devoted to physical realizations of $1 \rightarrow N$ QCMs where $N = 2, 3...$, no attention has been paid to realization of universal and equatorial $N \rightarrow N + K$ QCMs. Therefore, it is hard to judge whether such cloning machines and corresponding optimal multiqubit state independent transformations can be efficiently realized in practice.

On the background of the experimental achievements in realization of QCM's, we like to mention recent progress in realization of standard state dependent C-NOT transformation (2.47) which is considered to be the necessary element to construct a quantum circuit for quantum computation. Several experimental realizations of this transformation using linear optical elements has been suggested [20]. Up to now, however, the best achieved C-NOT transformation (2.47) has been reported to have an average fidelity $\overline{F} = 0.82 \pm 0.01$ between the output and the ideal output, which is indeed far from the theoretically predicted unit fidelity [26]. Significant progress has been also achieved in the realization of the C-NOT transformation (2.47) with trapped ions. To our knowledge the best realization of the C-NOT transformation is to have an average fidelity $\overline{F} = 0.940 \pm 0.004$ between the output and the ideal output [26]. Although our suggested state independent C-NOT transformation (2.57) as well as the multiqubit controlled unitary transformation (2.70) allow to perform the required operations only approximately, the efficiency of their experimental realizations may exceed the achieved efficiencies of the state dependent transformations.

Outlook

This thesis aimed to extend the existing knowledge about entanglement dynamics of multiparticle finite-dimensional quantum systems and optimal ways of manipulation of information encoded in states of such systems.

In the first chapter of our work, we recalled first how entanglement can be quantified with the help of such entanglement measures as the convex roof for concurrence and the lower bound for concurrence. Then, we applied these measures to analyze entanglement dynamics of three-qubit systems subjected to non-unitary evolution. In this analysis, in more details, we used the exact expressions for the three-qubit mixed state density matrices obtained from analytical solutions of the master equation. We found that the accuracy of the lower bound approximation with regard to the convex roof depends on the rank of the given mixed state density matrix. For density matrices with rank no higher than four, the lower bound is found to coincide with the convex roof. By testing randomly generated density matrices, moreover, we checked that this statement remains true for all (verified) density matrices. For density matrices with higher rank, the lower bound was found to vanish just after finite time being unable to describe long time entanglement evolution of the mixed state.

Knowing how the accuracy of the lower bound depends on the rank of the given state, we considered another approach for describing the entanglement dynamics of a three-qubit quantum system. We proposed an evolution equation for quantum entanglement of multiqubit systems which manifests that the entanglement dynamics of an arbitrary state of a three-qubit system, when one or several of its qubits undergoes the action of an arbitrary noisy environment, is subordinated to the dynamics of one of the maximally entangled states of three qubits. Moreover, we verified this result by analyzing three examples of the entanglement dynamics of a three-qubit system which was deduced from the suggested evolution equation.

The results of the first chapter were mainly obtained for a particular case of three qubits. However, the convex roof and the lower bound for concurrence can be easily defined for multiqubit systems with more than three particles as well as for multiqudit systems. Following to the same method of analysis as we used in section 1.3, one may establish how the accuracy of the lower bound approximation depends on the parameters of a given composite state and, hereinafter, construct evolution equations for quantum entanglement of general multiqudit systems. Therefore, from the methodological point of view our analysis is not restricted by three qubits.

We also like to admit that during the last years significant progress in generation of entangled states have been achieved: up to eight ions in a cavity [59] and up to

six photons [58] can be prepared in entangled states. As the underlying techniques of quantum control improve continuously, it can be expected that in the nearest future even larger systems can be entangled. All these experimental achievements certify actuality of our treatment in the first chapter.

In the second chapter, we discussed how information encoded in states of finite-dimensional quantum systems can be copied, transformed and read out. Having started from recalling the fundamental limitations on quantum information processing, namely the no-cloning and the general impossibility theorems, we presented a theory of quantum cloning machine (QCM) which has been developed during last 15 years. Focusing on the particular case of optimal deterministic symmetric and ancilla assisted QCM, we derived the (meridional) QCM that allows to provide two high-fidelity copies from a single input qubit, if the state of the input is known to belong to a chosen restricted set of states. We also analyzed an application of the suggested meridional QCM in the eavesdropping attack on B92 protocol.

Having discussed optimal copying of quantum states, we considered a general class of quantum transformations that allow us to perform certain operations on given inputs independently on particular states of these inputs. In particular, we constructed two- and multiqubit controlled unitary state independent transformations for qubits and showed the deep analogy between such quantum transformations and QCMs. This analogy allowed us to associate efficiencies of state independent transformations with efficiencies of corresponding optimal cloning machines. Although we focused only on construction of optimal state independent transformations for qubits, similar methods as reported in section 2.1, can be applied to construct optimal state independent transformations for qudits.

We also showed how a circuit for quantum computation can be constructed from the suggested state independent transformations. While we have not been able to perform a complete analysis of the efficiency of the suggested implementation of state independent transformations in quantum computing in the framework of this thesis, we pointed out several reasons why this implementation may have advantages compared to the common ways to implement quantum computation. Namely that the efficiency of a multiqubit state independent transformation decreases linearly (in contrast to polynomial decrease for basis dependent transformations), if applied to inial pseudo-pure states. This efficiency, moreover, can be improved by varying the number of qubits involved in a transformation and/or by appropriate preparation of the input qubits. In addition, we recalled recent experimental achievements in realization of state dependent and state independent transformations which justify (but, of course, not prove) our conjecture about usefulness of the suggested implementation.

In order to complete at some level our analysis of the fundamental features of quantum information processing, we considered in addition state and fidelity estimation problems by example of finite ensembles of uncorrelated pure equatorial qubit states. We suggested and analyzed the best strategy for the fidelity estimation between two finite ensembles of pure equatorial qubit states which includes a specific unitary state independent transformation on two ensembles and state estimation of the output states of this transformation.

Bibliography

[1] A.M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. Lond. Math. Soc. **42**, 230 (1936). 1

[2] C.E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27**, 379 & 623 (1948). 1

[3] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000). 1, 4, 8, 18, 19, 20, 32, 36, 50, 52, 54, 59, 62

[4] A.M. Childs and W. van Dam, *Quantum algorithms for algebratic problems*, Rev. Mod. Phys. **82**, 1 (2010). 1

[5] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. Roy. Soc. Lond. A **400**, 97 (1985). 2

[6] D. Deutsch and R. Jozsa, *Rapid solutions of problems by quantum computation*, Proc. Roy. Soc. Lond. A **439**, 553 (1992). 2

[7] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM J. Comput. **26**, 1411 (1997). 2

[8] D.R. Simon, *On the power of quantum computation*, SIAM J. Comput. **26**, 1474 (1997). 2

[9] P.W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26**, 1484 (1997). 2

[10] L.K. Grover, *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett. **79**, 325 (1997). 2

[11] E. Farhi and S. Gutmann, *Quantum computation and decision trees*, Phys. Rev. A **58**, 915 (1998). 2

[12] J. Watrous, *Quantum simulations of classical random walks and undirected graph connectivity*, J. Comput. Syst. Sci. **62**, 376 (2001). 2

[13] J. Eisert, M. Wilkens and M. Lewenstein, *Quantum games and quantum strategies*, Phys. Rev. Lett. **83**, 3077 (1999). 2

[14] R. Jozsa and N. Linden, *On the role of entanglement in quantum-computational speed-up*, Proc. Soc. Lond. A **459**, 2011 (2003). 2, 59, 60

[15] E. Biham, G. Brassard, D. Kenigsberg and T. Mor, *Quantum computing without entanglement*, Theor. Comp. Sci. **320**, 15 (2004). 2, 60

[16] N. Linden and S. Popescu, *Good dynamics versus bad kinematics: is entanglement needed for quantum computation?*, Phys. Rev. Lett. **87**, 047901 (2001). 2

[17] S.L. Braunstein and A.K. Pati, *Speed-up and entanglement in quantum searching*, Quantum Inf. Comput. **2**, 399 (2002). 2, 60

[18] R. Blume-Kohout, C.M. Caves and I.H. Deutsch, *Climbing mount scalable: physical resource requirements for a scalable quantum computer*, Found. Phys. **32**, 1641 (2002). 2, 59, 60

[19] E. Knill, R. Laflamme and G.J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature **409**, 46 (2001). 2

[20] P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J.P. Dowling and G.J. Milburn, *Linear optical quantum computing with photonic qubits*, Rev. Mod. Phys. **79**, 135 (2007). 2, 65, 69

[21] D. Gottesman and I.L. Chuang, *Demonstraiting the viability of universal quantum computation using teleportation and single-qubit operations*, Nature **402**, 390 (1999). 2

[22] R. Raussendorf and H.J. Briegel, *A one-way quantum computer*, Phys. Rev. Lett. **86**, 5188 (2001). 2

[23] H.J. Briegel, D.E. Browne, W. Dür, R. Raussendorf and M. Van den Nest, *Measurement-based quantum computation*, Nature Phys. **5**, 19 (2009). 2

[24] P.Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, A. Aspelmeyer and A. Zeilinger, *Experimental one-way quantum computing*, Nature **434**, 169 (2005). 2

[25] D. Hanneke, J.P. Home, J.D. Jost, J.M. Amini, D. Leibfried and D.J. Wineland, *Realization of a programmable two-qubit quantum processor*, Nature Phys. **6**, 13 (2010). 2

[26] T.D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe and J.L.O'Brien, *Quantum computers*, Nature **464**, 45 (2010). 2, 69

[27] W.K. Wootters and W.H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802 (1982). 2, 38

[28] D. Dieks, *Communication by EPR devices*, Phys. Lett. A **92**, 271 (1982). 2, 38

[29] H.-K. Lo and H.F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances*, Science **283**, 2050 (1999). 2

[30] P. Shor, *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett. **85**, 441 (2000). 2

[31] C.H. Bennett and G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 175 (1985). 2, 48

[32] C.H. Bennett, *Quantum cruptography using any two nonorthogonal states*, Phys. Rev. Lett. **68**, 3121 (1992). 2, 37, 49, 68

[33] D. Bruß, *Optimal eavesdropping in quantum cryptography with six states*, Phys. Rev. Lett. **81**, 3018 (1998). 2, 49

[34] A.K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661 (1991). 2

[35] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W.K Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993). 2

[36] P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller and J.E. Nordholt, *Long-distance quantum key distribution in optical fibre*, New J. Phys. **8**, 193 (2006). 2

[37] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, and A.J. Shields, *Gigahertz decoy quantum key distribution with* 1 *Mbit/s secure key rate*, Optics Express **16**, 18790 (2008). 2

[38] E. Schrödinger, *Die gegenwärtige situation in der Quantenmechanik*, Die Naturwissenschaften **23**, 807 (1935). 3

[39] A. Aspect, J. Dalibar and G. Roger, *Experimental test of Bell's inequalities using time-varying analysers*, Phys. Rev. Lett. **49**, 1804 (1982). 3

[40] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Quantum entanglement*, Rev. Mod. Phys. **81**, 865 (2009). 3, 8, 13, 16, 35, 36

[41] F. Mintert, A.R.R. Carvalho, M. Kus and A. Buchleitner, *Measures and dynamics of entangled states*, Phys. Rep. **415**, 207 (2005). 3, 13, 16, 18

[42] A. Böhm, *Quantum Mechanics* (Springer-Verlag, New-York, USA, 1979). 3

[43] S. Massar and S. Popescu, *Optimal extraction of information from finite quantum ensembles*, Phys. Rev. Lett. **74**, 1259 (1995). 3, 64

[44] Z. Hradil, *Quantum-state estimation*, Phys. Rev. A **55**, R1561 (1997). 3

[45] R. Derka, V. Buzek and A.K. Ekert, *Universal algorithm for optimal estimation of quantum states from finite ensembles via realizable generalized measurement*, Phys. Rev. Lett. **80**, 1571 (1998). 3, 64

[46] V. Scarani, S. Iblisdir, N. Gisin, A. Acin, *Quantum cloning*, Rev. Mod. Phys. **77**, 1225 (2005). 3, 39, 40, 45, 49, 63, 69

[47] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145 (2002). 4

[48] R.F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A **40**, 4277 (1989). 7

[49] P.A. Horn and C.R. Johnson, *Matrix Analysis* (Cambridge University Press, New York, USA, 1985). 8

[50] A.Peres, *Higher order Schmidt decompositions*, Phys. Lett. A **202**, 16 (1995). 9

[51] M. Horodecki, P. Horodecki and R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Phys. Lett. A **223**, 1 (1996). 9, 10

[52] A. Peres, *Separability criterion for density matrices*, Phys. Rev. Lett. **77**, 1413 (1996). 9

[53] M. Horodecki, P. Horodecki and R. Horodecki, *Mixed-state entanglement and distillation: Is there a 'bound' entanglement in nature?*, Phys. Rev. Lett. **80**, 5239 (1998). 10

[54] M. Horodecki, P. Horodecki and R. Horodecki, *Bound entanglement can be activated*, Phys. Rev. Lett. **82**, 1056 (1999). 10

[55] L.M. Ioannou, *Computational complexity of the quantum separability problem*, Quantum Inf. Comput **7**, 335 (2007). 10

[56] G. Vidal, *Entanglement monotones*, J. Mod. Opt. **47**, 355 (2000). 10, 12

[57] F. Mintert, *Measures and dynamics of entangled states*, Ph.D. thesis, University of Munich, 2005. 11, 12, 13, 18

[58] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, J.-W. Pan, *Experimental entanglement of six photons in graph states*, Nature Phys. **3**, 91 (2007). 11, 72

[59] O. Gühne and G. Tóth, *Entanglement detection*, Phys. Rep. **474**, 1 (2009). 11, 16, 36, 71

[60] M. Tiersch, *Benchmarks and statistics of entanglement dynamics*, Ph.D. thesis, University of Freiburg, 2009. 12, 13, 27

[61] W.K. Wootters, *Entanglement of formation of an arbitrary state of two qubits*, Phys. Rev. Lett. **80**, 2245 (1998). 13, 15

[62] A. Uhlmann, *Fidelity and concurrence of conjugated states*, Phys. Rev. A **62**, 032307 (2000). 15

[63] P. Rungta, V. Bužek, C.M. Caves, M. Hillery and G.J. Milburn, *Universal state inversion and concurrence in arbitrary dimensions*, Phys. Rev. A **64**, 042315 (2001). 15, 16

[64] S. Albeverio and S.-M. Fei, *A note on invariants and entanglements*, J. Mod. B: Quantum Semiclass. Opt. **3**, 223 (2001). 15, 16

[65] S.J. Akhtarshenas, *Concurrence vectors in arbitrary multipartite quantum systems*, J. Phys. A: Math. Gen. **38**, 6777 (2005). 15

[66] Y.-C. Ou, H. Fan, S.-M. Fei, *Proper monogamy inequality for arbitrary pure quantum states*, Phys. Rev. A **78**, 012311 (2008). 15, 16

[67] M. Li, S.-M. Fei and Z.-X. Wang, *A lower bound of concurrence for multipartite systems*, J. Phys. A **42**, 145303 (2009). 16, 17

[68] H.F. Jones, *Groups, Representations and Physics* (Inst. of Phys. Publishing Bristol and Philadelphia, USA, 1998). 17

[69] A. Uhlmann, *Optimizing entropy relative to a channel or a subalgebra*, Open System Inform. Dyn. **5**, 209 (1998). 18

[70] C.W. Gardiner and P. Zoller, *Quantum noise*, 2nd Edition (Springer, Berlin, Germany, 2000). 18, 19

[71] H.P. Breuer and F. Petruccione, *The theory of open quantum systems* (Oxford University Press, Oxford, England, 2002). 18, 19

[72] K. Kraus, *States, Effects and Operations: Fundamental Notations in Quantum Theory* (Springer-Verlag, Berlin, 1983). 18

[73] P. Štelmachovič and V. Bužek, *Dynamics of open quantum systems initially entangled with environment: Beyond the Kraus representation*, Phys. Rev. A **64**, 062106 (2001). 19

[74] G. Lindblad, *On the generators of quantum dynamical semigroups*, Commun. Math. Phys. **40**, 147 (1975). 19

[75] A.R.R. Carvalho, F. Mintert and A. Buchleitner, *Decoherence and multipartite entanglement*, Phys. Rev. Lett. **93**, 230501 (2004). 18, 21, 26, 32, 35

[76] T. Yu and J.H. Eberly, *Quantum open system theory: bipartite aspects*, Phys. Rev. Lett. **97**, 140403 (2006). 18, 32

[77] W. Duer, G. Vidal and J.I. Cirac, *Three qubits can be entangled in two inequivalent ways*, Phys. Rev. A **62**, 062314 (2000). 20, 29, 30

[78] A. Karlsson, M. Bourennane, *Quantum teleportation using three-particle entanglement*, Phys. Rev. A **58**, 4394 (1998). 20

[79] J. Joo, Y.-J. Park, S. Oh and J. Kim, *Quantum teleportation via a W state*, New J. Phys. **5**, 136 (2003). 20

[80] P. Agrawal, A. Pati, *Perfect teleportation and superdense coding with W states*, Phys. Rev. A **74**, 062320 (2006). 20

[81] E. Jung, M.-R. Hwang, Y.H. Ju, M.-S. Kim, S.-K. Yoo, H. Kim, D. Park, J.-W. Son, S. Tamaryan, S.-K. Cha, *Greenberger-Horne-Zeilinger versus W states: quantum teleportation through noisy channels*, Phys. Rev. A **78**, 012312 (2008). 19, 20

[82] T. Konrad, F. DeMelo, M. Tiersch, C. Kasztelan, A. Aragao and A. Buchleitner, *Evolution equation for quantum entanglement*, Nature Phys. **4**, 99 (2008). 20, 27, 31

[83] Z.-G. Li, S.-M. Fei, Z.D. Wang and W.M. Liu, *Evolution equation of entanglement for bipartite systems*, Phys. Rev. A **79**, 024303 (2009). 20, 27, 28, 35

[84] Z. Liu and H. Fan, *Dynamics of the bounds of squared concurrence*, Phys. Rev. A **79**, 064305 (2009). 20

[85] N. Gisin, *Hidden quantum nonlocality revealed by local filters*, Phys. Lett. A **210**, 151 (1996). 27

[86] V. Coffman, J. Kundu, W.K. Wootters, *Distributed entanglement*, Phys. Rev. A **61**, 052306 (2000). 29

[87] F. Verstraete, J. Dehaene, B.De Moor and H. Verschelde, *Four qubits can be entangled in nine different ways*, Phys. Rev. A **65**, 052112 (2002). 30

[88] R. Lohmayer, A. Osterloh, J. Siewert, A. Uhlmann, *Entangled three-qubit states without concurrence and three-tangle*, Phys. Rev. Lett. **97**, 260502 (2006). 31

[89] G. Vidal and R.F. Werner, *Computable measure of entanglement*, Phys. Rev. A **65**, 032314 (2002). 36

[90] H.S. Park, S.-S.B. Lee, H. Kim, S.-K. Choi and H.-S. Sim, *Construction of an optimal witness for unknown two-qubit entanglement*, Phys. Rev. Lett. **105**, 230404 (2010). 36

[91] O.J. Farías, C.L. Latune, S.P. Walborn, L. Davidovich and P.H.S. Ribeiro, *Determining the dynamics of entanglement*, Science **324**, 1414 (2009). 36

[92] J.-S. Xu, C.-F. Li, X.-Y. Xu, C.-H. Shi, X.-B. Zou and G.-C. Guo, *Experimental characterization of entanglement dynamics in noisy channels*, Phys. Rev. Lett. **103**, 240502 (2009). 36

[93] A.K. Pati, *General impossible operations in quantum information*, Phys. Rev. A **66**, 062319 (2002). 39, 53

[94] V. Bužek and M. Hillery, *Quantum copying: beyond the no-cloning theorem*, Phys. Rev. A **54**, 1844 (1996). 40, 43, 68

[95] D. Bruß, D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello and J.A. Smolin, *Optimal universal and state-dependent quantum cloning*, Phys. Rev. A **57**, 2368 (1998). 40, 44

[96] C.-S. Nui and R.B. Griffiths, *Two-qubit copying machine for economical quantum eavesdropping*, Phys. Rev. A **60**, 2764 (1999). 40

[97] L.-M. Duan and G.-C. Guo, *Probabilistic cloning and identification of linearly independent quantum states*, Phys. Rev. Lett. **80**, 4999 (1998). 40

[98] A.K. Pati, *Quantum superposition of multiple clones and the novel cloning machine*, Phys. Rev. Lett. **83**, 2849 (1999). 40

[99] A. Peres, *Classical interventions in quantum systems. I. The measuring process*, Phys. Rev. A **61**, 022116 (2000). 42

[100] K. Audenaert, B.De. Moor, *Optimizing completely positive maps using semidefinite programming*, Phys. Rev. A **65**, 030302(R) (2002). 44

[101] J. Fiurášek, *Optical implementations of the optimal phase-covariant quantum cloning machine*, Phys. Rev. A **67**, 052314 (2003). 44, 63

[102] D. Bruß, M. Cinchetti, G.M. D'Ariano and C.Macchiavello, *Phase-covariant quantum cloning*, Phys. Rev. A **62**, 012302 (2000). 47, 48, 65, 68

[103] R.F. Werner, *Optimal cloning of pure states*, Phys. Rev. A **58**, 1827 (1998). 47

[104] G.-F. Dang and H. Fan, *Optimal broadcasting of mixed states*, Phys. Rev. A **76**, 022323 (2007). 48

[105] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu and A. Peres, *Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy*, Phys. Rev. A **56**, 1163 (1997). 48

[106] A.K. Ekert, B. Huttner, G.M. Palma and A. Peres, *Eavesdropping on quantum-cryptographical systems*, Phys. Rev. A **50**, 1047 (1994). 49

[107] A. Peres, *Quantum theory: concepts and methods* (Kluwer Academic Publishers, Dordrecht, the Netherlands, 2002). 50

[108] V. Bužek, M. Hillery and R.F. Werner, *Optimal manipulations with qubits: Universal-NOT gate*, Phys. Rev. A **60**, R2626 (1999). 52, 53

[109] N. Gisin and S. Popescu, *Spin flips and quantum information for antiparallel spins*, Phys. Rev. Lett. **83**, 432 (1999). 52

[110] A.K. Pati, *Minimum classical bit for remote preparation and measurement of a qubit*, Phys. Rev. Lett. **63**, 014302 (2000). 53

[111] D.P. DiVincenzo, *The physical implementation of quantum computation*, Fortschr. Phys. **48**, 771 (2000). 59

[112] J.I. Cirac and P. Zoller, *Quantum computations with cold trapped ions* Phys. Rev. Lett. **74**, 4091 (1995). 59

[113] T. Pelizzari, S.A. Gardiner, J.I. Cirac and P. Zoller, *Decoherence, continuous observation and quantum computing: A cavity QED model*, Phys. Rev. Lett. **75**, 3788 (1995). 59

[114] N.A. Gershenfeld and I.L. Chuang, *Bulk spin-resonance quantum computation*, Science **275**, 350 (1997). 59

[115] E. Knill and R. Laflamme, *Power of one bit of quantum information*, Phys. Rev. Lett. **81**, 5672 (1998). 60

[116] G.M. Palma, K.-A. Suominen and A.K. Ekert, *Quantum computers and dissipation*, Proc. Roy. Soc. Lond. A **452**, 567 (1996). 60

[117] R. Blume-Kohout, *Optimal, reliable estimation of quantum states*, New J. Phys. **12**, 043034 (2010). 63

[118] S.M. Barnett and S. Croke, *Quantum state discrimination*, Adv. Opt. Photon. **1**, 238 (2009). 63

[119] J.A. Bergou, *Discrimination of quantum states*, J. Mod. Opt. **57**, 160 (2010). 63

[120] S.M. Barnett, A. Chefles and I. Jex, *Comparison of two unknown pure quantum states*, Phys. Lett. A **307**, 189 (2003). 63

[121] J. Bae and A. Acin, *Asymptotic quantum cloning is state estimation*, Phys. Rev. Lett. **97**, 030402 (2006). 66

[122] E. Bagan, M.A. Ballester, R.D. Gill, A. Monras and R. Munoz-Tapia, *Optimal full estimation of qubit mixed states*, Phys. Rev. A **73**, 032301 (2006). 67, 68

[123] F. DeMartini, V. Bužek, F. Sciarrino and C. Sias, *Experimental realization of the quantum universal NOT gate*, Nature **419**, 815 (2002). 69