CZECH TECHNICAL UNIVERSITY IN PRAGUE
The Faculty of Nuclear Science and Physical Engineering

DIPLOMA THESIS

Properties and Applications of Purification Protocols

Stanislav Vymětal
Supervisor: Doc. Ing. Igor Jex, DrSc.

I declare that I wrote this diploma thesis independently using listed references.

Stanislav Vymětal, 19. 5. 2003, Prague

Content:

Chapter 1

Introduction

Quantum theory was born at the beginning of the 20-th century. Louis de Broglie, one of the fathers, in his Nobel prize lecture in December 1929, wrote:

"...Thirty years ago, physics was divided into two camps: the physics of matter, based on the concepts of particles and atoms which were supposed to obey the laws of classical Newtonian mechanics, and the physics of radiation, based on the idea of wave propagation in a hypothetical continuous medium, the luminous and electromagnetic ether. But these two systems of physics could not remain detached from each other: they had to be united by the formulation of a theory of exchanges of energy between matter and radiation. ..."

Since these days the quantum formalism matured. Nowadays the postulates of quantum theory can be formulated as follows [1]:

q1.a: To every quantum system corresponds a Hilbert space $\mathcal{H}$, also called the state space of the system.

q1.b: To each (pure or mixed) state of a quantum system corresponds a statistical operator (called density matrix) ρ on $\mathcal{H}$.

q1.c: To every observable (dynamic variable) of the quantum system corresponds a self-adjoined operator A on $\mathcal{H}$.

q2.a: Possible values of the observable A belong to the spectrum $\sigma(A)$ of A.

q2.b: The probability that the value of the observable A lies in the Borel set $\Delta \subset R$ for the system in the state ρ is equal

$$w(\Delta, A; \rho) = Tr(E_A(\Delta)\rho)$$

where $E_A(\Delta)$ is the projector onto the respective subspace. The operation $Tr(\cdot)$ is defined by the action on respective linear bounded operator A on Hilbert space $\mathcal{H}$ with scalar product $(.,.)$ and for arbitrary orthonormal base $\{e_i\}$ as $Tr(A) = \sum_i (e_i, A(e_i))$.

q3: Let us assume that the quantum system before measurement is in state ρ. If the measured value of observable A lies in Δ, then the state of the system after measurement is described by the statistical operator

$$\rho' = \frac{E_A(\Delta)\rho E_A(\Delta)}{Tr(E_A(\Delta)\rho)}.$$

q4.a: The time evolution of the quantum system is described by the unitary propagator $U(t,s)$ and ρ_t at time t is defined by the density matrix ρ_s at time s and $U(t,s)$ as

$$\rho_t = U(t,s)\rho_s U(t,s)^{-1}.$$

q4.b: The propagator $U(t,s)$ of the conservative system $\big(U(t+\tau,s+\tau) = U(t,s)$ for all $t,s,\tau \in R\big)$ with Hamiltonian H is defined as

$$U(t+\tau,\tau) = \exp(-iHt)$$

for all $t \in R$ and arbitrary but fixed $\tau \in R$.

q4.c: The time evolution for a non-conservative system with the Hamiltonian $H(t)$ is given by

$$i\frac{d}{dt}\rho_t = H(t)\rho_t - \rho_t H(t).$$

q5: The state space of the composed quantum system for distinguishable particles is given by the tensor product of state spaces of the particles i.e.: $\mathbf{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$. In case of indistinguishable particles $\mathcal{H}_1 = ... = \mathcal{H}_n = \mathcal{H}$ with whole integer resp. half integer spin the $\mathbf{H}$ is defined as

$$S_n(\mathcal{H} \otimes ... \otimes \mathcal{H})$$

resp.

$$A_n(\mathcal{H} \otimes ... \otimes \mathcal{H})$$

where

$$S_n := \frac{1}{n!}\sum_{\pi \in \mathcal{S}_n} U(\pi),$$

$$A_n := \frac{1}{n!}\sum_{\pi \in \mathcal{S}_n} \varepsilon_\pi U(\pi)$$

symmetrizes resp. antisymmetrizes $\mathcal{H} \otimes ... \otimes \mathcal{H}$. π denotes a permutation of the n-component set. $\mathcal{S}_n$ denotes the group of permutations of the n-component set, ε_π denotes the parity

of the respective permutation. $U(\pi)$ permutes pure states of the particles, it is defined by the action on $\mathbf{H}$ as

$$U(\pi)(\phi_1 \otimes \cdots \otimes \phi_n) = \phi_{\pi_1} \otimes \cdots \otimes \phi_{\pi_n}$$

for each permutation π and each $\phi_j \in \mathcal{H}$.

The formulation of the postulates of the theory was not an easy task and goes hand to hand with the modern branch of mathematics, the functional analysis. With the help of quantum theory large a number of amazing effects has been predicated, explained and employed for practical use. Many of them do not have a classical analogue. One of them is the existence of entangled quantum systems, a special type of correlated states, which do not have a classical counterpart.

Entangled systems were known since the beginning of quantum mechanics because they are a straightforward consequence of the linearity principle of quantum theory for composed systems. In 1935 Albert Einstein and two colleagues, Boris Podolsky and Nathan Rosen (EPR) developed a thought experiment [2] to demonstrate what they felt to be a lack of completeness in quantum mechanics. The autors defined what can be real, defined an element of physical reality by following criterion: "If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exist an element of physical reality corresponding to this physical quantity."

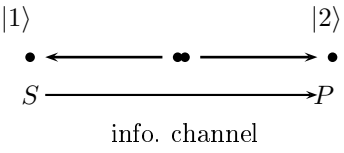

Fig.1: Scheme for EPR experiment.

They considered an idealized situation involving two participants P and S which have at their disposal one particle 1, 2 of a two-particle system. They wish to determine their momenta and positions. The system has been prepared in such a way that it possesses a well defined total momentum P and relative distance L of the particles. The participants are assumed to apply the measurements on their respective particles at locations far apart so that they cannot influence each others measurement. For this conditions the state of the two-particle system has the form

$$|\psi\rangle_{12} = \delta(x_1 - x_2 - L)\delta(p_1 + p_2 - P). \tag{1}$$

If S performs a measurement of the position on particle 1, the position of particle 2 is known for him too without disturbing particle 2. He can send the result to P via a channel and it implies that x_2 corresponds to element of physical reality for both S and P. On the other hand if S perform a measurement of momentum on particle 1, the

momentum of particle 2 is known for him too again without disturbing particle 2. From the same argument as above p_2 also correspond to an element of physical reality. However in quantum theory position and momentum measurement on 1 are noncommuting observables i.e. they can not be measured simultaneously with arbitrary precision in any experiment. Thus it seems that something is wrong with quantum theory.

Niels Bohr defended the postulates of quantum theory and in his answer wrote to Einstein that there exist another point of view of such result. He conceded that "there is no question of a mechanical disturbance of the system under investigation, there is essentially the question of an influence on the very conditions which define the possible types of predictions regarding the future behavior of the system."

Measurements on particles 1 and 2 are related to mutually incompatible tests i.e. those having the property that the execution of any one of these experiments precludes the execution of the others, no conclusion can be drawn from the comparison of possible results such tests.

The special kind of correlation between 1,2 which is responsible for the EPR paradox is the entanglement. In the sixties the interest in entanglement as a fundamental problem of quantum mechanics was reviewed. Attempts have been made to distinguish experimentally between the predictions of quantum mechanics and alternative theories like for instance the local hidden variables theories.

In recent years entangled states became useful for solving some tasks in quantum information physics, a new branch of quantum physics which analyses the possibilities of using quantum object as medium for safe storing and transporting of information.

The following examples demonstrate how amazing the entangled quantum states are.

Example 1: Quantum coding

A **bit** [3] is a computational quantity that can take on one of two values such as true and false or "0" and "1". Let us consider a digital encoding scheme which is equivalent to encoding the answer of a yes or no question. Usually these are expressed by the bit value "1" for yes, "0" for no. A good coding scheme should then be such that "0" or "1" can be distinguish safely. The physical realization of such coding scheme will therefore use a system which has two well defined states, in classical coding these could be for example the two positions of a switch. Let us consider the quantum mechanical analogue. It is then natural to associate two different orthogonal states to "0" and "1". Let us define a **qubit** [4] a two-level quantum system. Its most general state has the form

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

The qubit also allows us to encode the information in form (2) i.e. simultaneously containing the answer yes and no. Quantum information explores how this superposition can be used for practical purposes.

The encoding of a large number of bits of information can be done simply by assigning each bit its own two-state forming a large system (register). Let us consider two bits information. The information is encoded into orthogonal product states e.g. for two bits

$$|0\rangle \otimes |0\rangle,$$

$$|1\rangle \otimes |0\rangle,$$

$$|0\rangle \otimes |1\rangle,$$

$$|1\rangle \otimes |1\rangle.$$

The corresponding, in general 2^n, states form a complete orthonormal base for the n-qubit space. Alternatively in such a space we could choose very different bases which could be even entangled. A maximally entangled base for the two independent particles, two qubits, is

$$|\Psi^+\rangle_{12} = \tfrac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2),$$

$$|\Psi^-\rangle_{12} = \tfrac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2),$$

$$|\Phi^+\rangle_{12} = \tfrac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 + |1\rangle_1 \otimes |1\rangle_2),$$

$$|\Phi^-\rangle_{12} = \tfrac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 - |1\rangle_1 \otimes |1\rangle_2), \tag{3}$$

the so called Bell basis. It is important to notice that here we can still encode two bits of information i.e. we have four different possibilities, but now this encoding is done in such a way that none of the bits carries any well-defined information on its own e.g. if we measure the first qubit in state $|0\rangle$ and the second in $|1\rangle$ the composed system could be in $|\Psi^+\rangle$ or in $|\Psi^-\rangle$ as well. All information is encoded into relational properties of the two qubits. To decode the information we need a so called Bell state measurement, which is technically a bit of a problem.

Let us show how the two participants S and P use the quantum coding for their secret communication. Let us suppose that S wish to communicate to P two bits information. They will do it by encoding the information into Bell states.

For the procedure a simple property of the Bell states (3) is crucial: applying the combination of unitary operations

$$R(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}_1 \otimes \mathbf{I}_2,$$

and

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_1 \otimes \mathbf{I}_2$$

on one qubit of the respective Bell state it is possible to obtain any of the four Bell states, for example

$$R(\pi)R(\pi)|\Psi^-\rangle = |\Psi^-\rangle, \qquad R(\pi)|\Psi^-\rangle = |\Psi^+\rangle, \qquad FR(\pi)|\Psi^-\rangle = |\Phi^+\rangle, \qquad R(\pi)FR(\pi)|\Psi^-\rangle = |\Phi^-\rangle.$$

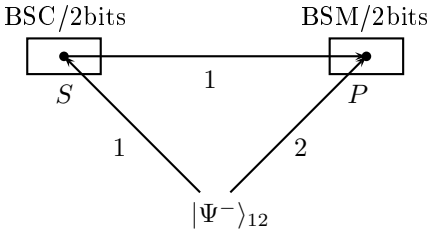

Fig.2: Two bits QC procedure.

Let us assume now that the participants P, S have a source of Bell states let say $|\Psi^-\rangle_{12}$ (1, 2 denotes respective qubits) and they have agreed on a secret coding key, for instant

$$|\Psi^+\rangle_{12} \to (00),\ |\Psi^-\rangle_{12} \to (01)$$

$$|\Phi^+\rangle_{12} \to (10),\ |\Phi^-\rangle_{12} \to (11). \qquad (4)$$

S will encode the two bits operation to Bell state 12 by local unitary transformation (BSC) on qubit 2. P must measure the received two particles 12 in the Bell basis (BSM) and interprets the result according to the secret key (4). Anyone who is in possesion of only one particle is unable to retrieve the information.

Example 2: Quantum teleportation

Our well known participants S and P are in following situation [3]. S has a source of qubits in a well defined state $|\psi\rangle_1 = \alpha|0\rangle + \beta|1\rangle$ and P needs one of them at a certain time too. In classical physics what S can do is to perform precise measurements to determine α and β and communicate the results to P, which can then generate her own copy. Let suppose now that S does not know the qubit state $|\psi\rangle_1$ (and he is unable to determine the state by measurement). Under such circumstances classically S can only send the particle directly to P what might be forbidden. Surprising quantum theory is able to transfer $|\psi\rangle_1$ to P without direct communication. However for the communication the Bell states (3)

will be needed.

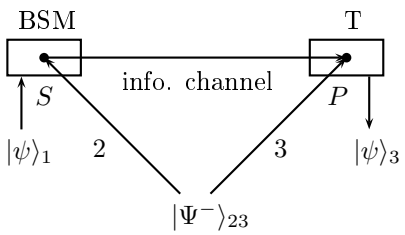

Fig.3: QT scheme

Participants S and P must share the two qubits 2 and 3 in an entangled state, say

$$|\Psi^-\rangle_{23} = \tfrac{1}{\sqrt{2}}(|0\rangle_2 \otimes |1\rangle_3 - |1\rangle_2 \otimes |0\rangle_3). \qquad (5)$$

System composed of the three qubits 1, 2, 3 is consequently in the state

$$|\psi\rangle_1 \otimes |\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(a|0\rangle_1 + b|1\rangle_1) \otimes (|0\rangle_2 \otimes |1\rangle_3 - |1\rangle_2 \otimes |0\rangle_3) =$$

$$= |\Phi^+\rangle_{12} \otimes (\frac{a}{2}|1\rangle_3 - \frac{b}{2}|0\rangle_3) + |\Phi^-\rangle_{12} \otimes (\frac{a}{2}|1\rangle_3 + \frac{b}{2}|0\rangle_3) + |\Psi^-\rangle_{12} \otimes (-\frac{a}{2}|0\rangle_3 - \frac{b}{2}|1\rangle_3) + |\Psi^+\rangle_{12} \otimes (-\frac{a}{2}|0\rangle_3 + \frac{b}{2}|1\rangle_3).$$

Now S projects the state of the particles 1 and 2 onto one of the Bell state (BSM) and communicates the result of the measurement to P via a classical public channel. With respect to the before agreed key (4) P performs one of the four transformations (T) on particle 3

$$(00) \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$(01) \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$(10) \rightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$(11) \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and obtains the particle 3 in the state $|\psi\rangle_3$. A remarkable property of the schema is, that cloning of the qubit 1 is impossible. By performing BSM the particle state $|\Psi\rangle_1$ is destroyed and can be retrieved on particle 3 only when the result of BSM is known to P. When P is ignorant to the result of S it is impossible to get $|\psi\rangle_3$ for her. She can only guess what the measurement on 1 of S was. Assume that all the outcomes of S measurements are equally probable, the state P obtained in this way will be

$$\frac{1}{4}(-a|0\rangle_3 + b|1\rangle_3)(-a^*\langle 0|_3 + b^*\langle 1|_3) + \frac{1}{4}(-a|0\rangle_3 - b|1\rangle_3)(-a^*\langle 0|_3 - b^*\langle 1|_3) +$$
$$\frac{1}{4}(-b|0\rangle_3 + a|1\rangle_3)(-b^*\langle 0|_3 + a^*\langle 1|_3) + \frac{1}{4}(b|0\rangle_3 + a|1\rangle_3)(b^*\langle 0|_3 + a^*\langle 1|_3) =$$
$$= \frac{1}{2}((\underbrace{a^2 + b^2}_{=1})|0\rangle_3\langle 0|_3 + (\underbrace{a^2 + b^2}_{=1})|1\rangle_3\langle 1|_3).$$

The output is a completely depolarized state without any relation to $|\psi\rangle_3$.

The entangled pair (5) is shared via a channel. The noise present in the channel influences the degree of entanglement and implicates a decrease in the efficiency of the teleportation. Hence it is desirable to decrease the influence of this noise as much as possible.

In the following we analyze the possibility how to improve the purity of entangled states for the case **finite quantum systems** [7] i.e. N-particles, $N < \infty$, D-levels, $D < \infty$ systems. Each particle, so called **qudit** [13], lives in C^D. The Hilbert space of the whole system is $C^D \otimes ... \otimes C^D$. The task will be solved by so called **purification protocols**. The existence of such a protocol for a certain class of states divides the set of available states onto "distillable" and "nondistillable". Studying the existence of such classes helps us to understand the still open question of entanglement in more detail.

Chapter 2

Review of Purifications Protocols

2.1 Definition of entanglement, the quantification

In the first chapter we mentioned that entanglement is a special type of correlation. Before we define entangled system, let us define correlations of system more precisely.

The two component system ab described by a density matrix ρ is correlated if a measurement on one of the components a, b influence the state of the other component i.e. the system is sad to be correlated if ρ can not be written in form $\rho = \rho_a \otimes \rho_b$ where ρ_a, ρ_b are density matrices related to each component a, b. When $\rho = \rho_a \otimes \rho_b$ applies the state is factorized.

This definition can be extend to N-particle systems. The system is **correlated** [4] if its state can not be described by density matrix ρ in form

$$\rho = \rho^1 \otimes ... \rho^N \tag{6}$$

where ρ^i, $i \in N$ is the density matrix of the i-th particle, in the other case the system is **factorized**.

Let us define an entangled system now. N-particles system is said to be **entangled** [5] if its density matrix ρ can not be written in the fully separable form

$$\rho = \sum_a p(a) \rho_a^{(1)} \otimes ... \otimes \rho_a^{(N)} \tag{7}$$

where $\rho_a^{(i)}$, $i \in N$ is density matrix of the i-th particle and $p(a)$ is the probability that ρ is in the state $\rho_a^{(1)} \otimes ... \otimes \rho_a^{(N)}$.

From the definitions we see that if a state is factorized it cannot be entangled and if it is entangled then it must be correlated somehow.

A very important problem is how to quantify entanglement, how to define a proper entanglement measure. A measure [1] is a non negative (zero for empty set), σ-aditive function on some system of Borel sets. Before we deal with the definition of a proper measure of entanglement we introduce measures of correlation, specially for the two particles systems.

A measure of the information content in the density matrix ρ is its entropy $S(\rho)$, in quantum mechanics defined by **von Neumann** [4] as a straightforward generalization of Boltzmann entropy in statistical mechanics

$$S(\rho) = -Tr(\rho \ln \rho). \tag{8}$$

This quantity is zero for pure states and positive for mixed states (mixed states require more information than pure to be fully specified) and so (8) measures the deviation from a pure state behavior. This quantity is also time independent because the dynamics of ρ is governed by unitary transformation.

If we are thinking about correlation of a two particle system **von Neumann index correlation** I_C [4] is able to quantify that. Based on (8) it has the form

$$I_C = S_a + S_b - S \tag{9}$$

where $S_{a(b)} = S(Tr_{b(a)}\rho)$ and the reduced density operators $Tr_{b(a)}\rho$ in respective matrix representation have the elements

$$\begin{aligned} (Tr_b\rho)_{ij} &= \sum_\mu \langle i\mu|\rho|j\mu\rangle \\ (Tr_a\rho)_{\mu\nu} &= \sum_i \langle i\mu|\rho|i\nu\rangle \end{aligned} \tag{10}$$

$\{|i\rangle\}$, $\{|\mu\rangle\}$ define the respective orthonormal base of the state space of a, b.

The Araki-Lieb inequality [4]

$$|S_a - S_b| \leq S \leq S_a + S_b$$

implies that $I_C \geq 0$ and is precisely zero only for uncorrelated systems.

If we order the components of the system so that $S_a \geq S_b$ then Araki-Lieb implies $I_c \leq 2S_b$. The maximum possible value I_C will be $2S_b$. Consequently from (9) the maximum degree of correlation is obtained when $S_a = S_b$ and $S = 0$ i.e. the total state is pure. We can conclude that two particle system which is maximally correlated must be pure.

Another useful measure of correlation is the **Shannon entropy** $\tilde{S}(\rho)$ [4] a special form of the von Neumann entropy $S(\rho)$ for diagonal form of the density matrix ρ defined by

$$\tilde{S}(\rho) = -\sum_{\mathbf{i}} \rho_{\mathbf{ii}} ln(\rho_{\mathbf{ii}}) \tag{11}$$

where $\rho_{\mathbf{ii}}$ are diagonal elements of ρ in the matrix representation with respect to the orthonormal basis $\{|i\rangle\}$ of state space. This quantity is dependent of the choice of coordinates

and is zero only for separable states in the given basis.

Shannon's index correlation [4] for two-component system C is based on (10), (11) and defined as

$$\tilde{I}_C = \tilde{S}(Tr_b\rho) + \tilde{S}(Tr_a\rho) - \tilde{S}(\rho) \tag{12}$$

where $\tilde{I}_C$ measures the amount of information about the system which is lost when the properties of both components are measured separately again and is dependent on the choice of coordinates. $\tilde{I}_C \geq 0$, and is zero only for separable states.

Let us make the next step and let us deal with entanglement measures. In general there exist two approaches how to define them. The **operational approach** [6] says that system is more entangled if it allows for better performance of some task (impossible without entanglement), one such task can be for instance teleportation.

The **abstract approach** [6] tries to introduce entanglement measures from certain properties which must be fulfilled.

Both approaches are studied for two kinds of systems, finite and asymptotic. A finite system is single, but generally composed of subsystems. Asymptotic systems are understood as a sequence of finite systems or likely the source of them. We will not deal with asymptotic systems here, our goal will be to study the one two-or more particle systems.

Let us first study the entangled states under certain special transformations. Let us study the possible physical operations first. They must map the density matrix ρ onto a density matrix $\Lambda(\rho)$ i.e. positivity and trace preserving is necessary

$$\rho \geq 0 \Rightarrow \Lambda(\rho) \geq 0,\ Tr(\Lambda(\rho)) = 1 \tag{13}$$

These mappings are said to be **positive and trace preserving** [6], but it is not enough to guarantee physical realizability. Let a, b denote the subsystems of the composed system in state ρ_{ab}. If components are correlated the operation on system can be described by the mapping $\Lambda = \Lambda_a \otimes \Lambda_b$, where $\Lambda_{a,b}$ represent the processes on both a, b. Another necessary condition for physical realization of the maps implies: their tensor product must be some positive mapping too. The positive maps which fulfill both conditions are said to be **completely positive** [6]. The following condition of complete positivity (CP) of Λ was proven [7]: Λ belongs to the family of CP only if $\Lambda \otimes I_N$ is positive for any N natural. I_N is an identity operator on $N \times N$ matrices.

Finally, let us point that for quantum information processes the trace preserving maps are of particular interest. Let us consider the three mappings.

(*i*) $\rho \to \rho \otimes \rho'$ i.e. process of the enlargement of the system ρ by ρ' is applied.

(*ii*) $\rho \to U\rho U^\dagger$, where U is the unitary operator on the $\mathcal{H}$ i.e. the unitary transformation U is applied on the system ρ.

(*iii*) $\rho_{ab} \to \rho_a$ resp. $\rho_{ab} \to \rho_a$ i.e. process of reduction of the system ρ_{ab} into subsystem ρ_a resp. ρ_b is applied.

These maps are completely positive and trace preserving. Maps (i), (iii) change the dimension of the total system, (ii) preserves it. It was shown in [9] that every physically realizable mapping can be written as a composition of these mappings. If we add a mapping which is measurement result selective, we obtain the whole class of completely positive mappings.

It was shown in [7] that not all positive mappings are completely positive. Differences appear when they act on an entangled states.
Let us introduce Λ, a positive mapping. Let us denote $\sum_i p_i \rho_a^i \otimes \rho_b^i$ a two-component separable state where $\rho_{a,b}^i$ are density matrices of a, b systems. Let Λ act on ρ_b^i, then

$$(I \otimes \Lambda)(\sum_i p_i \rho_a^i \otimes \rho_b^i) = \sum_i p_i \rho_a^i \otimes \Lambda(\rho_b^i) \geq 0,$$

because $\Lambda(\rho_b^i) \geq 0$ with regard to the positivity of a Λ. So if the two component state is separable, there is no difference between the action of positive and complete positive mappings. The difference appears when acting on entangled states. This is why positive mappings are useful tools for checking the entanglement of given state.
The following statement was proven in [7]: the two component state ρ is entangled only if there exist a positive mapping Λ for which $(I \otimes \Lambda)(\rho)$ is not positive.

Our goal to define proper entanglement measure need more information yet. Physically possible states can be treated as **state to ensemble** and **ensemble to state** [6]. The input state is denoted as ρ_{in} and the ensemble $\{p_i, \rho_{out}^i\}$ is a mixture of the states with respective probabilities.
State to state, completely positive and trace preserving operations are so called **proper operations** [6]. State to ensemble mapping is in general described by a class of completely positive maps i.e.

$$\Lambda_i : \ \Lambda_i(\rho) = \sum_j V_j^i \rho {V_j}^{i\dagger}$$

where $p_i = Tr(\Lambda_i \rho_{in})$, trace-decreasing i.e. $\sum_{ij} V_j^i V_j^i \leq I$, I identity operator i.e. $Tr(\Lambda\rho) \leq Tr(\rho) = 1$. **Pure operations** [6] are state to ensemble for which $\Lambda_i(\rho) = V^i \rho V^i$. The only pure proper operations are unitary and isometric, for example the procedure of adding some pure state.

An interesting class of operations are **LOCC** transformations [6] formed by the application of local operations by first participant, sending the result to another participant by classical information channel and following application of another local operations based on the received information by another participant. Remember we used such operations in examples of quantum coding and teleportation. It is interesting that proper LOCC can not be done without composing state to ensemble and ensemble to state operation.
With our knowledge we can divide the states into two basic complementary sets: **distillable** and **non-distillable** [6]. A state belongs to the distillable set when there exist a sequence of physically possible LOCC - so called **purification protocol** [6] - which drives it to the desirable entangled state. It is easy to see that any separable state can not be transformed to an entangled under LOCC. On the other hand it was shown in [7] that not all the entangled states are distillable, these are said to be the **bound entangled** . We can write the following relations.

$$\text{states} = \text{separable} \cup \text{entangle} = \text{distilable} \cup \text{non-distilable},$$

$$\text{separable} \cap \text{entangle} = \text{distilable} \cap \text{non-distilable} = 0,$$

$$\text{entangle} \cap \text{non-distilable} = \text{bound-entangle} \neq 0.$$

The necessary conditions of separability are useful to tell us whether a state is entangled or not. The **Peres's criterium** [9] was derived for two particle quantum systems ab with components a, b. It states, that the necessary condition of separability of the state with density matrix ρ is the positivity of the partial transpose toward each component a, b i.e. operators $\rho^T_{a(b)}$ defined by

$$(\rho^T_a)_{i\mu,j\nu} = \langle j\mu|\rho|i\nu\rangle,$$

$$(\rho^T_b)_{i\mu,j\nu} = \langle i\nu|\rho|j\mu\rangle$$

must be positive. Another, weaker condition, based on Schwarz inequality [1], was found in [10]: the necessary condition of separability for general two component quantum system represented by density matrix ρ is

$$\sqrt{\langle j_1, j_2|\rho|j_1, j_2\rangle}\sqrt{\langle k_1, k_2|\rho|k_1, k_2\rangle} \geq \sqrt{\langle \pi^1_1, \pi^2_1|\rho|\pi^1_2, \pi^2_2\rangle}$$

where $|j_1, j_2\rangle$ represent an orthonormal basis of the state space and π^i is the permutation of the two-component sets j_i, k_i for all $i \in \{1, 2\}$.

With our knowledge about entangled states and about physical operation we can summarize the operational postulates for the entanglement measure E on finite system with

state space $\mathcal{H}$ and define proper entangled measure analytically. The general conditions for an entanglement measure [6] can be postulated as follows. For the measures of entanglement E the conditions of monotonicity are required.

M1: For any proper LOCC, state to ensemble operation T and any state ρ: $E(T(\rho)) \leq E(\rho)$.

M2: Let an LOCC, state to ensemble operation produce the output $\{p_i, \rho_{out}^i\}$ from input state ρ_{in}. We require

$$\sum_i p_i E(\rho_{out}^i) \leq E(\rho_{in}).$$

M3.a: Let local, pure operation produces an output $\{p_i, \rho_i\}$ from input state ρ_{in}. We require

$$\sum_i p_i E(\rho_{out}^i) \leq E(\rho_{in}).$$

M3.b: E is convex

$$E(\sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i).$$

The condition of separability on separable states is required.

S1: For any separable state ρ: $E(\rho) = 0$.

To find the proper measure of entanglement based on the just mentioned steps is not an easy task. However there are known examples [6].

Entanglement of distillation

E_D of the state ρ is defined as the asymptotic ratio

$$E_D(\rho) = \sup_{\mathcal{P}} \frac{m}{n}$$

of m sufficiently distilated pairs via the purification protocol $\mathcal{P}$ toward the respective fixed entangled state σ and n denotes the number of unperfect states ρ.

The success of the protocol is quantified by the projection

$$F^{out} = Tr(\sigma \rho^{out} \sigma^{\dagger}) \tag{14}$$

of the output state ρ^{out} toward the σ. The protocol $\mathcal{P}$ is successful if $F \longrightarrow 1$.

Entanglement cost

$E_{\mathcal{D},\mathcal{S}}$ is defined by following equation

$$E_{\mathcal{D},\mathcal{S}}(\rho) = \inf_{\sigma \in \mathcal{S}} \mathcal{D}(\rho, \sigma)$$

where $\mathcal{D}$ means a measure on respective Hilbert space, $\mathcal{S}$ is the set of all separable states.

2.2 Special classes of states

Purification protocols involve several special types of density matrices. Let us introduce some of them.

Isotropic states

Isotropic states [6] are defined by the D-dimensional density matrix

$$\rho_\alpha = (1-\alpha)\frac{I}{D^2} + \alpha P \tag{15}$$

where $P = |\Phi^+\rangle\langle\Phi^+|$, $|\Phi^+\rangle = \frac{1}{\sqrt{D}}\sum\limits_i |i\rangle \otimes |i\rangle$. States (15) are $U \otimes U^*$ invariant for an arbitrary unitary U ($*$-means the complex conjugate) as can be proven by direct calculation.

$$U \otimes U^* |\Phi^+\rangle = \frac{1}{\sqrt{D}} \sum_{ijk} u_{ji} u^*_{ki} |j\rangle \otimes |k\rangle =$$

$$= \frac{1}{\sqrt{D}} \sum_{ijk} u_{ji} u^{-1}_{ik} |j\rangle \otimes |k\rangle = \frac{1}{\sqrt{D}} \sum_{jk} \delta_{jk} |j\rangle \otimes |k\rangle = \frac{1}{\sqrt{D}} \sum_{k} |k\rangle \otimes |k\rangle = |\Phi^+\rangle.$$

The condition of positivity is fulfilled for

$$\frac{1}{D^2-1} \leq \alpha \leq 1.$$

Using the fidelity (14)

$$F = Tr(\rho_\alpha P) = D\alpha - 2\alpha + 1$$

we can rewrite (15) in form

$$\rho_\alpha(F) = \frac{D^2}{D^2-1}[(1-F)\frac{I}{D^2} + (F - \frac{1}{D^2})P], \ 0 \leq F \leq 1. \tag{16}$$

The condition of separability and Peres's necessary condition of separability give

$$F \leq \frac{1}{D}.$$

These states are the only $U \otimes U^*$ invariant, where U is any unitary mapping on C^D, as was shown in [7].

Werner states

Werner states are defined by D-dimensional density matrix

$$\rho_p = p\frac{P_-}{N_-} + (1-p)\frac{P_+}{N_+},\ 0 \leq p \leq 1 \tag{17}$$

where $P_\pm$ are the projectors on the symmetric resp. antisymmetric subspaces of $\mathcal{H}$. $P_\pm$ are defined by equations

$$P_+(|ij\rangle \pm |ji\rangle) = \{_0^{(|ij\rangle+|ji\rangle)}$$

$$P_-(|ij\rangle \pm |ji\rangle) = \{_{(|ij\rangle-|ji\rangle)}^0.$$

It follows that

$$P_\pm = \frac{1}{2}\sum_{ij}(|ij\rangle \pm |ji\rangle)\langle ij| = \frac{1}{2}(1 \pm \sum_{ij}|ij\rangle\langle ji|).$$

The dimensions of respective subspaces are

$$N_\pm = \frac{D^2 \pm D}{2}.$$

For $p \leq 1/2$ Werner states fulfill Peres's separability criterium.
These states are $U \otimes U$ invariant for arbitrary unitary U.

$$U \otimes U\rho_p U^\dagger \otimes U^\dagger = U \otimes U[\frac{p}{N_-}(1 - |ji\rangle\langle ij|) + \frac{1-p}{N_+}(1 + |ji\rangle\langle ij|)]U^\dagger \otimes U^\dagger = \rho_p,$$

because for $(U)_{ij} = u_{ij}$

$$U \otimes U\sum_{ij}|ij\rangle\langle ji|U^\dagger \otimes U^\dagger = \sum_{klmnij} u_{ki}u_{lj}u^\star_{ni}u^\star_{mj}|kl\rangle\langle nm| = \sum_{klmn}\delta_{kn}\delta_{lm}|kl\rangle\langle nm| = \sum_{kl}|kl\rangle\langle kl|.$$

The set of density matrices which are $U \otimes U$ invariant for arbitrary unitary U is composed from matrices in form (17). It implies from following discussion. Let ρ is a density matrix invariant under $U \otimes U$. Let us choose U so that it multiplies arbitrary, but fixed, $|k\rangle$ from orthonormal base of C^D by -1 and other states of the ON-basis stay unchanged under U. It implies that nonzero elements of ρ are the only $\langle ij|\rho|ij\rangle$, $\langle ij|\rho|ji\rangle$, $\langle ii|\rho|jj\rangle$ for $i \neq j$ and $\langle ii|\rho|ii\rangle$.
Let us choose now U so that it multiplies arbitrary, but fixed vector, $|k\rangle$ from orthonormal base of C^D by imaginary unit i and other states of the ON-basis stay unchanged under U. It implies that nonzero elements of ρ are only the $\langle ii|\rho|ii\rangle$ and $\langle ij|\rho|ij\rangle$, $\langle ij|\rho|ji\rangle$ for all $i \neq j$.
Elements of each group must be equal because we can define U such that it flip the $|i\rangle$, $|j\rangle$ and other states stay unchanged under U.
It implies that the $\rho = aA + bB + cC$ where $A = \sum_i |ii\rangle\langle ii|$, $B = \sum_{i\neq j}|ij\rangle\langle ij|$, $C = \sum_{i\neq j}|ij\rangle\langle ji|$.
Hermiticity of ρ implies that a, b, c must be real.

Let us choose U defined in respective matrix representation by the form $U = \widetilde{U_2} \oplus I_{D-2}$ where matrix U_2 represent single rotation

$$U_2 = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}$$

on $\mathcal{H}_1 \equiv [|i\rangle, |j\rangle]_\lambda$ for respective arbitrary, but fixed $|i\rangle$, $|j\rangle$ from ON-base. I_{D-2} is the projector onto the orthogonal complement $\mathcal{H}_1$ on the C^D. It can be verify that term A is not invariant under $U \otimes U$, it implies that a must be linearly dependent on b and c somehow. Because $Tr(\rho) = 1$, the number of free parameters decreases for one. Werner states (17) are $U \otimes U$ invariant, so we can conclude that (17) compose the set of all the $U \otimes U$ states.

Let us now discuss classes of one parametric states for more component states.

Symmetric and antisymmetric states

Let us define:

$$\rho = (1-p)\frac{1}{D^N} I + p|\Psi\rangle\langle\Psi|, \tag{18}$$

where I is the identity operator on

$$\mathcal{H} = \underbrace{C^D \otimes ... \otimes C^D}_{N\times}, \ 0 \leq p \leq 1$$

and

$$|\Psi\rangle = |S\rangle = \tfrac{1}{\sqrt{D}} \textstyle\sum_j \underbrace{|j\rangle \otimes ... \otimes |j\rangle}_{N\times}, \tag{18a}$$

N, D arbitrary resp.

$$|\Psi\rangle = |A\rangle = \tfrac{1}{\sqrt{D!}} \textstyle\sum_\pi sgn(\pi) \underbrace{|\pi_1\rangle \otimes ... \otimes |\pi_N\rangle}_{N\times}, \tag{18b}$$

where π is permutations of D elements set i.e. in this case $N = D$.

The states defined by (18a), (18b) are said to be symmetric (not general) resp. antisymmetric (general) states with completely unpolarized mixture. Bell states are a special case of them. Let us ask which of these states are completely separable.
It was shown in [5] that a necessary and sufficient condition of separability for symmetric states is

$$p \leq [1 + D^{N-1}]^{-1}.$$

The necessary condition of separability for the antisymmetric states is

$$p \leq [1 + \frac{(D-1)!}{D^{D-1}}]^{-1}.$$

Based on construction of some purification protocol we can shown, that this condition is not sufficient. Before we do that let us ask if there exist some class of mappings for which symmetric resp. antisymmetric states are the only stable states.

Symmetric states

If U for arbitrary, but fixed $|k\rangle$ from orthonormal base of C^D and $\mu \in \mathbf{C}$, $|\mu| = 1$ preserves $|k\rangle$ i.e. $U|k\rangle = \mu|k\rangle$ and others vectors of the base stay unchanged under U then symmetric states are invariant under $U \otimes ... \otimes U$.
Symmetric states are also invariant under $U \otimes ... \otimes U$ where $U|k\rangle = |l\rangle$, $U|l\rangle = |k\rangle$ for arbitrary, but fixed, two vectors $|k\rangle$, $|l\rangle$ from an orthonormal base of C^D and other vectors of the base leave unchanged under U.
We know that isotropic and Werner states are the only states invariant under some special class of operations. This is useful for construction of purification protocol. The map $U_1 \otimes ... \otimes U_N$ which preserves the symmetric states must fulfill following equation

$$\sum_{ij} u^1_{k_1 i} ... u^N_{k_N i} u^{1*}_{l_1 j} ... u^{N*}_{l_N j} = \delta_{k_1,...,k_N} \delta_{l_1,...,l_N}$$

where $u^i_{jk} = (U_i)_{jk}$, $i, j, k_p, l_p \in \{1, ..., D\}$. It implies D^{2N} nonlinear equations for $N.(D(D-1))$ parameters. Such equation is not easy to solve. I am going to find such maps in future with the help of the theory of representation of groups.

Antisymmetric states

The map $U_1 \otimes ... \otimes U_N$ which preserves the antisymmetric states must fulfill following equation

$$\sum_{\sigma\pi} sgn(\pi) sgn(\sigma) u^1_{i_1 \pi_1} ... u^D_{i_D \pi_D} u^{1*}_{j_1 \sigma_1} ... u^{D*}_{j_D \sigma_D} = sgn(i_1, ..., i_D) sgn(j_1, ..., j_D)$$

where $\pi_p, \sigma_p, i_p, j_p \in \{1, ..., D\}$. It means $(D!)^2$ equations for $D^2(D-1))$ parameters in general. If we define

$$U_1 = ... = U_D = U, \tag{19}$$

we realize that

$$U \otimes ... \otimes U|A\rangle = \frac{1}{\sqrt{D!}} \sum_{\pi} \varepsilon_\pi U|\pi_1\rangle \otimes U.... \otimes U|\pi_D\rangle =$$

$$= \frac{1}{\sqrt{D!}} \sum_{i_1 \ldots i_D} \sum_{\pi} sgn(\pi) u_{i_l \pi_1} \ldots u_{i_D \pi_D} |i_1 \ldots i_N\rangle =$$

$$= \frac{1}{\sqrt{D!}} \sum_{i_1 \ldots i_D} \sum_{\pi} sgn(i_1 \ldots i_D) sgn(\pi) u_{1\pi_1} \ldots u_{D\pi_D} |i_1 \ldots i_N\rangle =$$

$$= \det U. |A\rangle = |A\rangle$$

(U is unitary implies that $\det(U) = 1$).
Unitary transformation $U \otimes \ldots \otimes U$ preserves every antisymmetric state. I want to point out that class of $U \otimes \ldots \otimes U$ will help us to construct purification protocol for tree particles.

2.3 Construction of purification protocols

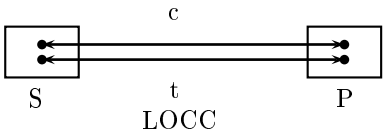

Fig.4: Scheme for pur. protocol

Scheme of general two particle systems purification protocol is given on fig.4. Participants S and P share the set of imperfect pairs at the beginning. They divide them to so called control (c) and target (t) pairs. Each particle from control resp. target pair belongs to S and P. S and P perform LOCC on respective particles. LOCC contains the measurement of the state of target particles, according to results the source pairs are held or destroyed. If source pairs are held they become source of target and control pairs for next step of protocol. For communication of results S and P use classical communication channel. The finally outputs are purified source pairs.
Purification protocols can be divide into two subclasses.

Non-deterministic purification protocols

The whole ensemble is processes with a set of randomly chosen unitary transformations in such a way that the set effort is described by the so called depolarization channel.

The Bennet-Brassard protocol (B-B)

The protocol of B-B [11] was designed for the purification of the two qubits system toward the entangled state $|\Psi^-\rangle$ of Bell base(3). B-B protocol is designed from following steps.

S1: Randomly chosen sequence of $\{B_x, B_y, B_z\}$ where

$$B_x(\pi/2) = R_x(\pi/2) \otimes R_x(\pi/2),$$

$$B_y(\pi/2) = R_y(\pi/2) \otimes R_y(\pi/2),$$

$$B_z(\pi/2) = R_z(\pi/2) \otimes R_z(\pi/2) \tag{20}$$

and

$$R_x(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & \sin\alpha \\ 0 & -\sin\alpha & \cos\alpha \end{pmatrix},$$

$$R_y(\alpha) = \begin{pmatrix} \cos\alpha & 0 & -\sin\alpha \\ 0 & 1 & 0 \\ \sin\alpha & 0 & \cos\alpha \end{pmatrix},$$

$$R_z(\alpha) = \begin{pmatrix} \cos\alpha & \sin\alpha & 0 \\ -\sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is applied by S and P bilaterally on each source and target pair. The (20) have sense because the qubit state can be (according to [8]) represent in form

$$|\psi\rangle = \frac{1}{2}(I + \mathbf{P}.\sigma)$$

where $\mathbf{P} = (P_x, P_y, P_z)$ is polarization vector and $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ are so called Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{21}$$

(20) map (3) onto itself as

$$B_x(\pi/2): \ \Psi^- \leftrightarrow \Psi^-, \ \Phi^- \leftrightarrow \Phi^-, \ \Psi^+ \leftrightarrow \Phi^+$$

$$B_y(\pi/2): \ \Psi^- \leftrightarrow \Psi^-, \ \Phi^+ \leftrightarrow \Phi^+, \ \Psi^+ \leftrightarrow \Phi^-$$

$$B_z(\pi/2): \ \Psi^- \leftrightarrow \Psi^-, \ \Psi^+ \leftrightarrow \Psi^+, \ \Phi^+ \leftrightarrow \Phi^-.$$

It implies that after S1 the pairs are in states

$$\rho = F|\Psi^-\rangle\langle\Psi^-| + \tfrac{1-F}{3}|\Psi^+\rangle\langle\Psi^+| + \tfrac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \tfrac{1-F}{3}|\Phi^+\rangle\langle\Phi^+| \tag{22}$$

where $F = \langle\Psi^-|\rho|\Psi^-\rangle$ is fidelity (14) according to $|\Psi^-\rangle$. ρ becomes a Werner state (16) where $p = F$.

S2: Participants apply $\sigma_y \otimes 1$. According to (21) it can be shown that

$$\sigma_x \otimes 1: \ \Psi^{\pm} \leftrightarrow \Phi^{\pm},$$

$$\sigma_y \otimes 1: \ \Psi^{\pm} \leftrightarrow \Phi^{\mp},$$

$$\sigma_z \otimes 1: \ \Psi^{\pm} \leftrightarrow \Psi^{\mp}, \ \Phi^{\pm} \leftrightarrow \Phi^{\mp}.$$

It implies that after S2 the pairs are in states

$$\rho = F|\Phi^+\rangle\langle\Phi^+| + \tfrac{1-F}{3}|\Psi^+\rangle\langle\Psi^+| + \tfrac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \tfrac{1-F}{3}|\Psi^-\rangle\langle\Psi^-|. \quad (23)$$

S3: Participants apply $BXOR$ (A1) and measure the polarizations in z axes on every particle of the target systems. Control pair survive if the polarizations of the particles of respective target pair have the same orientation. Such situation happens when target system is in $|\Phi^{\pm}\rangle$ i.e. with probability $p(F) = F + (1-F)/3 = (1+2F)/3$. The control systems become in states

$$\tfrac{1}{F^2+\frac{2F(1-F)}{3}+5\frac{(1-F)^2}{9}}((F^2+\tfrac{1-F^2}{9})|\Phi^+\rangle\langle\Phi^+| + \tfrac{2F(1-F)}{3}|\Phi^-\rangle\langle\Phi^-| + 3\tfrac{1-F^2}{9}|\Psi^-\rangle\langle\Psi^-| + \tfrac{1-F^2}{9}|\Psi^+\rangle\langle\Psi^+|). \quad (24)$$

S4: The operation $\sigma_y \otimes 1$ is used on the surviving control systems in state (24). Participants share pairs in states

$$\rho = \tfrac{1}{F^2+\frac{2F(1-F)}{3}+5\frac{(1-F)^2}{9}}((F^2+\tfrac{1-F^2}{9})|\Psi^-\rangle\langle\Psi^-| + \tfrac{2F(1-F)}{3}|\Psi^+\rangle\langle\Psi^+| + 3\tfrac{1-F^2}{9}|\Phi^+\rangle\langle\Phi^+| + \tfrac{1-F^2}{9}|\Phi^-\rangle\langle\Phi^-|). \quad (25)$$

According to (14) and (25) the fidelity of the output after n steps of procedure is given by the recurrent form

$$F_{n+1} = \frac{F_n^2 + \frac{1-{F_n}^2}{9}}{F_n^2 + \frac{2F_n(1-F_n)}{3} + 5\frac{1-{F_n}^2}{9}}.$$

Behavior of output fidelity is shown in fig.5. For $F_{in} \in (1/2; 1]$ the $F_n \to 1$, it coincides with Peres criterium.

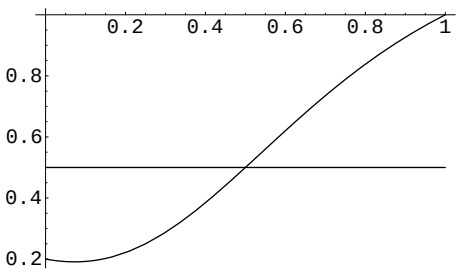

Fig.5: $F_{n+1} = F_n$ for B-B protocol.

Let us discuss the efficiency η of the protocol i.e. ratio of the number of output, purified states $N_{out}(N_{in}, n)$ after n steps of protocol and number of the input, impure states N_{in}. Source pairs are divided into control and target pairs each consist from $N_{in}/2$ pairs. Step S2 do not change the number of pairs in protocol. Control pair survive S3 with probability $p(F)$, because of the polarization measurement. The number of output pairs is $N_{in}/2.p(F)$. After n iterations of the protocol we obtain

$$\frac{N_{in}}{2^n}\prod_{i=1}^{n} p(F_i)$$

output distilled systems, so

$$\eta = \frac{1}{2^n}\prod_{i=1}^{n} p(F_i).$$

The Horodecki protocol

The Horodecki protocol [6] is generalization of the B-B protocol, designed for the purification of two D-qudits systems to the given entangled state

$$|\psi\rangle = \textstyle\sum_{mn} a_{mn}|m\rangle \otimes |n\rangle. \tag{26}$$

In each step of B-B protocol the pairs are in Werner states (17). During the Horodecki protocol the pairs are in isotropic states (15).

The Horodecki protocol is designed from following steps

S0: At the beginning the participants apply $A \otimes 1$ on each pair, such that

$$|\psi\rangle = A \otimes I|\Phi^+\rangle,$$

$|\Phi^+\rangle$ has form (18 a). It is easy to verify that $(A)_{mn} = a_{mn}$ where $|\psi\rangle = \sum_{mn} a_{mn}|m\rangle \otimes |n\rangle$ and $\{|m\rangle\}$ is respective orthonormal base of qudit state space.
Pairs become to the isotropic state

$$\rho' = \frac{A^\dagger \otimes I\rho A \otimes I}{Tr(A^\dagger \otimes I\rho A \otimes I)}. \tag{27}$$

The fidelity F of the (27) toward the $|\Psi\rangle$ is the same as fidelity ρ toward the $|\psi\rangle$ i.e. $\langle\psi|\rho|\psi\rangle = \langle\Phi^+|\rho'|\Phi^+\rangle$.

Following steps are iterated in protocol.

S1: Randomly chosen $U \otimes U^{\star}$ is applied. State ρ' is mapped onto

$$\rho_{\alpha} = \frac{(1-\alpha)}{D^2} I + \alpha P$$

where

$$\alpha = \frac{D^2 F - 1}{D^2 - 1},$$

it can be seen from (16).

S2: Bilateral $GXOR$ (A1) is applied by participants. Control pair is hold if the respective target particles are measured in the same state. It implies that an isotropic state ρ_{α} is mapped onto isotropic state $\rho_{\alpha'}$ where

$$\alpha' = \alpha \frac{[D(D+1)-2]\alpha + 2}{(D+1)[1+(D-1)\alpha^2]}. \tag{28}$$

S3: Protocol ends with applying of $A \otimes 1$. The outputs are mapped onto desired $|\psi\rangle$.

Probability that performance S2 is successful is given by

$$p(\alpha) = \alpha + (1-\alpha)/D = (1 + (D-1)\alpha)/D$$

Dependence $\alpha'(\alpha)$ is simulated in fig.6. Fidelity is monotonic increasing for initial $\alpha \in [1/(D+1), 1]$. If the input fidelity of the system is bigger than $1/D$ the output fidelity increase, in accord with the reduction criteria. Efficiency η of the protocol is

$$\eta = \frac{1}{2^n} \prod_{i=1}^{n} p(\alpha_i),$$

n denotes the number of step of iteration.

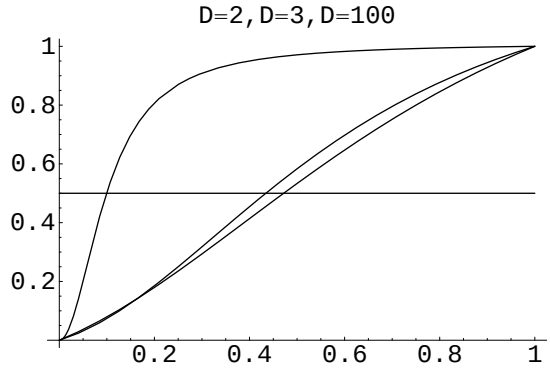

Fig.6: $\alpha'(\alpha)$ in Horodecki protocol.

2.4 Deterministic protocol and nonlinear mapping of density matrices

Non-deterministic protocols require a large number transformations to be applied. New approach was found to eliminate the use of depolarization on each step, deterministic protocols were proposed.

Deutsch protocol-Benneth-Brasard's deterministic analogue

was designed for the purification of the two qubits system towards the entangled state $|\Psi^-\rangle$ of Bell base (3) [12]. Nondeterministic operation included in each step of B-B are not needed, instead the nonlinear mapping are used.

Deutsch protocol is designed from following steps

S1: Participants apply the

$$(1_c \otimes P_-)_S (1_c \otimes P_-)_P U_S U_P \tag{29}$$

onto own source and target particles where

$$U_S = \begin{pmatrix} -i\sigma_y & 0 \\ 0 & 1 \end{pmatrix},$$

$$U_P = \begin{pmatrix} i\sigma_y & 0 \\ 0 & 1 \end{pmatrix}$$

are unitary transformations according to

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

$P_- = |0\rangle_t\langle 0|_t$ is projection onto state 0 of respective particle of target system.
(29) maps the input states ρ onto

$$\rho' = \frac{1}{\sum\limits_i \rho_{ii}^2} \begin{pmatrix} \rho_{11}^2 & -\rho_{12}^2 & \rho_{13}^2 & -\rho_{14}^2 \\ -\rho_{21}^2 & \rho_{22}^2 & -\rho_{23}^2 & \rho_{24}^2 \\ \rho_{31}^2 & -\rho_{32}^2 & \rho_{33}^2 & -\rho_{34}^2 \\ -\rho_{41}^2 & \rho_{42}^2 & -\rho_{43}^2 & \rho_{44}^2 \end{pmatrix} \tag{30}$$

The probability of success of S1 is

$$p(\rho) = \sum_i \rho_{ii}^2. \tag{31}$$

S2: Participants apply $B_x(\pi/2)$ (20) on their remaining control particles.

Repeating steps S1, S2 they obtain purification protocol toward the desired state $|\Psi^-\rangle$ of (3). Projection on target pair in each step of the procedure decrease the number of desirable purified states. The efficiency η after n steps of iterations is given by

$$\eta = \frac{1}{2^{2n}} \prod_{i=1}^{n} p_{\rho_i}.$$

Comparing of the protocol with B-B was done in [11], let us point out that Deutsch protocol purify all the states with initial fidelity greater then with coincidence the Peres criteria.

Chapter 3

General deterministic protocol

Using the $GXOR$ gate [A1] we can define an interesting class of nonlinear maps which help us to construct the deterministic purification protocols [13].

Let us assume that we have the same number of control and target D-qudits systems in states

$$\sigma^c = \sum_{ij}^{D-1} \sigma_{ij}^c |i\rangle_c\langle j|_c,$$

$$\sigma^t = \sum_{ij}^{D-1} \sigma_{ij}^t |i\rangle_t\langle j|_t,$$

respective Hilbert spaces are denoted as $\mathcal{H}^c$, $\mathcal{H}^t$. Let us define the operator

$$T : \mathcal{B}(\mathcal{H}^c) \otimes \mathcal{B}(\mathcal{H}^t) \to \mathcal{B}(\mathcal{H}^c) \otimes \mathcal{B}(\mathcal{H}^t)$$

as

$$T(\sigma^c, \sigma^t) = \frac{A(\sigma^c \otimes \sigma^t)A^\dagger}{Tr(A(\sigma^c \otimes \sigma^t)A^\dagger)} \tag{32}$$

where

$$A = (1_c \otimes P)GXOR_{ct},$$

$P = |p\rangle_t\langle p|_t$ denotes a projector onto the $|p\rangle_t$ of the target system.
(32) can be written in form

$$T(\sigma^c, \sigma^t) = \frac{A(\sigma^c \otimes \sigma^t)A^\dagger}{Tr(A(\sigma^c \otimes \sigma^t)A^\dagger)} = (1_c \otimes P)GXOR_{ct}(\sigma^c \otimes \sigma^t)GXOR_{ct}(1_c \otimes P)/Tr(...) =$$

$$= (1_c \otimes P)GXOR_{ct}(\sum_{ijkl}^{D-1} \sigma_{ij}^c \sigma_{kl}^t |i\rangle_c|k\rangle_t\langle j|_c\langle l|_t)GXOR_{ct}(1_c \otimes P)/Tr(...) = \sigma_{out}^c \otimes P$$

where

$$\sigma_{out}^c = \frac{\sum_{i,j}^{D-1} \sigma_{ij}^c \sigma_{i-p,j-p}^t |i\rangle_c\langle j|_c}{\sum_{i}^{D-1} \sigma_{ii}^c \sigma_{i-p,i-p}^t}. \tag{33}$$

For $\sigma^c = \sigma^t = \sigma$, according to (33), we obtain

$$T(\sigma, \sigma) = \sigma_{out} \otimes P$$

where

$$\sigma_{out} = \frac{\sum\limits_{i,j}^{D-1} \sigma_{ij}\sigma_{i-p,j-p}|i\rangle_c\langle j_c|}{\sum\limits_{i}^{D-1} \sigma_{ii}\sigma_{i-p,i-p}}. \tag{34}$$

The density matrix is mapped again onto a density matrix, the mapping is not injective and is nonlinear. The choice of p influence the set and type of the respective fixed points. The protocol can be further generalized. Let us suppose that we have the control and N target systems, each composed from M pairs of D-qudits, in the states

$$\sigma^c = \sum_{\mathbf{ij}} \sigma^c_{\mathbf{ij}}|\mathbf{i}\rangle_{\mathbf{c}}\langle\mathbf{j}|_{\mathbf{c}},$$

$$\sigma^t = \sum_{\mathbf{ij}} \sigma^c_{\mathbf{ij}}|\mathbf{i}\rangle_{\mathbf{t}}\langle\mathbf{j}|_{\mathbf{t}}$$

where $\mathbf{i} = (i_1, ..., i_M), \mathbf{j} = (j_1, ..., j_M)$. Let us define

$$A = (1_c \otimes P) \prod_{j=1}^{M} \prod_{i}^{N} GXOR^{(j)}_{ct_i} \tag{35}$$

where

$$P = \prod_{i=1}^{N} \otimes P_{t_i}$$

and

$$P_{t_i} = |\mathbf{p_i}\rangle_{\mathbf{t_i}}\langle\mathbf{p_i}|_{\mathbf{t_i}}$$

represent a projector onto i-th state of the target system. $GXOR^{(j)}_{ct_i}$ denotes $GXOR$ onto the j-th component of the control and of the i-th target system. According to (35) the action of (32) has the form

$$T(\sigma^c, \sigma^t, ..., \sigma^t) = (1_c \otimes P) \prod_{j=1}^{M} \prod_{i=1}^{N} GXOR^{(j)}_{ct_i} (\sigma^c \otimes \sigma^t)((1_c \otimes P) \prod_{j=1}^{M} \prod_{i=1}^{N} GXOR^{(j)}_{ct_i})^\dagger / Tr(...) =$$

$$= (1_c \otimes P) \prod_{j=1}^{M} \prod_{i=1}^{N} GXOR^{(j)}_{ct_i} (\sum_{\mathbf{kl}} \sigma^c_{\mathbf{kl}}|\mathbf{k}\rangle\langle\mathbf{l}| \otimes \sum_{\mathbf{k_1 l_1}} \sigma^t_{\mathbf{k_1 l_1}}|\mathbf{k}_1\rangle\langle\mathbf{l}_1| \otimes \sum_{\mathbf{k_2 l_2}} \sigma^t_{\mathbf{k_2 l_2}}|\mathbf{k_2}\rangle\langle\mathbf{l_2}| \otimes ...$$

$$... \otimes \sum_{\mathbf{k_N}} \sigma^t_{\mathbf{k}_N \mathbf{l}_N}|\mathbf{k}_N\rangle\langle\mathbf{l}_N|)((1_c \otimes P) \prod_{j=1}^{M} \prod_{i=1}^{N} GXOR^{(j)}_{ct_i})^\dagger / Tr(...) =$$

$$= \sum_{\mathbf{kl}} \sigma^c_{\mathbf{kl}} |\mathbf{k}\rangle_c \langle \mathbf{l}|_c \otimes \sigma^t_{\mathbf{k}\ominus\mathbf{p}_1, \mathbf{l}\ominus\mathbf{p}_1} \otimes ... \otimes \sigma^t_{\mathbf{k}\ominus\mathbf{p_N}, \mathbf{l}\ominus\mathbf{p_N}} \otimes P/Tr(...)$$

where $\mathbf{i} \ominus \mathbf{p} = (i_1 \ominus p_1, ..., i_M \ominus p_M)$.

If all the target and control systems are identical and the projections onto each target system are the same too, the action has the form

$$T(\sigma, \sigma, ..., \sigma) = \frac{\sum_{\mathbf{kl}} \sigma_{\mathbf{kl}} \sigma^N_{\mathbf{k}\ominus\mathbf{p}, \mathbf{l}\ominus\mathbf{p}} |\mathbf{k}\rangle_\mathbf{c} \langle \mathbf{l}|_\mathbf{c}}{\sum_{\mathbf{k}} \sigma_{\mathbf{kk}} \sigma^N_{\mathbf{k}\ominus\mathbf{p}, \mathbf{k}\ominus\mathbf{p}}}. \tag{36}$$

The mapping has the same properties as (34), however in matrix representation its elements appear in the $N+1$-th power.

Let us discuss now the crucial steps of the deterministic protocol based on the nonlinear map T. The desirable pure states are denoted as ρ.

1. The protocol must preserve ρ, ρ is the fixed point (A2) of the first order of (34), i.e. $T(\rho, \rho, ..., \rho) = \rho$.

2. Another local unitary transformations are applied to remove unwanted density matrix admixture after the successfully application of the nonlinear mapping.

The construction of purification protocol has been done in [13] for the two D-qudits systems toward the respective element of general Bell base (A1) i.e. the deterministic analogue of Horodecki protocol was found. Let us give an example for the three particles in an antisymmetric states (18b).

The three particles antisymmetric states purification

Our goal will be to construct a purification protocol which effectively distills input impure antisymmetric states in the form

$$\sigma = \frac{\lambda}{6} |A\rangle\langle A| + |\frac{1-\lambda}{27} I \tag{37}$$

towards $|A\rangle\langle A|$ from (18b) for as small λ as possible (with respect to (14)). The Hilbert space of the system is $\mathcal{H} = C^3 \otimes C^3 \otimes C^3$. According to the 1-st step of the construction of the purification protocol, T has to preserve the state $\rho = |A\rangle\langle A|$ i.e. according to (36)

$$\rho_{\mathbf{i},\mathbf{j}} = \frac{\rho_{\mathbf{i},\mathbf{j}} (\rho_{\mathbf{i}\ominus\mathbf{p},\mathbf{j}\ominus\mathbf{p}})^N}{\sum_{\mathbf{i}} \rho_{\mathbf{i},\mathbf{i}} (\rho_{\mathbf{i}\ominus\mathbf{p},\mathbf{i}\ominus\mathbf{p}})^N} \tag{38}$$

where $\rho_{\mathbf{i},\mathbf{j}} = sgn(\mathbf{i})sgn(\mathbf{j}) \in \{0, \pm 1\}$.

Let us define $\mathbf{p} = (p_1, p_2, p_3)$. We have to determine the possible values of $\mathbf{p}$ which fulfill (38). For this purpose the mapping $\ominus : \{0,1,2\} \times i \to \{0,1,2\}$ is important. Let us point out that it maps the set $\{0,1,2\}$ onto itself for any fixed $i \in \{0,1,2\}$.

Let us discuss the possible cases. If $p_1 = p_2 = p_3 \in \{0,1,2\}$: for any permutation $\pi = (\pi_1, \pi_2, \pi_3)$ of $\{0,1,2\}$ the $\pi \ominus \mathbf{p}$ is permutation too. In case that $p_1 \neq p_2$: for any $i \in \{0,1,2\}$ exist $j \in \{1,2,3\}$, $j \neq i$ such that $p_1 \ominus i = p_2 \ominus j$. Especially for $i = 1$, $p_1 = 1$, $p_1 = 2$, is $j = 2$ and $(123) \to (0,0,3 \ominus \pi_3)$. It implies that possible choices of $\mathbf{p}$ are only those when $p_1 = p_2 = p_3 = p$. For such choices $sgn(\pi) = sgn(\pi \ominus \mathbf{p})$ and from (38), for $\mathbf{i} = \pi$ odd and $\mathbf{j} = \sigma$ even, implies that $N = 2k$, $k \in \mathbf{N}$.

Let us study T in more details and start with the behavior for large N first. We want to know for which σ the following equation

$$\lim_{N\to\infty} T(\sigma, \sigma, ..., \sigma) = |A\rangle\langle A| \tag{39}$$

is valid i.e. we want to know what is necessary for $|A\rangle\langle A|$ to be an attractor (A2) in the flow of N.
For $p = 0$ the (39) can be written in the form

$$\lim_{N\to\infty} T(\sigma, \sigma, ..., \sigma)_{\mathbf{i},\mathbf{j}} = \lim_{k\to\infty} \frac{\sigma_{\mathbf{i},\mathbf{j}}^{2k+1}}{\sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}}^{2k+1}} = \frac{1}{6} sgn(\mathbf{i})sgn(\mathbf{j})$$

equal with the condition

$$\lim_{k\to\infty} \frac{1}{\sum_{\mathbf{k}} (\frac{\sigma_{\mathbf{k},\mathbf{k}}}{\sigma_{\mathbf{i},\mathbf{j}}})^{2k+1}} = \frac{1}{6} sgn(\mathbf{i})sgn(\mathbf{j}). \tag{40}$$

Because of (37) the elements of σ are

$$\sigma_{\pi\pi} = \frac{\lambda}{6} + \frac{1-\lambda}{27} \tag{41}$$

$$\sigma_{\pi\tilde{\pi}} = \frac{\lambda}{6} sgn\pi sgn\tilde{\pi}, \ \pi \neq \tilde{\pi} \tag{42}$$

$$\sigma_{\mathbf{kl}} = \frac{1-\lambda}{27} \delta_{\mathbf{kl}}. \tag{43}$$

If we check behavior (41), (42), (43) in (40) we realize that (18b) can not be the attractor of only T with respect to (37).
Because of $i \ominus j = k \ominus j \Leftrightarrow i = k$ the solution of (39) for $p \in 1,2$ is identical with solution for the case $p = 0$. We can conclude that for large N only the T is not enough to create a purification protocol for input imperfect states in form (37).

Let us study if $|A\rangle\langle A|$ can be an attractor in the flow of $T(\sigma,...,\sigma)$ for any $\mathbf{p}$ i.e. let us study if

$$lim_{n\to\infty}\underbrace{T(...T(}_{n}\sigma,\sigma,...,\sigma)...) = |A\rangle\langle A|. \tag{44}$$

The complicated analytical behavior of (44) was studied by simulations. They reviewed that to apply only the T is not enough to form the successful purification protocol for any p and any k. For example fig.7 shows the typical behavior of fidelity in the first 10 iterations when only T is applied and for the case $p = 0$ and $k = 1$. Scale 0-100 represents parameter λ from 0 to 2π with elementary step $2\pi/100$. Scale 1-10 represents the ten iteration steps.

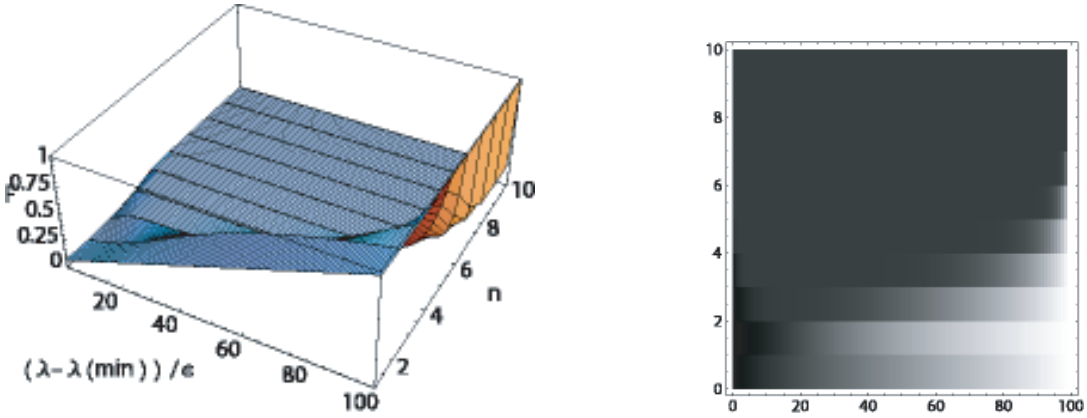

Fig.7: Dependence of the fidelity of the output state with respect to the initial parameter λ and the step of iteration when only nonlinear mapping is used. λ is scaled from 0 to 1 by 0.01, step of the procedure is scaled by 1. Black areas in 2-D density plot of 3-D plot represent fidelity equals 0, white areas represent fidelity equals 1.

This is why we have to find an additional local unitary transformations as defined in the 2-nd point of the construction. We will deal with the case when only a small number of target qudits is used, to create a protocol as simple as possible.

Under the (36) an input state (37) came to

$$\sigma_{out}^{1T} = \frac{D_1}{D}|A\rangle\langle A| + \frac{D_2}{27D}I + \frac{D_3}{6D}\sum_{\pi}|\pi\rangle\langle\pi|$$

where

$$D_1 = 6^{-2k}\lambda^{2k+1},$$

$$D_2 = 27^{-2k}(1-\lambda)^{2k+1},$$

$$D_3 = (\frac{1-\lambda}{27} + \frac{\lambda}{6})^{2k+1} - \frac{D1}{6} - \frac{D2}{27}.$$

The only $U \otimes U \otimes U$ is known to preserve $|A\rangle\langle A|$. It is easy to see that

$$\sum_{\pi} U \otimes U \otimes U |\pi\rangle\langle\pi| U^{\dagger} \otimes U^{\dagger} \otimes U^{\dagger} = \sum_{ijk,i'j'k'} \sum_{\pi} u_{\pi_1 i} u^{*}_{\pi_1 i'} u_{\pi_2 j} u^{*}_{\pi_2 j'} u_{\pi_3 k} u^{*}_{\pi_3 k'} |ijk\rangle\langle i'j'k'| =$$

$$= \sum_{ijk,i' \neq ij' \neq jk' \neq k} \sum_{\pi} (u_{i\pi_1} u^{\dagger}_{\pi_1 i'})^{T} (u_{j\pi_2} u^{\dagger}_{\pi_2 j'})^{T} (u_{k\pi_3} u^{\dagger}_{\pi_3 k'})^{T} |ijk\rangle\langle i'j'k'| + 3I.$$

Generally it is not easy to create an recurrent form of state after m steps of the procedure. Dealing with one particle rotations around x, y, z axes (which represent $\{|0\rangle\,|1\rangle\,|2\rangle\}$ the orthonormal base of C^3) the desired unitary transformation was found. The T (for each $p \in \{0,1,2\}$ and k=1) together with $U \otimes U \otimes U$ where

$$\begin{aligned} U = U_{12} &= R_x(\tfrac{\pi}{4}) R_y(\tfrac{\pi}{4}), \\ U = U_{23} &= R_y(\tfrac{\pi}{4}) R_z(\tfrac{\pi}{4}), \\ U = U_{13} &= R_x(\tfrac{\pi}{4}) R_z(\tfrac{\pi}{4}), \end{aligned} \tag{45}$$

or their cyclic permutation, create the purification protocol.
Fig.8,9,10 illustrate the behavior for $p = 0, 1, 2$ for first 10 steps of procedure.

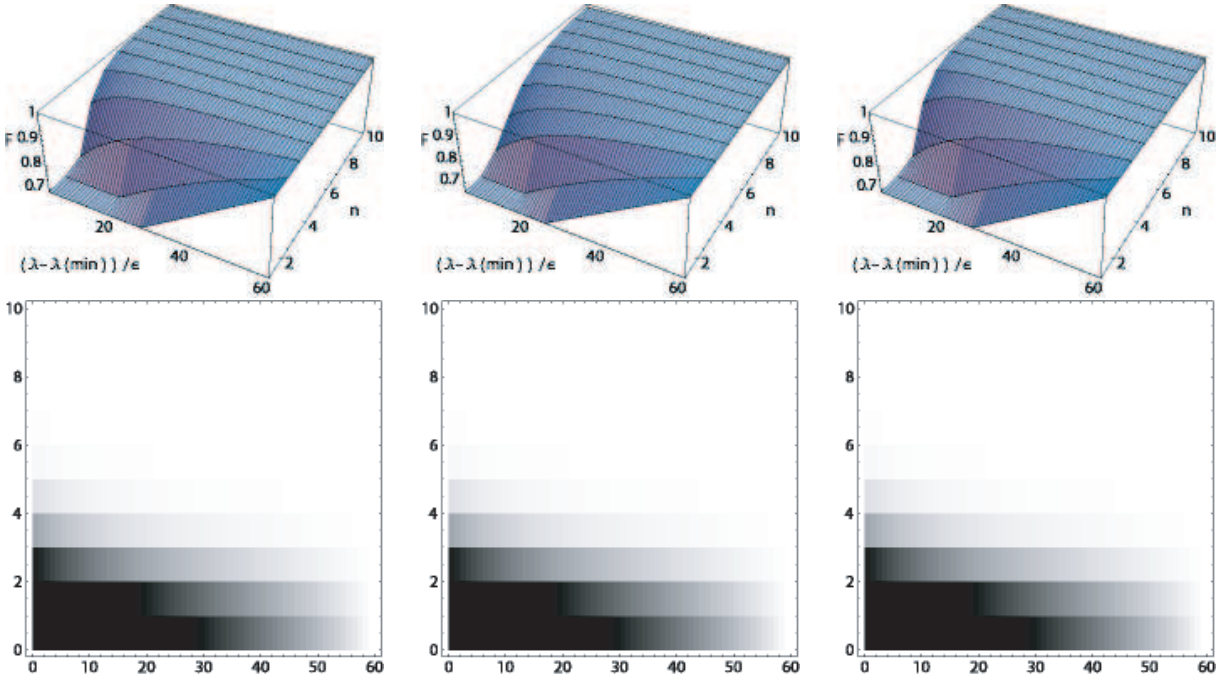

Fig.8: 3-D plots show the dependence of output fidelity with respect to the initial parameter λ (scaled from $\lambda_{min} = 0.4$ to 1 by 0.01) and the number of steps of the protocol (from 1 to 10). Nonlinear mapping is defined by $p = 0$, unitary transformation $U = U_{12}$ resp. $U = U_{13}$ resp. $U = U_{23}$. 2-D plots are respective density plots of 3-D plots. Black areas in 2-D density plot of 3-D plot represent fidelity equals 0, white areas represent fidelity equals 1.

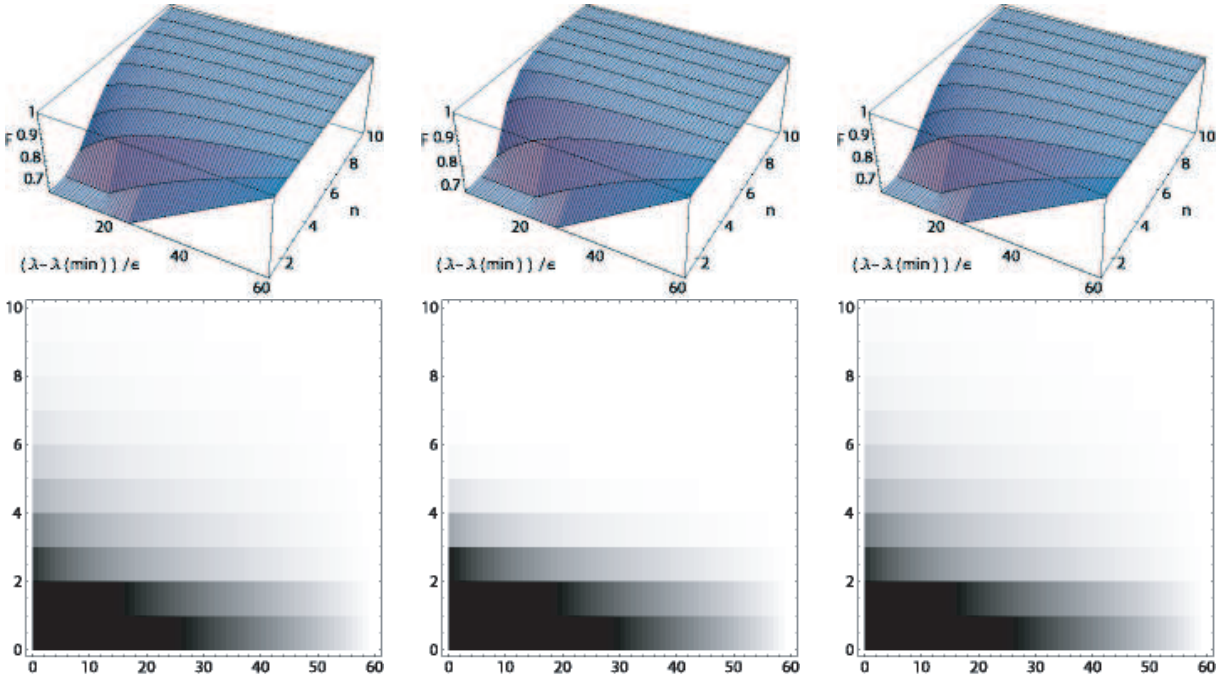

Fig.9: 3-D plots show the dependence of output fidelity with respect to the initial parameter λ (scaled from $\lambda_{min} = 0.4$ to 1 by 0.01) and the number of steps of the protocol (from 1 to 10). Nonlinear mapping is defined by $p = 1$, unitary transformation $U = U_{12}$ resp. $U = U_{13}$ resp. $U = U_{23}$. 2-D plots are respective density plots of 3-D plots. Black areas in 2-D density plot of 3-D plot represent fidelity equals 0, white areas represent fidelity equals 1.

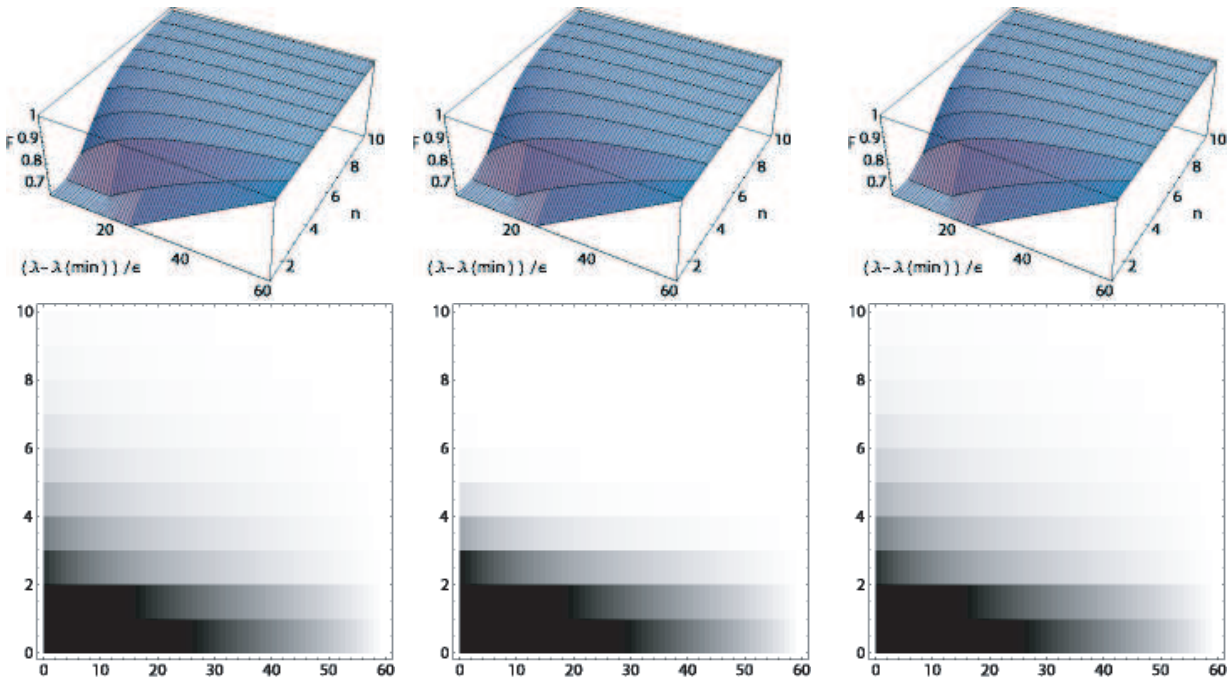

Fig.10: 3-D plots show the dependence of output fidelity with respect to the initial parameter λ (scaled from $\lambda_{min} = 0.4$ to 1 by 0.01) and the number of steps of the protocol (from 1 to 10). Nonlinear mapping is

defined by $p = 2$, unitary transformation $U = U_{12}$ resp. $U = U_{13}$ resp. $U = U_{23}$. Black areas in 2-D density plot of 3-D plot represent fidelity equals 0, white areas represent fidelity equals 1.

Additional numerical simulations suggest that all the protocols with respect to (45) are reasonably stable (with respect to Fig. 8-10) for argument of rotations in $[\pi/4-0.1, \pi/4+0.1]$. Efficiency η of the protocols was studied too. It extremely decrease with number of iterations. Respective plots are shown in fig.11.

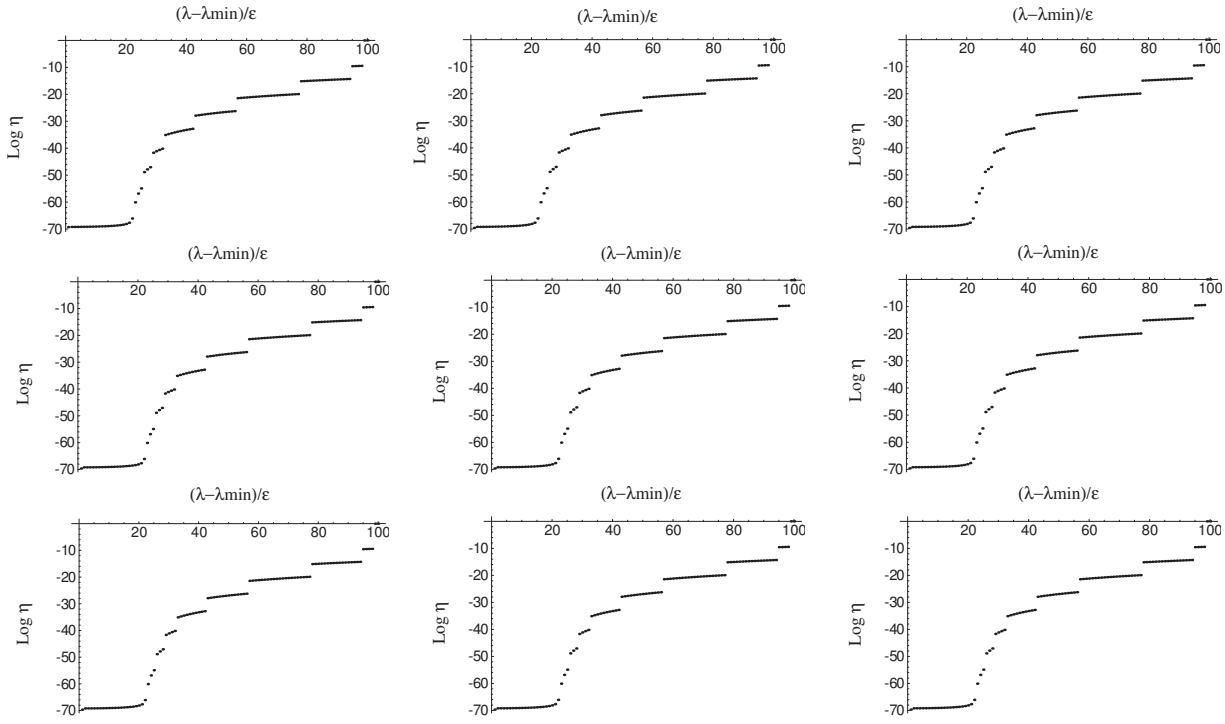

Fig.11: Plots of efficiency η of the respective protocol in dependendence on λ (scaled from 0 to 1 by 0.01) with precision 0.01. Maximal number of iteration in the protocol is 10. In rows are plots for respective $p \in \{0, 1, 2\}$, the columns are plotted for the protocol with $U = U_{12}$ resp. $U = U_{13}$ resp. $U = U_{23}$.

Chapter 4

The stability

The realization of the purification protocol is unideal. Typically unwanted noise appears and disturbs the initial parameters which define the protocol. This is why it is important to study the stability of the purification protocol toward such noise.
We dealt with deterministic protocol in the last chapter which is composed from only the few mappings, only few parameters define it. It might be possible to study the stability of such protocol with respect to its parameters. Let us deal with the stability of the following deterministic protocol.

Separable states

Consider now the nonlinear mapping $T : C^2 \to C^2$ where

$$T(\rho)_{i,j} = \frac{\rho_{i,j}^N}{\sum_k \rho_{k,k}^N}, \tag{46}$$

is defined in an orthonormal base $|i\rangle$, $i \in \{0, 1\}$.
For $N = 2$ the map (46) is closely joined with Deutsch protocol. We will deal with the general action of (46) on the factorized states first i.e. on

$$\rho = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \tag{47}$$

where

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{48}$$

The two complex parameters α, β of (48) can be define via r, φ as

$$\alpha = r \exp(i\varphi),$$

$$\beta = \sqrt{1 - r^2} \exp(-i\varphi).$$

Under the map (46) the factorized state (47) is mapped onto the factorized state

$$|\psi'\rangle = T|\Psi\rangle = \frac{\alpha^N}{\sqrt{|\alpha|^{2N}+|\beta|^{2N}}}|0\rangle + \frac{\beta^N}{\sqrt{|\alpha|^{2N}+|\beta|^{2N}}}|1\rangle. \tag{49}$$

Let us define a mapping $U : C^2 \to C^2$ with matrix representation

$$U = \begin{pmatrix} \cos x & \sin x \exp(i\phi) \\ -\sin x \exp(-i\phi) & \cos x \end{pmatrix} \tag{50}$$

which helps us to define a local unitary transformation $U \otimes U$. After its action of (50) on (49) the state is mapped onto

$$\alpha'' = \frac{\alpha^N \cos x + \beta^N \sin x \exp(i\phi)}{\sqrt{|\alpha|^{2N}+|\beta|^{2N}}},$$

$$\beta'' = \frac{-\alpha^N \sin x \exp(-i\phi) + \beta^N \cos x}{\sqrt{|\alpha|^{2N}+|\beta|^{2N}}}.$$

Let us define the parameter

$$Z = \frac{\alpha}{\beta} = \frac{r}{\sqrt{1-r^2}} \exp(2i\varphi) \tag{51}$$

to characterize the state of the system. Then

$$Z'' = \frac{\alpha''}{\beta''} = \frac{Z^N + \tan x \exp(i\phi)}{-\tan x \exp(-i\phi) Z^N + 1}. \tag{52}$$

Let us compose T and $U \otimes U$ and denote such composition as $\Lambda = (U \otimes U)T$. Let us define a mapping F which represent action Λ on Z.
Our first goal will be to find all the fixed points of Λ for respective x and ϕ. Fixed points of first order are defined by solving the equation

$$Z_f = \frac{Z_f^N + \tan x \exp(i\phi)}{-\tan x \exp(-i\phi) Z_f^N + 1}. \tag{53}$$

If for Z_f the inequality

$$\left|\frac{\partial Z''}{\partial Z}\right|_{Z_f} = \left|\frac{N Z_f}{\cos x - \sin x \exp(-i\phi) Z_f^N}\right| < 1 \tag{54}$$

holds, then Z_f is stable with respect to perturbation in Z.

If for Z_f the equality

$$\left|\frac{\partial Z''}{\partial Z}\right|_{Z_f} = \left|\frac{N Z_f}{\cos x - \sin x \exp(-i\phi) Z_f^N}\right| = 1 \tag{55}$$

holds, then they are marginal and for

$$|\frac{\partial Z''}{\partial Z}|_{Z_f} = |\frac{NZ_f}{\cos x - \sin x \exp(-i\phi) Z_f^N}| > 1 \tag{56}$$

are unstable.
Let us deal with the simplest case when $N = 2$. Solving (53) means to solve a qubic equation. The solutions can be found easily numerically. Due to the periodicity of (53) we can restrict the searching area onto $(0, \pi) \times (0, 2\pi)$ in the $x \times \Phi$ plane. The existence of stable fixed points up to third order for $N = 2$ are represented graphically on fig.12, the determination of higher orders seems to be too time consuming.

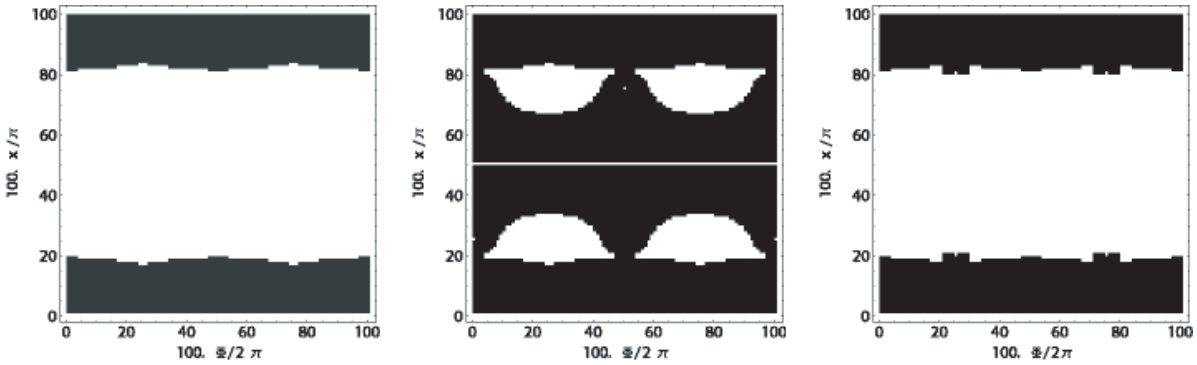

Fig.12: The plots show the existence of stable fixed point of order 1-3. The x-interval is represented on vertical axes $(0, \pi)$, Φ-interval on the horizontal axes $(0, 2\pi)$. Scaling was done by $\pi/100$ resp. $2\pi/100$. Black area denotes the existence of stable fixed point. In the white areas stable fixed point do not exist. White isolated points mean the unsufficient computer precision, stable fixed points exist there.

We can find the fixed points of first order analytically in the limit case of mapping (52) when $N \to \infty$ i.e.

$$\lim_{N\to\infty} \frac{Z^N + \tan x \exp(i\phi)}{-\tan x \exp -(i\phi) Z^N + 1}. \tag{57}$$

Three essentially cases appear

$$\text{If } |Z| > 1 \text{ then } F''(Z) \to -\cot x \exp(i\Phi),\ x \in (0, \pi/4) \cup (3\pi/4, \pi) \tag{58}$$

$$\text{If } |Z| < 1 \text{ then } F''(Z) \to \tan x \exp(i\Phi),\ x \in (0, \pi/4) \cup (3\pi/4, \pi) \tag{59}$$

$$\text{If } |Z| = 1 \text{ then } \lim_{n\to\infty} F''(Z) \text{ does not exist and oscillates.} \tag{60}$$

It is of particular interest to know if these points are stable. For this purpose we have to study the first derivative

$$\lim_{N\to\infty}|\frac{\partial F''(Z)}{\partial Z}| = \lim_{N\to\infty}|\frac{NZ_f}{\cos x - \sin x \exp(-i\phi)Z_f^N}|. \tag{61}$$

For the case (58) the fixed point is stable, for the case (59) is unstable and for case (60) can not decide.

Let us study the dynamics of map (52) in more details. Let Z_0 is one of fixed points of first order for respective x_0, Φ_0 i.e. $F(Z_0) = Z_0$. Denote we $\Delta Z = Z - Z_0$ for each Z closely to Z_0 and let $\xi = \Delta Z$. Then we can write for $\Delta n = 1$

$$\frac{d\xi}{n} \approx \frac{\Delta\xi}{\Delta n} = \xi' - \xi = \Delta Z' - \Delta Z = \Delta F(Z) - \Delta(Z) = F(Z) - F(Z_0) - \Delta Z \approx$$

$$\approx \Delta M + \frac{\partial F}{\partial Z}|_{Z_0}\xi + \frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}\xi^2 - \Delta Z = \Delta M + (\frac{\partial F}{\partial Z}|_{Z_0} - 1)\xi + \frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}\xi^2$$

where

$$\Delta M = \frac{\partial F}{\partial x}|_{x_0,\Phi_0,Z_0}(x - x_0) + \frac{\partial F}{\partial \Phi}|_{x_0,\Phi_0,Z_0}(\Phi - \Phi_0).$$

Only terms linear in Z are considered to be relevant. We can separate both sides of the equation and use the decomposition into two partial fractions. The solution is given by

$$\xi(n) = \frac{\xi_+ - W(n)\xi_-}{1 - W(n)}$$

with

$$W(n) = \frac{\xi_0 - \xi_+}{\xi_0 - \xi_-}\exp[(\xi_+ - \xi_-)\frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}(n - n_0)],$$

$$\xi_\pm = \frac{-\frac{1}{2}(\frac{\partial F}{\partial Z}|_{Z_0} - 1) \pm \sqrt{[\frac{1}{2}(\frac{\partial F}{\partial Z}|_{Z_0} - 1)]^2 - \frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}\Delta M}}{\frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}}.$$

$\xi(n)$ is close to zero only if the output state after n iterations of mapping Λ is near the Z_0. It is a sufficient condition for Z_0 to be the stable fixed point in perturbation in x, Φ. $\xi(n)$ depends mostly on $W(n)$. Three kinds of regime can be expected.

1. $Re((\xi_+ - \xi_-)\frac{1}{2}\frac{\partial^2 F}{\partial Z}|_{Z_0}) = Re\sqrt{[\frac{1}{4}(\frac{\partial F}{\partial Z}|_{Z_0} - 1)^2 - \frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}\Delta M]} < 0$. In this case $\lim_{n\to\infty} W(n) = 0$ so $\lim_{n\to\infty}\xi(n) = \xi_+$. If we assume only small perturbation in x and Φ then $\Delta M \approx 0$ and consequently from the definition of ξ_+ follows that $\xi_+ \approx 0$. This is why for this case Z_0 is a stable fixed point under the perturbation in x, Φ.

2. $Re((\xi_+ - \xi_-)\frac{1}{2}\frac{\partial^2 F}{\partial Z}|_{Z_0}) = Re\sqrt{[\frac{1}{4}(\frac{\partial F}{\partial Z}|_{Z_0} - 1)^2 - \frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}\Delta M]} > 0$. In this case $\lim_{n\to\infty} \mid W(n) \mid = \infty$ so $\lim_{n\to\infty}\xi(n) = \xi_-$ and Z_0 is unstable.

3. $Re((\xi_+ - \xi_-)\frac{1}{2}\frac{\partial^2 F}{\partial Z}|_{Z_0}) = Re\sqrt{[\frac{1}{4}(\frac{\partial F}{\partial Z}|_{Z_0} - 1)^2 - \frac{1}{2}\frac{\partial^2 F}{\partial Z^2}|_{Z_0}\Delta M]} = 0$. In this case $\xi(n)$ can have a complicated behavior.

I studied the behavior of the fixed points for the case $N = 2$, for perturbation in x (useful for real rotations i.e. $\Phi = 0$). After initial $n = 1000$ iterations of (52) following 100 iterations were studied. I studied the higher orders too, up to third order. I studied the Shannon entropy (11), parameter r which is related directly to Z and projection (14) onto initial fixed point. Especially I studied real rotations $\Phi = 0$ in more details. From the simulations the following conclusions can be drawn.
The Area $x \times \Phi$ can be divide onto two basic subareas: subareas where do not exist any stable fixed point up to third order and subareas where exist some stable fixed point up to 3rd order. In the first type of subareas chaotic motion can be seen, fig.13,14. Fig.13 represents this situation for fixed point of 2nd order for the conditions $x = \pi/4$, $\Phi = \pi/4$ $(Z = -1.52538 - 0.962054i)$. It seems that intermittency is the route to absolutely irregular motion. Fig.14 represent situation for fixed point of 3rd order for conditions $x = \pi/5 + \pi/2000$, $\Phi = \pi/2 + \pi/100$ $(Z = -0.897875 - 0.658448i)$. Bifurcation appears first and intermittency is the route to chaos again.

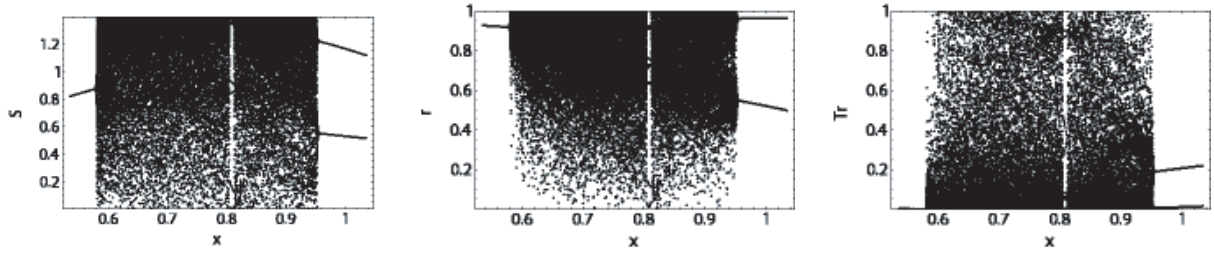

Fig.13: Typical behavior of the Shannon entropy S, parameter r and projection Tr onto the initial state for area where any stable fixed point of any order up to 3 does not exist (for example $x = \pi/4$, $\Phi = \pi/4$).
Chaotic, irregular motion appears.

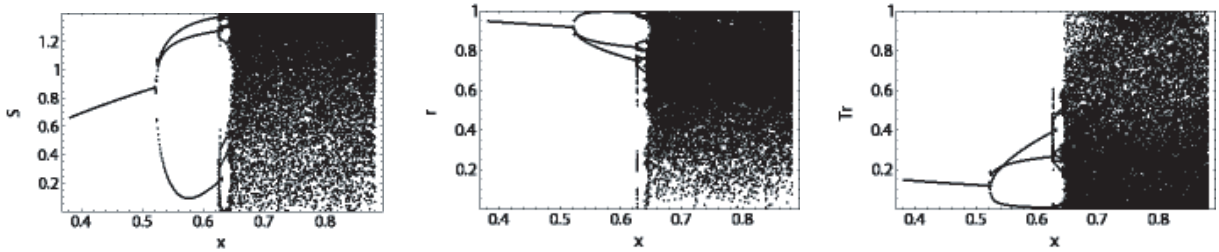

Fig.14: Typical behavior of the Shannon entropy S, parameter r and projection Tr onto the initial state for area where any stable fixed point of any order up to 3 does not exist (for example $x = \pi/5 + \pi/2000$, $\Phi = \pi/2 + \pi/100$). The system changes its regular motion into chaotic.

For real rotations only fixed points of second order can be seen in addition to fixed points of first order (when the latter ones loose stability). For real rotations only limit cycles at most can be found. See for instance fig.15: $x = 142\pi/2000$, $\Phi = 0$, 1st order fixed point $Z = -5.27956$ or fig.16: $x = 3\pi/20 + \pi/50$, $\Phi = 0$, 2nd order fixed point $Z = -06574275 - 0.301878i$.

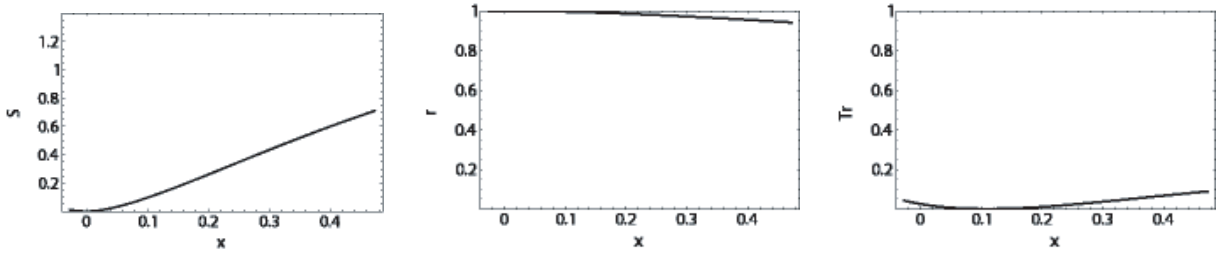

Fig.15: Typical behavior for the Shannon entropy S, parameter r and projection Tr onto the initial state in area of existence the stable fixed point of first order.

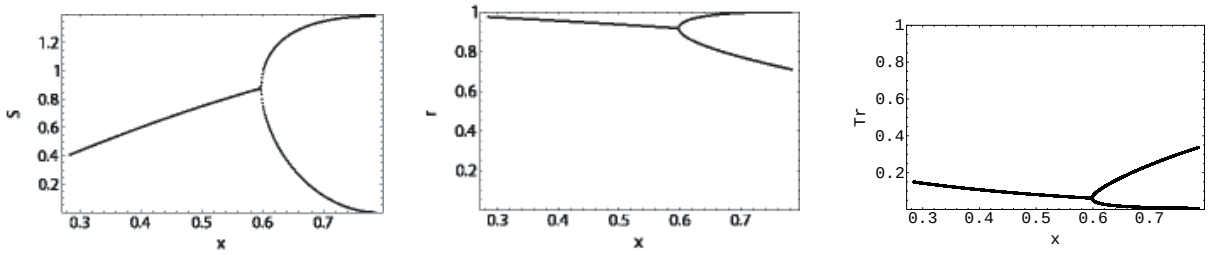

Fig.16: Typical behavior for the Shannon entropy S, parameter r and projection Tr onto the initial state for real rotations in area where fixed point of first do not exist.

For $\Phi \neq \{0, \pi, 2\pi\}$ higher order cycle can exist. For instance limit cycle of third order can be found, fig.17: $x = 4/10\pi$, $\Phi = 1/2\pi$, 2nd order fixed point $Z = -0.591693 - 1.04835i$.

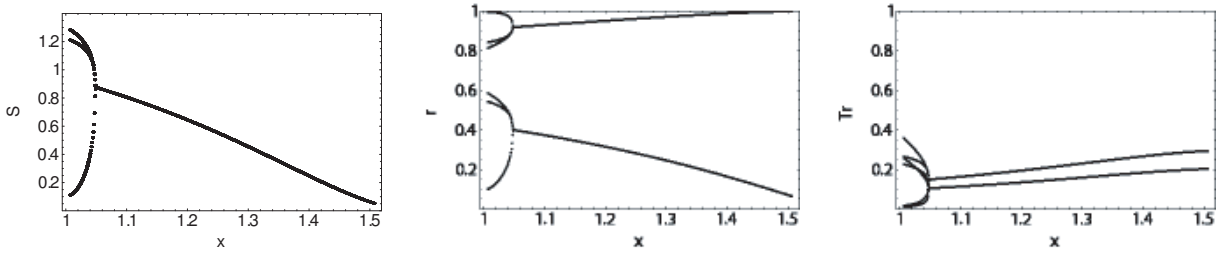

Fig.17: Behavior for the Shannon entropy S, parameter r and projection Tr onto the initial state for unreal rotations.

The behavior of two qubits for nonfactorized initial states is hard to solve. The general input pure state can be written in the Bell base (3) in the form

$$|\Psi\rangle = a|\Psi^+\rangle + b|\Psi^-\rangle + c|\Phi^+\rangle + d|\Phi^-\rangle \tag{62}$$

where $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. The problem involves many parameters and becomes much more complicated. It will be addressed in the future.

Chapter 5

Conclusion

In the early days of quantum theory the predicted existence of entanglement was a impulse for studies on the foundations of quantum theory. In recent years entangled states became again the focus of interest especially in a new branch of quantum physics, quantum information theory. This diploma thesis is closely related to entangled states. Particular interest was given to the construction of so called purification protocols, those processes which allows the participants to share perfectly entangled states, using only local operations and starting with nonideal (noisy) entangled states. Especially we focused on the construction of a deterministic purification protocol for the tree particle antisymmetric states with completely depolarized disturbance. We defined the respective class of nonlinear mappings, defined feasible parameters to preserve antisymmetric states and constructed the purification protocol using a special class of unitary transformation of the form $U \otimes U \otimes U$ (which preserve antisymmetric states in general). 10 iterates is enough to distill a state with purity $0,4 + (1 - 0,4)/27 \approx 0,42$ to a state with purity 0.9. The protocol works for all the cases of the considered nonlinear mapping. In addition it is not crucial for the protocol which combination of $R_x(\pi/4)R_y(\pi/4)$, $R_x(\pi/4)R_z(\pi/4)$, $R_y(\pi/4)R_z(\pi/4)$ or respective cyclic permutation in x, y, z we used for U. The protocol appears to be stable under perturbation in the rotation parameter $[\pi - 0.1, \pi + 0.1]$ and its efficiency exponentially decreased with the number of iterates used in the protocol.

Particular interest was paid to the task of stability of the purification protocol under the perturbation of its parameters. Such task have to be solved because in real the realization of the protocol is not perfect and we have to know for which ranges of parameters the protocol can be used. We started with the simple case of a nonlinear map (which "squared" the density matrices) applied to two qubits in a factorized state . In addition an unitary transformation $U \otimes U$ was used where U represents a general rotation. We found stable fixed points of the protocol composed of the two transforms. We found them up to 3rd order. We studied the case of real rotations in more details and realized that the motion is regular in this case. Only one bifurcation can be seen and hence limit cycles were maximally of the second order. For areas where stable fixed point of second and third order exist bifurcations of higher orders could be observed. If the fixed point motion goes though the area where no stable point of the second respective third order exists the motion becomes chaotic. It

does not seem that chaos is generated by a sequence of bifurcations but that intermittency is the "right" mechanism.

The remaining problems to be solved are the detailed analysis of the intermittency (a analytic approach seems to be possible but goes beyond the scope of the thesis), the studies for initial entangled states and studies for more component initial states. In the latter case the essential problem is the great number of parameters involved which makes analytic as well as numerical studies quite demanding.

Chapter 6

Appendix A1: *GXOR*-generalized *XOR*-gate

XOR-gate [13] was defined as a linear operator on a $\mathcal{H} \equiv C^2 \otimes C^2$ by relation

$$XOR|i\rangle_1|j\rangle_2 = |i\rangle_1|i \oplus j\rangle_2 = |i\rangle_1|(i+j)mod2\rangle_2 \tag{63}$$

where $i, j \in \{1, 2\}$ describes each qubits. This transformation has following characteristic properties: it is unitary [1] and thus reversible gate [14], it is hermitian [1] and $i \oplus j = 0$ only if $i = j$ i.e. $XOR|i\rangle_1|j\rangle_2 = |i\rangle_1|0\rangle_2$ only if $i = j$.
Let us generalize *XOR* gate to the *GXOR* gate for two D-qudits. If we define

$$GXOR|i\rangle_1|j\rangle_2 = |i\rangle_1|i \oplus j\rangle_2 = |i\rangle_1|(i+j)modD\rangle_2 \tag{64}$$

where $i, j \in \{0, 1, ..., D-1\}$ we realize that such operator is unitary but not hermitian for $D > 2$. The generalization is defined by

$$GXOR|i\rangle_1|j\rangle_2 = |i\rangle_1|i \ominus j\rangle_2 = |i\rangle_1|(i-j)modD\rangle_2. \tag{65}$$

For $D = 2$ the *GXOR* is equivalent with *XOR*. This operator is unitary, hermitian and $i \ominus j = 0$ only if $i = j$. Physical realization of *GXOR* is closely related with nonlinear optical elements. Discrete Fourier transformation $F : C^D \to C^D$ where

$$F|k\rangle \equiv 1/\sqrt{D} \sum_{n=0}^{D-1} exp(i2\pi kn/D)|n\rangle$$

is important, whole construction was discussed in [13].
An important application of *GXOR* is the creation of entangled two qudits systems. Let $|i\rangle|j\rangle$, $i, j \in \{0, ..., D-1\}$ is an orthonormal basis $\mathcal{H} = C^D \otimes C^D$ than

$$|\psi_{lm}\rangle = GXOR_{12}[F|l\rangle_1|m\rangle_2]$$

where F is the Fourier transformation operator. For $D = 2$ we obtain the Bell states (3). For $D > 2$ we obtain the so called generalized Bell states. It is easy to check, that these entangled states are orthogonal.

$$\langle\psi_{lm}|\psi_{kn}\rangle = \langle GXOR_{12}[F|l\rangle_1|m\rangle_2]|GXOR_{12}[F|k\rangle_1|n\rangle_2]\rangle =$$

$$= \frac{1}{D}\sum_x\sum_y exp(i2\pi(yk-xl)/D)\langle x|y\rangle\langle x\ominus m|y\ominus n\rangle = \delta_{kl}\delta_{mn}$$

where δ_{ab} is the Kronecker delta. It implies from the fact: $x = y$, $m = n$ then for $k \neq l$ is $\frac{1}{D}\sum_x exp(i2\pi x(k-l)/D) = 0$, for $k = l$ the summation is 1. The number of Bell states is D^2, the same as dimension $\mathcal{H}$, so they form orthogonal basis $\mathcal{H}$.

Chapter 7

Appendix A2: Routes to chaos

Let us introduce few basic concepts [14] related to the behavior of the nonlinear map Λ: $\mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$, which maps a density matrix onto a density matrix. If for some $\rho \in \mathcal{B}(\mathcal{H})$

$$\underbrace{\Lambda(...\Lambda}_{n}(\rho)...) = \rho$$

than ρ is said to be the **fixed point of n-th order** [14] of Λ. Fixed point ρ of respective order of Λ is an **attractor** [14] of respective order if there exist an open neighborhood around ρ that it shrinks down to ρ under the flow of T i.e. $\exists\ B_\varepsilon(\rho) \in \mathcal{B}(\mathcal{H})$ for which

$$\lim_{n \longrightarrow \infty} \underbrace{\Lambda(...\Lambda}_{n}(B_\varepsilon(\rho))...) = \rho.$$

Physical realization of Λ is unideal, it can be perturbed in its own inner parameters. It is useful to know the influence of such perturbation on fixed points of Λ, for example for the construction of purification protocols. From this point of view fixed points can be **stable** if they are unchanged during the flow for respective perturbed Λ. Stable cycles represent so called **regular motion**. Along the trajectories of such stable cycles the motion diverges and behavior of the Λ on respective state become irregular, so called **chaotic**.
There are at least two basic routes to chaos. Period doubling bifurcation and intermittency. **Bifurcation** appears when the state leaves the area of stability (area of equilibrium) under perturbation. **Intermittency** appears when the regular motion of varying lengths is interspersed with burst of chaotic motion. Intermittency is closely related with the existence of bifurcation in respective area. It has been classified into three types, depending on the type of bifurcation and its eigenvalue transition. A complete description can be found in [14] and the problem will be analyzed in more details in future.

Chapter 8

References

[1] Blank J., Exner P., Havlíček M.: Lineárníoperátory v kvantové fyzice Karolinum, Praha (1993)

[2] Einstein A., Podolsky B., Rosen N.: Phys. Rev. 47 777 (1935)

[3] Zeilinger A.: Physica Scripta 46 203 (1998)

[4] Barnett S. M., Phoenix S.: Phys. Rev. A 44 535 (1991)

[5] Pittenger A. O., Rubin M. H.: Optics Comm. 179 (2000)

[6] Horodecki M., Horodecki P.: Phys. Rev. A 59 4205 (1999)

[7] Horodecki M., Horodecki P.: Quant. Inf. and Comp. 1 1 (2001)

[8] Blum K.: Density matrix theory and applicantions, Plenum, New York (1981)

[9] Kraus K.: States, Effects and Operations: Fundamental Notions of Quantum Theory, Wiley, New York (1991)

[10] Peres A.: Quantum theory, concepts and methods, Kluwer Academic Publisher, Dordrecht (1989)

[11]: Bennett Ch. H., Brassard G., Popescu S., Schumacher B., Smolin J. A., Wootters K.: Phys. Rev. Lett. 76 722 (1996)

[12]: Bechmann-Pasquinucci H., Huttner B., Gisin N.: quant-ph/9708040, (1997)

[13]: Alber G., Delgado A., Gisin N., Jex I.: J. Phys. A: Math. Gen. 34 8821 (2001)

[14]: Liechtenberg A., Lieberman M.: Regular and chaotic dynamics, Springer, Berlin (2003)