POLITECHNIKA GDAŃSKA
Wydział Fizyki Technicznej
i Matematyki Stosowanej

Imię i nazwisko autora rozprawy: mgr inż. Marcin Nowakowski
Dyscyplina naukowa: Fizyka

ROZPRAWA DOKTORSKA

Tytuł rozprawy w języku polskim: O symetrycznej rozszerzalności stanów kwantowych i jej zastosowaniach.

Tytuł rozprawy w języku angielskim: On symmetric extendibility of quantum states and its applications.

Promotor *Podpis*
Prof. Dr hab. Paweł Horodecki

Gdańsk, rok 2016

On Symmetric Extendibility of Quantum States and Its Applications

Marcin Nowakowski

Supervisor: Prof. Pawel Horodecki

Faculty of Applied Physics and Mathematics
Gdansk University of Technology

This dissertation is submitted for the degree of
Doctor of Philosophy in Physics

2016

To my wife Miroslawa, and children Lidia and Teodor.

Acknowledgements

I would like to acknowledge Prof. Pawel Horodecki for many years of scientific support and stimulating discussions in the matter of foundations of quantum physics and quantum information theory. I acknowledge also a financial support from the European Research Project SCALA and from the ERC grant QOLAPS. Part of the research work presented in this PhD thesis was performed at the National Quantum Information Center of Gdansk.

Abstract

This dissertation is focused on analysis of the symmetric extendibility of quantum states and its applications in the quantum information theory, with special attention paid to the area of quantum entanglement distillation, quantum channels theory, quantum security, and monogamy of quantum entanglement in time.

We analyze geometry of the set of symmetric extendible states, i.e. such states that possess symmetric extensions and in particular, prove that the set is closed under action of the 1-LOCC operators which is of a great importance for further applications in one-way distillability of quantum states and quantum channels theory.

Basing on the Choi-Jamiolkowski isomorphism between quantum states and quantum channels, we derive a simple test for the quantum channel capacity. We discuss also monogamy of quantum entanglement and its relations with Bell theorem, and the symmetric extendibility.

Further, the subject of our analysis is also the theory of quantum entanglement measures and their relation to the symmetric extendibility. A new entanglement monotone and parameter are introduced basing on this concept, which are applied as new upper bounds on distillable entanglement. We introduce the concept of reduced variants of the quantum communication rates, showing that they can efficiently estimate non-reduced quantum measures.

Finally, it is derived that in the paradigm of the entangled consistent histories, introducing the concept of quantum entanglement in time, a particular history is monogamous and we can derive the Tsirelson bound on the Leggett-Garg temporal inequalities.

The results presented in this PhD thesis show importance of the concept of the symmetric extendibility for further development of quantum information theory, especially in domain of one-way communication.

Table of contents

List of figures

Chapter 1

Introduction

The main objective of this PhD thesis is to analyze the concept of symmetric extendibility of quantum states, i.e. states having the so-called symmetric extensions, and applications of this property to the quantum information theory, with a particular attention paid to the area of quantum entanglement distillation, quantum channels theory, quantum privacy, and monogamy of quantum entanglement in time. Due to a strong relation between monogamy of quantum entanglement and the symmetric extendibility of quantum states, we discuss separability of quantum states in a context of symmetric extendibility. As a natural consequence of this analysis, we analyze the Bell inequalities for quantum states having symmetric extensions and structure of the set of symmetric extendible states.

Further, the subject of analysis is also the theory of quantum entanglement measures and their relation to the symmetric extendibility. New entanglement monotones and parameters are introduced basing on this concept, which are applied as new upper bounds on distillable entanglement. Due to the Choi-Jamiolkowski isomorphism between states and quantum channels, the symmetric extendibility is also a substantial concept for the theory of quantum channel capacities in domain which is a matter of research of this thesis. We discuss also the new concept of quantum entanglement in time and initiate analysis of its monogamy on the ground of the consistent entangled histories, in similarity to the concept of monogamy of spatial quantum entanglement directly related to symmetric extendibility. Since it is a newly emerging discipline in quantum information theory, many fundamental tools, widely used for spatial correlations, have to be further developed for temporal correlations in future research. The outline of this thesis is as follows:

In chapter 2, we introduce the fundamental concepts and tools of quantum information theory which are necessary for understanding the following chapters. A special focus is put on the theory of quantum channels and quantum entanglement.

Chapter 3 is devoted to the concept of monogamy of quantum entanglement and the famous Bell theorem. We recall the key assumptions behind *local realism* and Bell inequalities. Further, the relations between symmetric extendibility of quantum states and violation of Bell inequalities is explored.

In chapter 4, we discuss in depth the symmetric extendible states analyzing geometry of the set consisting of quantum symmetric extendible states. In particular, we prove that one cannot reduce maximal extendibility of quantum states even if acts with one-way LOCC operations on multiple copies of the state [126, 128] which is now broadly used in the literature [123, 124, 122, 112, 121]. Composite systems and their symmetric extendibility is discussed with a general representation of the composite extensions [128]. We present also the separability test hierarchy based on the symmetric extendibility of quantum states.

In chapter 5, we present analytically derived symmetric extensions of isotropic states [126]. This result is important due to the fact that all bipartite quantum states can be transformed under $U \otimes U^*$-twirling operations into isotropic states. Basing on that, we propose a new entanglement parameter [126] built on a normalized relative entropy distance to the set of symmetric extendible states in analogy to the relative entropy of entanglement. We recall also the conditions for symmetric extendibility of two-qubit states and present the regions for Bell diagonal states.

Chapter 6 is focused on applications of symmetric extendibility concept to distillation of quantum entanglement and entanglement measures. We recall the fundamental concepts of quantum entanglement distillation protocols and entanglement measures. We present the concept of best symmetric extendible approximation and a new entanglement monotone [128]. We introduce the reduced version of one-way distillable entanglement [127] and prove that it is an upper bound on one-way distillable entanglement. It is also proved that asymptotically regularized new entanglement parameter [126] is a good upper bound on one-way distillable entanglement.

The subject of chapter 7 is the concept of quantum channels and its symmetric extendibility. We recall classical and quantum channel capacities measures and discuss their additivity. We present a simple test for quantum channel capacities [126] which is based on the observation that quantum entanglement is monogamous and prevents parties from perfect cloning of quantum states, thus, imposing on quantum channels, isomorphic (by means of Choi-Jamiolkowski isomorphism) with symmetric extendible states, zero quantum capacity. We present new reduced variant of quantum channel capacity [127] which in some cases can dramatically reduce complexity of analysis of the search problem for quantum channel capacities and which is a new upper bound on quantum channel capacity. Finally, we discuss

the subject of super-activation of quantum channel capacities with symmetric extendible channels.

In chapter 8 we discussed shareability of quantum private correlations. We recall the concept of a quantum secret key and quantum private states. We introduce a reduced secret key [127] and show that it can be used as an upper bound on the secret key rate of quantum protocols. We present also some new lemmas bounding the one-way secret key rate in terms of a distance to the set of symmetric extendible states [128].

Chapter 9 is devoted to the new emerging discipline focused on analysis of quantum correlations in time. The issue of quantum entanglement in time [129, 130] is discussed on the ground of the entangled consistent histories [40–42], a recently extended version of the consistent (decoherent) histories theory [77–80, 85–87]. It is argued that in similarity to quantum entanglement in space, temporal quantum entanglement as a new concept is also monogamous for a particular history [129, 130]. Further, basing on the concept of entangled histories we prove analytically the Tsirelson bound [38] on temporal CHSH-like [39] inequalities which confirms the previous results based on convex optimization of correlator spaces for correlations between the consecutive measurements [71].

In chapter 10, we summarize the key results of this PhD Thesis and elaborate on further interesting open research problems and future research directions in this area.

List of publications:

1. M. L. Nowakowski, P. Horodecki, **A simple test for quantum channel capacity**, J. Phys. A: Math. Theor. **42**, 135306 (2009).

2. M. L. Nowakowski, P. Horodecki, **Efficient bounds on quantum communication rates *via* their reduced variants**, Phys. Rev. A **82**, 042342 (2010).

3. M. Nowakowski, **The symmetric extendibility of quantum states**, J. Phys. A: Math. Theor. **49**, 385301 (2016).

4. M. Nowakowski, **Monogamy of quantum entanglement in time**, Preprint quant-ph/1604.03976 (submitted to Phys. Rev. A).

5. M. Nowakowski, **Quantum entanglement in time**, American Institute of Phys. Conf. Proc.: Quantum Retrocausation III (2016).

Chapter 2

Foundations of quantum information theory

In this chapter we study the fundamental concepts related to quantum states and operations on them which form a language of quantum information theory and will be a necessary tool for understanding following chapters. Our present discussion will allow us to face more complex matters related to symmetric extendibility of quantum states and quantum channels through which they or their parts are sent. More extensive considerations on quantum information theory foundations can be found in [3, 28, 13, 76, 125, 143].

2.1 Quantum states

In classical information theory, a source generates a binary state element represented by 0 or 1 in a binary space and in general, the classical source generates objects over a finite discrete alphabet. In the world of quantum mechanics, a state $|\Psi\rangle$ of a physical object A can be a convex linear combination over basis vectors corresponding to a complex Hilbert space $\mathscr{H}$ in which the state of the physical object lives[1], i.e. $|\Psi\rangle \in \mathscr{H}$. This fact is formulated in the following postulate of quantum mechanics: *The state of an isolated physical system is represented by the normalized state vector* $|\Psi\rangle$ *in the Hilbert space* $\mathscr{H}$ *and* $\||\Psi\rangle\| = 1$. The system is then in a so-called pure state.

We will use further Dirac notation for representation of normalized quantum states $|\Psi\rangle \in \mathscr{H}$ ('kets'). As an example, one can represent the basis vectors of two-dimensional Hilbert space $\mathscr{H} = \mathbb{C}^{\in}$ as follows:$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. There always exists a dual space

[1] We will consider states living in Hilbert spaces of finite dimension: $dim\mathscr{H} < \infty$.

$\mathscr{H}^*$ associated with $\mathscr{H}$, which is a set of all linear functionals on $\mathscr{H}$. This represents the corresponding relation:

$$\mathscr{H} \ni |\Psi\rangle \longrightarrow \langle\Psi| \in \mathscr{H}^* \tag{2.1}$$

Each ket $|\Psi\rangle \in \mathscr{H}$ can be now associated with a Hermitian conjugation $\langle\Psi| \in \mathscr{H}^*$ (called 'bra') and the scalar product between the vectors is a 'bra-ket':

$$\mathscr{H} \times \mathscr{H} \ni (|\phi\rangle, |\psi\rangle) \longrightarrow \langle\phi|\psi\rangle \in \mathbb{C} \tag{2.2}$$

Let us now remind properties of the inner product in Hilbert spaces:

$$\langle\phi|\phi\rangle \geq 0, \tag{2.3}$$
$$\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*, \tag{2.4}$$
$$\langle\psi_1 + \psi_2|\phi\rangle = \langle\psi_1|\phi\rangle + \langle\psi_2|\phi\rangle, \tag{2.5}$$
$$\langle\alpha\phi|\psi\rangle = \alpha^*\langle\phi|\psi\rangle,\ \alpha \in \mathbb{C}, \tag{2.6}$$
$$(\langle\phi|\phi\rangle = 0) \Leftrightarrow (|\phi\rangle = 0). \tag{2.7}$$

The inner product generates a natural norm $\||\Psi\rangle\| = \sqrt{\langle\Psi|\Psi\rangle}$ which induces the metric: $Dist(|\Psi\rangle, |\Phi\rangle) = \||\Psi\rangle - |\Phi\rangle\| = \sqrt{\langle\Psi - \Phi|\Psi - \Phi\rangle}$.

A state of the physical object can be represented by the pure state only if the observer can possess maximal information about the object. Otherwise, the object is correlated with the environment, i.e. it is correlated classically or quantum entangled with the environment (quantum entanglement will be presented in the following sections) and then, there does not exist a local observer measuring the state of the object that could possess a complete knowledge about the state of the object. It should be emphasized that in the latter case lack of full information about the object is not due to uncertainty in the classical sense, but is a result of the inability of full description of the object correlated with other objects. The object is then in a mixed state $\rho \in \mathscr{B}(\mathscr{H})$. The set of quantum states is a subset of the operator algebra $\mathscr{B}(\mathscr{H})$ acting on a Hilbert space $\mathscr{H}$, and the elements of the the set are called *density matrices*.

Definition 2.1.1 *The Banach algebra $\mathscr{B}(\mathscr{H})$ will denote a Banach algebra of bounded linear operators Λ on a complex Hilbert space $\mathscr{H}$ with a norm:*

$$\|\Lambda\| = \sup\{\|\Lambda x\| : x \in \mathscr{H},\ \|x\| \leq \infty\}. \tag{2.8}$$

The boundedness of a linear operator Λ represents a fact that it maps bounded subsets in $\mathscr{H}$ into bounded subsets in $\mathscr{H}$ which is a substantial property for physical quantities that can be a subject of measurements as we will show further.

It can be shown (a proof in e.g. [19]) that an algebra $\mathscr{B}(\mathscr{H})$ is endowed in involution $\Lambda \to \Lambda^*$ where exists the only one element $\Lambda^* \in \mathscr{B}(\mathscr{H})$ so that:

$$\forall_{x,y\in\mathscr{B}(\mathscr{H})}\ (\Lambda x, y) = (x, \Lambda^* y), \tag{2.9}$$

$$\| \Lambda \| = \| \Lambda^* \| . \tag{2.10}$$

It is worth mentioning that the $\mathscr{B}(\mathscr{H})$ is also a C^*-algebra which is implied by the aforementioned properties. We remind now definitions of operator classes important for applications in quantum information theory and quantum mechanics:

Definition 2.1.2 *An operator $\Lambda \in \mathscr{B}(\mathscr{H})$ is:*

$$Hermitian\ if\ \Lambda = \Lambda^*, \tag{2.11}$$

$$unitary\ if\ \Lambda\Lambda^* = \Lambda^*\Lambda = \mathbb{I}\ where\ \mathbb{I}\ denotes\ identity\ in\ \mathscr{B}(\mathscr{H}), \tag{2.12}$$

$$a\ projector\ if\ \Lambda^2 = \Lambda. \tag{2.13}$$

Further, one introduce the scalar product for these operators:

$$\forall_{A,B\in\mathscr{B}(\mathscr{H})}(A,B) = Tr(A^\dagger B), \tag{2.14}$$

where $Tr(\cdot)$ denotes the trace operation on the operator. Having defined such a product, we can derive a norm in the algebra:

$$\forall_{A\in\mathscr{B}(\mathscr{H})}\ \| A \| = \sqrt{(A,A)}. \tag{2.15}$$

The set of such operators endowed with the aforementioned scalar product and norm is a special case of a Hilbert space, and is called a Hilbert-Schmidt space. Thus, whenever we use the notation $\rho \in \mathscr{B}(\mathscr{H})$ in this thesis, we consider a quantum state from a Hilbert-Schmidt space.

Assume that the system is in one of the states $|\psi_i\rangle$ (i indexes the potential physical states) with probability p_i, the set $\{p_i, |\psi_i\rangle\}$ is called *an ensemble of pure states* and a density matrix of such a setup is:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{2.16}$$

where $\sum_i p_i = 1$. Now, we can pose a question: *when does an operator $\rho \in \mathscr{B}(\mathscr{H})$ is a density matrix representing a physical state?* The answer comes from the following well-known theorem:

Theorem 2.1.3 *An operator ρ is a density matrix associated with $\{p_i, |\psi_i\rangle\}$ if and only if the conditions hold:*

(1) $Tr(\rho) = 1$.

(2) $\rho \geq 0$, *i.e.* $\forall_{|\psi\rangle \in \mathscr{H}} \ \langle\psi|\rho|\psi\rangle \geq 0$.

It is worth mentioning that pure states $|\Psi\rangle \in \mathscr{H}$ can be associated with density matrix $\rho = |\Psi\rangle\langle\Psi|$ which is a projector on one-dimensional subspace $\mathscr{H}_{|\psi\rangle} = span\{|\psi\rangle\}$ since:

$$\rho^2 = |\psi\rangle\langle\psi||\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho. \tag{2.17}$$

This leads to the assumption that one can easily explore the degree of purity of the state ρ engaging this observation. The following lemma gives a quick test of purity of a quantum state ρ:

Lemma 2.1.4 *Let $\rho \in \mathscr{B}(\mathscr{H})$ be a density matrix then $Tr(\rho^2) \leq 1$ and $Tr(\rho^2) = 1$ only if ρ is a pure state.*

The state $\rho \in \mathscr{B}(\mathbb{C}^n)$ is called a maximally mixed state if it has a form: $\rho = \frac{1}{n} I$, with the identity operator $I = \sum_i |i\rangle\langle i|$ and a standard orthonormal basis $\{|i\rangle\}$ where $\langle i|j\rangle = \delta_{ij}$.

Since any convex combination of two states of the system $\rho_X \in \mathscr{B}(\mathscr{H})$ and $\rho_Y \in \mathscr{B}(\mathscr{H})$ is again a proper normalized quantum state, i.e. $(1-\alpha)\rho_X + \alpha\rho_X \in \mathscr{B}(\mathscr{H})(0 \leq \alpha \leq 1)$, the set $S \ni \rho$ of all possible states of the system is *a convex set*. Thus, a geometrical analysis of sets of quantum states comes down to studying geometry of convex sets to a great extent [13]. Further, all extreme points [2] of the set S are one-dimensional projectors of the form $P = |\phi\rangle\langle\phi|$.

Example 2.1.5 *We will consider now a two-dimensional quantum system - a qubit which state can be represented by a 2×2 positive Hermitian matrix. It should be noted that the Pauli matrices (generators of $\mathbb{SU}(2)$ group) create a complete orthogonal basis for all density matrices $\rho \in \mathscr{B}(\mathbb{C}^2)$ representing a qubit state:*

$$\sigma_0 = \mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.18}$$

[2] An extreme point of a convex set cannot be represented as a non-trivial convex combination of other extreme points, i.e. so that $0 < \alpha < 1$.

with an inner product meeting the condition $\forall_{i,j}\ Tr\sigma_i\sigma_j = 2\delta_{ij}$ *where* δ_{ij} *stands for the Kronecker delta. Then, the qubit density matrix can be represented as follows:*

$$\rho = \frac{1}{2}(\mathbb{I}_2 + \sum_{i=1}^{3} x_i\sigma_i) = \frac{1}{2}(\mathbb{I}_2 + \vec{x}\cdot\vec{\sigma}), \tag{2.19}$$

$$x_i = Tr(\sigma_i\rho) \in \mathbb{R} \tag{2.20}$$

where $\vec{x}\cdot\vec{\sigma}$ *is a scalar product and* $\vec{x} = col(x_1, x_2, x_3)$ *is called a Bloch vector. The matrix* ρ *represents a state of a physical system if besides being Hermitian, satisfies the positivity condition which occurs when the vector indicates a point inside the unit sphere (it represents a pure state if the Bloch vector is a unit vector).*

2.2 Composite systems

A pure state of a composite system $A_1A_2\ldots A_n$ is represented by a state vector in a tensor Hilbert space, i.e. $|\Psi\rangle \in \mathscr{H}_{A_1} \otimes \mathscr{H}_{A_2} \cdots \otimes \mathscr{H}_{A_n}$.

Let us consider a bipartite system AB. If a state of A is characterized by a vector $|\Phi\rangle_A = \sum_i \alpha_i|\phi\rangle_i \in \mathscr{H}_A$ and $|\Psi\rangle_B = \sum_i \beta_i|\psi\rangle_i \in \mathscr{H}_B$ for B subsystem, then the tensor product is defined as follows:

$$|\Phi\rangle_A \otimes |\Phi\rangle_B = \sum_{ij} \alpha_i\beta_j|\phi_i\rangle \otimes |\psi_j\rangle \tag{2.21}$$

If the basis in $\mathscr{H}_A$ is $\mathbf{B}_A = \{|0\rangle, |1\rangle, \ldots, |i\rangle\}$ and for $\mathscr{H}_B$ is $\mathbf{B}_B = \{|0\rangle, |1\rangle, \ldots, |j\rangle\}$, then $\mathscr{H}_A \otimes \mathscr{H}_B$ is spanned by the basis $\mathbf{B}_{AB} = \{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, \ldots, |i\rangle \otimes |j\rangle\}$. It implies: $\dim \mathscr{H}_A \otimes \mathscr{H}_B = \dim \mathscr{H}_A \cdot \dim \mathscr{H}_B$. In many cases, the tensor sign will be omitted and the element $|i\rangle \otimes |j\rangle$ will be replaced by $|ij\rangle$. As a consequence, the scalar product of tensor vectors is:

$$\langle\phi_1| \otimes \langle\phi_2||\psi_1\rangle \otimes |\psi_2\rangle = \langle\phi_1|\psi_1\rangle\langle\phi_2|\psi_2\rangle \tag{2.22}$$

A local state of a subsystem A, that is a part of a larger system AB, is determined by the reduced matrix: e.g. when the state of the bipartite system is represented by the density matrix $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$, then a state of the A-subsystem is represented by the reduced density matrix $\rho_A \in \mathscr{B}(\mathscr{H}_A)$. This means that Alice possessing A system does not have any complete knowledge about the global state ρ_{AB}. The matrix of the reduced system is defined by means of the partial trace operator [19–21]:

Definition 2.2.1 *Let* $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ *be a state of bipartite system AB, then the state of A-subsystem is represented by the reduced matrix* $\rho_A = Tr_B\rho_{AB}$ *which elements are*

determined by the partial trace operation:

$$\rho_A(i,j) = \sum_{k}^{\dim \mathscr{H}_{\mathscr{B}}} \langle i|_A \langle k|_B \rho_{AB} |j\rangle_A |k\rangle_B, \tag{2.23}$$

where vectors $|\cdot\rangle_A$ (and $|\cdot\rangle_B$) form an orthonormal basis in $\mathscr{H}_A$ (and $\mathscr{H}_B$).

For a system consisting of n subsystems $A_1A_2..A_n$, we can generalize the above definitions distinguishing between two subsets $A \equiv A_1 \ldots A_k$ and $B \equiv A_{k+1} \ldots A_n$ $(1 \leq k \leq n-1)$ applying the same procedure of deriving the reduced states. As an example, let us consider the state ρ_{AB} acting on $\mathscr{H}_A \otimes \mathscr{H}_B$ where $\mathscr{H}_A \cong \mathbb{C}^3$ and $\mathscr{H}_{\mathscr{B}} \cong \mathbb{C}^{\mathscr{N}}$:

$$\rho_{AB} = \sum_{i,j}^{3} |i\rangle_A \langle j| \otimes A_{ij} = \begin{pmatrix} A_{00} & A_{01} & A_{02} \\ A_{01}^\dagger & A_{11} & A_{12} \\ A_{02}^\dagger & A_{12}^\dagger & A_{22} \end{pmatrix} \tag{2.24}$$

where A_{ij} is a matrix of dimension $N \times N$ and for the Hermiticity of ρ_{AB}, $A_{ij} = A_{ji}^\dagger$. The the reduced states of A and B are:

$$\rho_{AB} = \sum_{i,j}^{3} |i\rangle_A \langle j| \otimes A_{ij} \Rightarrow \begin{cases} \rho_A = Tr_B \rho_{AB} = \sum_{i,j}^3 Tr(A_{ij}) |i\rangle_A \langle j| \\ \rho_B = Tr_A \rho_{AB} = \sum_i^3 A_{ii} \end{cases} \tag{2.25}$$

Extensions and purifications of quantum states

We will now consider *extensions* of a quantum state ρ_{AB} and its special case - *purification*:

Definition 2.2.2 *An extension of a bipartite state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ to E-system is any such a state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E)$ so that $Tr_E \rho_{ABE} = \rho_{AB}$. A pure extension $|\Psi_{ABE}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E$ of a state ρ_{AB} is called its purification.*

In general, for any $\rho_A \in \mathscr{B}(\mathscr{H}_A)$ we can always find its purification as an extension $|\Psi_{AB}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ so that after tracing out the ancillary system B, one gets again:

$$\rho_A = Tr_B |\Psi_{AB}\rangle\langle\Psi_{AB}|. \tag{2.26}$$

Noteworthily, one can find infinitely many purifications $|\widetilde{\Psi}_{AB}\rangle$ of a given state ρ_A since:

$$|\widetilde{\Psi}_{AB}\rangle = [\mathbb{I} \otimes U_B] |\Psi_{AB}\rangle \Rightarrow \rho_A = Tr_B |\Psi_{AB}\rangle\langle\Psi_{AB}| = Tr_B |\widetilde{\Psi}_{AB}\rangle\langle\widetilde{\Psi}_{AB}|. \tag{2.27}$$

where U_B is a unitary operation acting on B-part of the system and $|\Psi_{AB}\rangle$ is an arbitrarily chosen purification of ρ_A. The most frequent purification procedure is based on a spectral

decomposition of a mixed state ρ:

$$\rho = \sum_i^M \alpha_i |\phi_i\rangle\langle\phi_i| \longrightarrow |\Psi\rangle = \sum_i^M \alpha_i |\phi_i\rangle|i\rangle, \tag{2.28}$$

where $|i\rangle$ form an orthogonal basis for the ancillary system.

No-cloning principle

Classical information theory allows the precise copying of information which is applied by classical computers in the instance of copying files. According to quantum information theory one can also copy states but only the base ones $\{|0\rangle, |1\rangle, \ldots\}$ (which actually can represent the classical states), however, it prohibits cloning of non-orthogonal states which is claimed in the following theorem [170]:

Theorem 2.2.3 *There does not exist an unitary operation $U \in \mathscr{B}(\mathscr{H})$ which could clone an 'unknown' state $|\Psi\rangle \in \mathscr{H}$ so that: $U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Psi\rangle$.*

Proof. Assume that there exists an operator U copying the states ideally $|\Psi\rangle,\ |\Phi\rangle \in \mathscr{H}$, i.e.:

$$\begin{cases} U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Psi\rangle \\ U|\Phi\rangle \otimes |0\rangle = |\Phi\rangle \otimes |\Phi\rangle \end{cases} \tag{2.29}$$

Since U is unitary, we can derive the scalar products:

$$\langle\Psi \otimes \Psi|\Phi \otimes \Phi\rangle = (\langle\Psi|\Phi\rangle)^2 = \langle 0| \otimes \langle\Psi|U^\dagger U|\Phi\rangle \otimes |0\rangle = \langle\Psi|\Phi\rangle\langle 0|0\rangle = \langle\Psi|\Phi\rangle. \tag{2.30}$$

which is a contradiction when $0 < \langle\Psi|\Phi\rangle < 1$ (for non-orthogonal $|\Psi\rangle$ and $|\Phi\rangle$). □

As previously noted, the no-cloning principle does not preclude cloning of orthogonal states, i.e. the cloning machine (device performing the operation U) can clone orthogonal states. As an example may serve the quantum gate *CNOT* (a quantum equivalent of the classic gate of a controlled negation) working on qubits with the matrix representation:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{2.31}$$

which clones basis states $|\phi\rangle \in \{|0\rangle,\ |1\rangle\}$:

$$CNOT|\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle. \tag{2.32}$$

2.3 Completely positive maps

After considering the static properties of quantum states, the question arises about the dynamics of quantum composite systems. We can state the following question: textitwhat operations on quantum states are physically allowed? This is an indirect question about the kind of quantum evolution that is allowed for a quantum system which is addressed by the well-known postulate about its unitarity: *the evolution of a closed quantum system is determined by a unitary operator U. A state $|\Psi\rangle \in \mathscr{H}$ of a system at time t_1 is mapped into a state $|\widetilde{\Psi}\rangle \in \mathscr{H}$ at time t_2: $|\widetilde{\Psi}\rangle = U|\Psi\rangle$.*

The above postulate determines the dynamics of closed systems and allows operation of unitary operators only. However, the issue appears in the case of analysis of an evolution of open systems that can interact with other systems. The issue boils down to finding a mathematical representation of the physical processes that will be further identified with the allowed quantum operations on quantum systems. To solve this problem, it is assumed initially that the system in a state ρ_S, which evolution we are studying, is in a product state with its environment $\rho_S \otimes \rho_E$ (i.e. totally uncorrelated with the environment). Thus, the evolution of the whole system is unitary (under assumption that the whole system $S \otimes E$ is now a closed system) in accordance with the above postulate and the state of the system after interaction with the environment is:

$$\widetilde{\rho}_S = Tr_E[U(\rho_S \otimes \rho_E)U^\dagger]. \tag{2.33}$$

It is worth mentioning that the expectation value of any observable A acting on S does not depend on whether we consider only $\widetilde{\rho}_S$ or the whole composite system including the environment, i.e. $\langle A\rangle = Tr[A\widetilde{\rho}_S] = Tr[A \otimes \mathbb{I}[U(\rho_S \otimes \rho_E)U^\dagger]]$[3]. The latter is a fundamental observation about the nature of operations on systems and their extensions reflecting the fact that any quantum operation on a local subsystem maps the global state again to a proper quantum state. The local observer performs measurements on the environment in the selected environment database by means of partial trace operation on the environment and then forgets measurement results. Consequently, the state of a local system is a statistical mixture of states corresponding to the measurement results on the environment.

The analysis of operators Λ performing the mapping: $\rho_S \longrightarrow \widetilde{\rho}_S = \Lambda(\rho_S)$ is a subject of completely positive (CP) maps theory. Namely, all quantum operations are characterized as a set of mappings $\Lambda : \mathscr{B}(\mathscr{H}_1) \to \mathscr{B}(\mathscr{H}_2)$ meeting the following axioms:

(1) Λ is a linear operation,

[3] Vide sec. Quantum measurements and operations.

(2) Λ is completely positive [115],

(3) Λ does not increase trace, i.e. $Tr[\Lambda(\rho)] \leq 1$.

Complete positivity [115] reflects the aforementioned fact of mapping a proper quantum state into a proper quantum state (where an operation can be on the subsystem):

Definition 2.3.1 [4] *A linear map $\Lambda : \mathscr{B}(\mathscr{H}_1) \to \mathscr{B}(\mathscr{H}_2)$ is completely positive if and only if for any ancillary system on $\mathscr{H}_a$ and any operator $\Omega \in \mathscr{B}(\mathscr{H} \otimes \mathscr{H}_a)$ there holds:*

$$\Omega \geq 0 \Rightarrow (\Lambda \otimes I)\Omega \geq 0, \tag{2.34}$$

where I is the identity operator acting on $\mathscr{B}(\mathscr{H}_a)$.

If the operator preserves the trace we call it completely positive trace-preserving (CPTP), otherwise, it decreases the trace and is just completely positive(CP) - in this case the process is probabilistic, i.e. Λ-process occurs with probability $p_\Lambda = Tr[\Lambda(\rho)]$.

2.4 Quantum measurements and operations

The measurement results on quantum systems are classical values and as such have to be represented by real numbers which is a subject of the quantum mechanics postulate: *Any measurable physical property can be represented by an observable - a positive Hermitian operator $M \in \mathscr{B}(\mathscr{H})$. The allowed measurement results are real eigenvalues of M.* Thus a physical system can be completely characterized by the Banach tensored algebra of potential observables that can act on it. This statement is of a very deep physical and philosophical meaning about what is real and when the gathered information about the system is objective. Before we start considering properties of observables, it is worth mentioning that classical systems can be characterized by commutative observable algebras which is not the case for general quantum states.

Due to the assumption that the measurement results have to be real numbers, the eigenvectors $|\psi_i\rangle$ and eigenvalues λ_i for an observable M are in relation:

$$M|\psi_i\rangle = \lambda_i|\psi_i\rangle, \tag{2.35}$$

and in degenerate case one eigenvalue λ_i corresponds to many eigenvectors $|\psi_i^k\rangle$ spanning the eigenspace V_{λ_i}:

$$M|\psi_i^k\rangle = \lambda_i|\psi_i^k\rangle \;\; k = 1, 2, ..., j_n. \tag{2.36}$$

[4] For operators A i B it holds: $A \geq B$, if $\forall_{|\psi\rangle \in \mathscr{H}} \;\; \langle\psi|A - B|\psi\rangle \geq 0$.

Eigenvectors span an orthonormal basis in $\mathscr{H}$, thus:

$$\langle \psi_i^k | \psi_j^l \rangle = \delta_{ij}\delta_{kl} \;\; and \;\; \sum_i \sum_{k=1}^{j_n} |\psi_i^k\rangle\langle\psi_i^k| = I \tag{2.37}$$

Note that the projective operator on j_n-dimensional subspace $V \subset \mathscr{H}$ can be decomposed as a sum of one-dimensional projectors on basis vectors in this subspace:

$$P = \sum_{i=1}^{j_n} P_i. \tag{2.38}$$

and such an operator is a multi-dimensional projector.

Now, for any observable A we can find a spectral decomposition:

$$\begin{aligned} A &= IAI \\ &= \sum_i \sum_{k=1}^{j_n} |\psi_i^k\rangle\langle\psi_i^k| A \sum_j \sum_{l=1}^{j_m} |\psi_j^l\rangle\langle\psi_j^l| \\ &= \sum_i \sum_{k=1}^{j_n} \sum_j \sum_{l=1}^{j_m} |\psi_i^k\rangle\langle\psi_i^k|A|\psi_j^l\rangle\langle\psi_j^l|. \end{aligned} \tag{2.39}$$

Since $\langle \psi_i^k | A | \psi_j^l \rangle = \lambda_j \langle \psi_i^k | \psi_j^l \rangle = \lambda_j \delta_{kl}\delta_{ij}$ (where $|\psi_j^l\rangle$ are eigenvectors of A), then:

$$\begin{aligned} A &= \sum_i \sum_{k=1}^{j_n} \sum_j \sum_{l=1}^{j_m} \lambda_j \delta_{kl}\delta_{ij} |\psi_i^k\rangle\langle\psi_j^l| \\ &= \sum_i \sum_{k=1}^{j_n} \lambda_i |\psi_i^k\rangle\langle\psi_i^k| \\ &= \sum_i \lambda_i \widetilde{P}_i, \end{aligned} \tag{2.40}$$

where $\widetilde{P}_i = \sum_{k=1}^{j_n} |\psi_i^k\rangle\langle\psi_i^k|$.

The expectation value[5] of an observable A on a state $\rho \in \mathscr{B}(\mathscr{H})$ is:

$$\langle A \rangle = Tr[A\rho]. \tag{2.41}$$

[5]For a smooth wave function $|\Psi(x)\rangle$, the expectation value of observable A is defined as: $\langle A \rangle = \int \langle \Psi(x)|A|\Psi(x)\rangle dx$.

It is easy to derive that $Tr[A|\Psi\rangle\langle\Psi|] = \langle\Psi|A|\Psi\rangle$, then for $\rho = |\Psi\rangle\langle\Psi|$:

$$\begin{aligned}\langle A\rangle &= \langle\Psi|A|\Psi\rangle \\ &= \sum_i \lambda_i \langle\Psi|P_i|\Psi\rangle \\ &= \sum_i \sum_{k=1}^{j_n} \lambda_i \langle\Psi|\psi_i^k\rangle\langle\psi_i^k|\Psi\rangle \\ &= \sum_i \sum_{k=1}^{j_n} \lambda_i |\langle\psi_i^k|\Psi\rangle|^2,\end{aligned} \tag{2.42}$$

where $\sum_{k=1}^{j_n} |\langle\psi_i^k|\Psi\rangle|^2$ is a probability that a measurement on a state $|\Psi\rangle$ generates a result λ_i corresponding to the projector on a subspace spanned by $|\psi_i^k\rangle$.

Note that for a composite system $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_A)$ measurement of the expectation value Γ on B-subsystem gives:

$$\langle\Gamma\rangle = Tr_A[(I \otimes \Gamma)\rho_{AB}] = Tr(\Gamma\rho_B), \tag{2.43}$$

where $\rho_B = Tr_A\rho_{AB}$, i.e. measuring the subsystem of a composite system is equivalent to measuring the subsystem after performing the measurements on the rest of the global system in its basis (that of the rest) and forgetting this knowledge.

In general, any quantum operation can be represented by a linear operator $\Lambda : \mathscr{B}(\mathscr{H}_1) \longrightarrow \mathscr{B}(\mathscr{H}_2)$ where $\dim\mathscr{H}_1 = d_1$ and $\dim\mathscr{H}_2 = d_2$ with which one can associate a set of $d_2 \times d_1$ complex matrices $\{M_m\}_{m=1}^N$ where $\sum_{m=1}^N M_m^\dagger M_m = \mathbb{I}_{d_1}$. The matrices are called *Kraus operators* and the decomposition of quantum operation Λ is called a *Kraus decomposition*:

$$\Lambda(\rho) = \sum_{m=1}^{N} M_m \rho M_m^\dagger \tag{2.44}$$

The M_m operation transforms ρ into ρ_m state with probability $p_m = Tr[M_m\rho M_m^\dagger]$:

$$\rho \longrightarrow \rho_m = \frac{M_m\rho M_m^\dagger}{Tr[M_m\rho M_m^\dagger]} \tag{2.45}$$

A special case of operation is a *von Neumann measurement* when the Kraus operators are just projectors. In general setup, for this type of measurements we measure an observable $O = \sum_i \alpha_i P_i$ where $\forall_{i\neq j}\ \alpha_i \neq \alpha_j$ and $i \leq dim\mathscr{H}$. The measurement results belong to the set

of results related to the projectors P_i and the state is mapped as follows:

$$\rho \longrightarrow \widetilde{\rho} = \frac{\sum_i P_i \rho P_i}{Tr(\sum_i P_i \rho P_i)}. \tag{2.46}$$

And for the composite system in a state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ a measurement on its subsystem, say for A, leads to the transformation:

$$\rho_{AB} \longrightarrow \widetilde{\rho_{AB}} = \frac{\sum_i (P_i \otimes I_B)\rho_{AB}(P_i \otimes I_B)}{Tr[\sum_i (P_i \otimes I_B)\rho_{AB}(P_i \otimes I_B)]}. \tag{2.47}$$

One more important class of quantum measurements is called *POVMs* (positive-operator valued measurements) where we are not interested in the form of the output state but rather in the probability $p_m = Tr[M_m \rho M_m^\dagger] = Tr[M_m^\dagger M_m \rho]$ of the m-th result with which we can associate POVM element $E_m = M_m^\dagger M_m$. This means that the protocol is built on measuring the probability distribution $P(M = m) = Tr[E_m \rho]$ of the random variable M. In practice, the POVM is performed by coupling with the ancilla and then performing e.g. projective measurements on the ancillary system.

To summarize discussion about quantum operations and measurements as completely positive (CP) maps, it is very informative to remind that all classes of operations are derived from the fundamental postulate about unitary evolution of quantum systems, which is articulated in the following theorem:

Theorem 2.4.1 *Any quantum operation Λ on a quantum system A in a state ρ_A can be performed by three elementary operations:*
1. Adding of an ancillary system R (called also the reference system) in a state ρ_R:

$$\rho_A \longrightarrow \rho_A \otimes \rho_R \tag{2.48}$$

2. Performing an unitary operation U on the composite system $A \otimes R$:

$$\rho_A \otimes \rho_R \longrightarrow U \rho_A \otimes \rho_R U^\dagger \tag{2.49}$$

3. Tracing out the ancillary system R:

$$U \rho_A \otimes \rho_R U^\dagger \longrightarrow Tr_R[U \rho_A \otimes \rho_R U^\dagger] \tag{2.50}$$

This simple theorem is a powerful tool for many crucial theorems in quantum information theory, especially in reference to symmetric extensions of quantum systems and quantum channels.

In particular, we define LOCC operations as a finite composition of local quantum operations and classical communication. For Alice and Bob sharing the state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A) \otimes \mathscr{H}_B)$ we distinguish the following types of LOCC:

1. Zero-way $LOCC_\emptyset$ where no classical communication is allowed between the parties, only local trace-preserving CP maps $\Lambda_A : \mathscr{B}(\mathscr{H}_A) \longrightarrow \mathscr{B}(\mathscr{H}_A)$ and $\Lambda_B : \mathscr{B}(\mathscr{H}_B) \longrightarrow \mathscr{B}(\mathscr{H}_B)$:

$$\Lambda_\emptyset(\rho_{AB}) = \Lambda_A \otimes \Lambda_B(\rho_{AB}) \tag{2.51}$$

2. One-way $LOCC_\rightarrow$ where classical communication is allowed only in one direction, either from Alice to Bob or from Bob to Alice:

$$\Lambda_\rightarrow(\rho_{AB}) = \sum_i \Lambda_A^i \otimes \Lambda_B^i(\rho_{AB}) \tag{2.52}$$

where for one-way communication from Alice to Bob, $Tr[\sum_i \Lambda_A^i \otimes \mathbb{I}(\rho_{AB})] \leq 1$ (trace non-increasing operations on Alice's side) and trace-preserving operations on Bob's side are allowed, i.e. $Tr[\sum_i \mathbb{I} \otimes \Lambda_B^i(\rho_{AB})] = 1$. For the direction of classical communication from Bob to Alice, we assume trace non-increasing operations on Bob's side and trace-preserving on Alice's side.

3. Two-way $LOCC_\leftrightarrow$ operations can be viewed as a composition of local operations and classical communication in both directions, thus can be represented as a composition of trace non-increasing operations on both sides of Alice and Bob.

It is vital to note that for operations not preserving the trace of ρ_{AB}, the correct output state is $\widetilde{\rho_{AB}} = \Lambda(\rho_{AB})/Tr[\Lambda(\rho_{AB})]$.

2.5 Quantum channels

A quantum channel is a completely positive trace-preserving map (CPTP) $\Lambda : \mathscr{B}(\mathscr{H}_{in}) \rightarrow \mathscr{B}(\mathscr{H}_{out})$ acting on an input state $\rho_{in} \in \mathscr{B}(\mathscr{H}_{in})$ and resulting with the output state $\rho_{out} = \Lambda(\rho_{in})$. This concept is inherited from the classical information theory where the discrete source generates a signal that is transmitted through the noisy channel e.g. by the wire.

There holds a fundamental *channel-state* duality between quantum channels and states called as *Choi-Jamiolkowski isomorphism* [36, 37, 111]. The Choi-Jamiolkowski isomorphism is an isomorphism between linear maps $\Lambda : \mathscr{B}(\mathscr{H}_{in}) \rightarrow \mathscr{B}(\mathscr{H}_{out})$ and states living in the tensor product space $\mathscr{B}(\mathscr{H}_{in} \otimes \mathscr{H}_{out})$:

Theorem 2.5.1 *[36, 37] Consider the map $\Lambda : \mathscr{M}_n(\mathbb{C}) \longrightarrow \mathscr{M}_d(\mathbb{C})$, then the following statements are equivalent:*

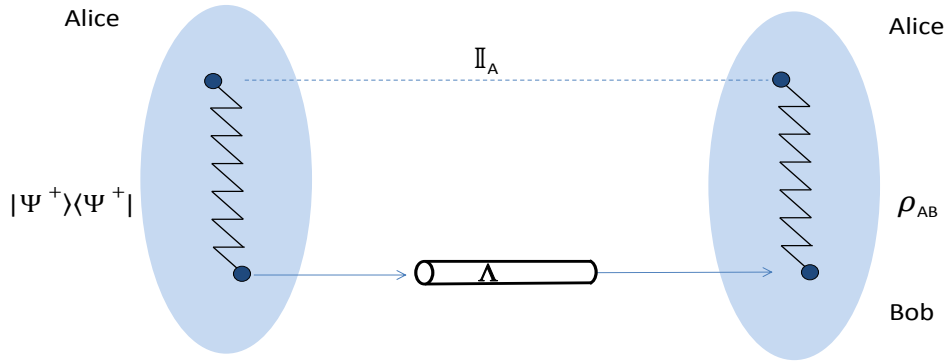

Fig. 2.1 Alice starts with a bipartite singlet state $|\Psi_+\rangle$ and sends one of the subsystem to Bob through the channel Λ. Alice and Bob after this operation share a state $\rho_{AB} = [\mathbb{I}_{\mathbb{A}} \otimes \Lambda]|\Psi_+\rangle\langle\Psi_+|$.

1. Λ *is completely positive,*

2. Λ *is n-positive, i.e.* $\Lambda \otimes \mathbb{I}_{\mathbb{C}^n}$ *is a positive map,*

3. For any orthonormal basis $\{|e_i\rangle\}$ *in* $\mathbb{C}^n$ *the* $nd \times nd$ *matrix is positive (known as Choi matrix of* Λ*):*

$$\Phi_\Lambda = \begin{pmatrix} \Lambda(|e_1\rangle\langle e_1|) & \cdots & \Lambda(|e_1\rangle\langle e_n|) \\ \vdots & \ddots & \vdots \\ \Lambda(|e_n\rangle\langle e_1|) & \cdots & \Lambda(|e_n\rangle\langle e_n|) \end{pmatrix} \tag{2.53}$$

Namely, assume that a quantum state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is shared between two parties Alice and Bob. The isomorphism states that it can be achieved if Alice holds initially a maximally entangled bipartite state $|\Psi_+\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}}|ii\rangle$ (a singlet, $d = dim\mathscr{H}_A$) and sends [111] one part of it to Bob through the channel $\Lambda : \mathscr{B}(\mathscr{H}_A) \longrightarrow \mathscr{B}(\mathscr{H}_B)$ [Fig. 2.1]:

$$\rho_{AB} = [\mathbb{I}_{\mathbb{A}} \otimes \Lambda]|\Psi_+\rangle\langle\Psi_+| \tag{2.54}$$

Every physical quantum system is a subject of interactions with the environment and decoherence which can be interpreted as an influence of noise. Quantum noise, in similar to the classical concept of *noise*, transforms the input state by means of a quantum channel Λ

characterizing the noise process. In general, it is assumed that noise is spatially *local and Markovian*. The former means that there are not spatial correlations between the operators introducing noise to the system and the latter means that they are not temporally correlated. Obviously, one can analyze other models of noise but for needs of these thesis, whenever we use the term 'noise', we think about local and Markovian noise.

As already observed, there are a couple of alternative representations of quantum channels. We have already used the famous Choi-Jamiolkowski isomorphism and the Kraus representation for quantum operations. We can also define quantum channels by means of the Stinespring dillation [156] which inherits its intuition on the aforementioned observation that any quantum operation on a quantum state ρ of a system can be perceived as an action of a unitary operation on the larger extended system extended with the auxiliary system, which is traced out after this action.

Theorem 2.5.2 *(Stinespring Theorem) Let $\Lambda : \mathscr{B}(\mathscr{H}) \longrightarrow \mathscr{B}(\mathscr{H})$ be a linear map. Then Λ is completely positive if and only if it has the form:*

$$\Lambda(A) = V^* \pi(A) V \tag{2.55}$$

for some unital $*$-homomorphism[6] *$\pi : A \longrightarrow \mathscr{B}(K)$ on a Hilbert space K and for some bounded linear map $V : \mathscr{H} \longrightarrow K$.*

Then, for every quantum channel $\Lambda : \mathscr{B}(\mathscr{H}_A) \longrightarrow \mathscr{B}(\mathscr{H}_{A'})$, there exist a unitary matrix U, some auxiliary space K and the state γ_B such that:

$$\rho_{A'} = \Lambda(\rho_A) = Tr_K U[\rho_A \otimes \gamma_B] U^\dagger \tag{2.56}$$

Below we present important examples of quantum channels.

Pauli channels

In a Pauli qubit channel $\Lambda : \mathscr{B}(\mathbb{C}^2) \longrightarrow \mathscr{B}(\mathbb{C}^2)$ every error (i.e. X, Y, Z) can occur with an arbitrary probability. Thus the input state will be not changed with probability $1-p = 1-(p_1+p_2+p_3)$ (i.e. with this probability the channel will act with identity mapping $\mathbb{I}$ on the state) and its representation is:

$$\Lambda(\rho) = (1-p)\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z, \tag{2.57}$$

[6] π is a unital $*$-homomorphism, i.e. is linear, multiplicative, and preserves the $*$-operation - an involution that is conjugate-linear and anti-multiplicative.

It can be represented in the formalism of linear operators A_i (so-called Kraus operators) as:

$$A_0 = \sqrt{1-p}I,\ A_1 = \sqrt{p_1}X,\ A_2 = \sqrt{p_2}Y,\ A_3 = \sqrt{p_3}Z, \tag{2.58}$$

Particular types of Pauli random channels are:

A bit flip channel:

$$A_0 = \sqrt{1-p}I,\ A_1 = \sqrt{p}X. \tag{2.59}$$

A phase flip channel:

$$A_0 = \sqrt{1-p}I,\ A_1 = \sqrt{p}Z. \tag{2.60}$$

A bit and phase flip channel:

$$A_0 = \sqrt{1-p}I,\ A_1 = \sqrt{p}Y. \tag{2.61}$$

A depolarizing channel:

$$\Lambda(\rho) = p\frac{I}{2} + (1-p)\rho, \tag{2.62}$$

which generates pure noise as a maximally mixed state $\frac{I}{2}$ with probability p. It has an operator representation:

$$A_0 = \sqrt{1-\frac{3p}{4}}I,\ A_1 = \sqrt{p}\frac{X}{2},\ A_2 = \sqrt{p}\frac{Y}{2},\ A_3 = \sqrt{p}\frac{Z}{2}\,, \tag{2.63}$$

which is derived from:

$$\frac{I}{2} = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z). \tag{2.64}$$

Amplitude damping channel

This channel models dissipation of energy when e.g. an excited atom in a state $|1\rangle$ during a process of spontaneous emission transitions to the ground state $|0\rangle$ having emitted a photon with probability γ:

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix},\ A_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}. \tag{2.65}$$

Noteworthily, this channels, as opposed to Pauli channels, do not preserve the identity ($\Lambda(I) \neq I$).

2.6 Quantum entanglement and separability of quantum states

Quantum mechanics allows the existence of composite systems spatially separated, in a global state $|\psi\rangle \in \mathscr{H}$, yet locally none of their sub-systems can have a pure state assigned. These "exotic" states called entangled states manifest a fundamental difference of correlations between classical and quantum world.

Theorem 2.6.1 *(The Schmidt decomposition [107]) Let* $\dim \mathscr{H}_1 = m$ *and* $\dim \mathscr{H}_2 = n$ *and* $|\widehat{\psi}\rangle$ *be a normalized vector in* $\mathscr{H}_1 \otimes \mathscr{H}_2$*, and* $\rho = |\widehat{\psi}\rangle\langle\widehat{\psi}|$, $\rho_1 = Tr_2\rho$, $\rho_2 = Tr_1\rho$. *Then:*

(1) *the reduced matrices* ρ_1 *i* ρ_2 *have the same positive eigenvalues* $\lambda_1, ..., \lambda_k$ *(with the same multiplicity) and every additional dimension of these matrices is 'built' with a zero-eigenvalue (note that then* $k \leq min(m,n)$*).*

(2) $|\widehat{\psi}\rangle$ *is represented as:*

$$|\widehat{\psi}\rangle = \sum_{i=1}^{k} \sqrt{\lambda_i}|\widehat{e_i}\rangle \otimes |\widehat{f_i}\rangle, \tag{2.66}$$

where $|\widehat{e_i}\rangle$ *(and* $|\widehat{f_i}\rangle$*) are orthonormal eigenvectors of* $\rho_1 \in \mathscr{B}(\mathscr{H}_1)$ *(and* $\rho_2 \in \mathscr{B}(\mathscr{H}_2)$*),* $\sum_i \lambda_i = 1$ *and* $\lambda_i \geq 0$.

The $\sqrt{\lambda_i}$ are so-called *Schmidt coefficients* and the number of non-zero coefficients in Schmidt decomposition of $|\widehat{\psi}\rangle$ is called *the Schmidt rank* of the state $|\widehat{\psi}\rangle$.

Example 2.6.2 *As an example let us consider a state* $\Psi \in \mathscr{H}_A \otimes \mathscr{H}_A \cong \mathbb{C}^2 \otimes \mathbb{C}^2$*, in that case the Schmidt decomposition can consist of at most two coefficients. The state is a product vector if* $\sqrt{\lambda_1} = 0$ *and* $\sqrt{\lambda_2} = 1$ *or* $\sqrt{\lambda_1} = 1$ *and* $\sqrt{\lambda_2} = 0$*. A state with coefficients* $\sqrt{\lambda_1} = \sqrt{\lambda_2} = \frac{1}{\sqrt{2}}$ *is maximally entangled in* $\mathscr{H}_A \otimes \mathscr{H}_B$ *(maximal entanglement means that quantum correlations are maximal in relation to a given entanglement measure [137] as shown in the following chapters). Maximally entangled states in a computation basis* $\{|0\rangle, |1\rangle\}$ *are the Bell states (which span the maximally entangled basis in* $\mathbb{C}^2 \otimes \mathbb{C}^2$*):*

$$\begin{cases} |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \\ |\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle). \end{cases} \tag{2.67}$$

Note that the Schmidt decomposition is unique because there do not exist two different decompositions of a given state with different number of λ_i. Moreover, if the Schmidt rank is more than 1 then the state is entangled and the subsystems are in mixed states.

In general, any separable state (in terms of density matrix) can be decomposed to product elements as a convex combination of separable states (i.e. any convex combination of separable states is again a separable state which is not always true for entangled states - e.g. one can find a decomposition of a noise state of a bipartite system in the Bell basis, $\mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2) \ni \rho_{AB} = \frac{1}{4}\mathbb{I} = \frac{1}{4}(|\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-| + |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|)$)

Applying the results by R. Werner [167], we remind now a definition of quantum separability:

Definition 2.6.3 *The state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is separable if and only if it can be represented as a convex combination of product states:*

$$\rho_{AB} = \sum_{i=1}^{k} p_i \rho_A^i \otimes \rho_B^i,\ 0 \leq p_i \leq 1,\ \sum_{i=1}^{k} p_i = 1, \tag{2.68}$$

or if it can be approximated by separable states in a trace norm[7]*. Otherwise, the state is called entangled or non-separable.*

Remark. Approximation in this case means that there exists such a series of separable states $\{\rho_n^{AB}\}$ where $\rho_n^{AB} = \sum_j p_j \rho_j^A \otimes \rho_j^B$ so that $\lim_{n\to\infty} \|\rho_n^{AB} - \rho_{AB}\| = 0$.

The aforementioned definition states clearly that any separable state $\rho_{AB} = \sum_i p_i |e_i\rangle\langle e_i| \otimes |f_i\rangle\langle f_i|$ shared between two parties Alice and Bob can be prepared by means of LOCC (local operations and classical communication) which is not possible for any entangled state. For such a setup, Alice generates states $|e_i\rangle$ with probability p_i locally and Bob generates $|f_i\rangle$ with probability p_i correspondingly, however, for generation of classical correlations between the local states they can use classical communication medium like e.g. a phone.

Quantum entanglement is one of central concepts in quantum information theory and as such is a subject of very extensive research, especially as a resource for quantum computation and quantum cryptography. For many years one of the main open problems was to define necessary and sufficient conditions for separability of all quantum states, that would be also operationally efficient (i.e. could be calculated quickly e.g. by semi-definite programming or analytically for a given state). To date we have known a couple of such conditions for different classes of states, however, this research field is still open. Below we recall key conditions and in the following chapters, a reader will see that symmetric extendibility is also a central concept for this field. The very first complete characterization of such a test in terms of necessary and sufficient conditions was based on a concept of completely positive maps:

[7] A trace norm is defined as $\|A\|_{Tr} = Tr|A|$.

Theorem 2.6.4 *[99] The state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is separable if and only if for any positive map $\Lambda : \mathscr{B}(\mathscr{H}_B) \longrightarrow \mathscr{B}(\mathscr{H}_B)$, an operator $(\mathbb{I} \otimes \Lambda)\rho_{AB}$ is positive.*

We introduce also a partial transposition operator Γ_B acting on B-part (or any subsystem of the composite state) of state ρ_{AB}:

Definition 2.6.5 *The partial transposition [143] on B-subsystem of the composite system AB in a state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is:*

$$\Gamma_B(\rho_{AB}) = (\mathbb{I}_A \otimes T_B)\rho_{AB} \tag{2.69}$$

where transposition $T_B : \mathscr{B}(\mathscr{H}_B) \longrightarrow \mathscr{B}(\mathscr{H}_B)$ acts only on B-part.

For matrix elements the Γ operation acts as follows:

$$\Gamma_B(\rho_{AB}) = \Gamma_B(\sum_{ijkl} a_{ijkl}|ij\rangle\langle kl|) = \sum_{ijkl} a_{ijkl}|il\rangle\langle kj| \tag{2.70}$$

The Peres citerion [143] of separability based on the above operation is:

Theorem 2.6.6 *Any separable state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is PPT:*

$$\Gamma_B(\rho_{AB}) \geq 0 \tag{2.71}$$

i.e. $\Gamma_B(\rho_{AB})$ has non-negative eigenvalues.

and it does not matter if we consider Γ_B or Γ_A. As a consequence of the above theorems, for $2 \otimes 2$ and $2 \otimes 3$ systems it is sufficient to check their partial transpositions and verify if the output state is positive (PPT) or negative (NPT). For the first case one immediately finds the PPT state separable, for the latter (NPT) entangled. This observation is stated in the following lemma:

Lemma 2.6.7 *[99] A state $\rho \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ or $\rho \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^3)$ is separable if and only if $\Gamma(\rho)$ is a positive operator.*

Of a great importance is an observation that although all separable states are PPT, not every entangled state is NPT. There exists a broad class of entangled states called *bound entangled* [100], which have positive partial transpositions (PPT) and from which no entanglement can be distilled by means of two-way LOCC (that will be a subject of further chapters).

Other entanglement criteria, which will be not a matter of consideration in this thesis, include the range and matrix realignment criteria, and the reduction criterion [101, 30]. In the following chapter, we will refer to the criteria based on Bell inequalities.

2.7 Quantum entropic quantities

In this section we recall fundamental quantum entropic quantities which will be a necessary tool for quantitative analysis of entanglement and its applications to quantum information processing.

The von Neumann entropy (a quantum counterpart of classical Shannon entropy for a probability distribution P: $H(P) \equiv -\sum_x P(x)\log P(x)$) is defined as:

$$S(\rho_{AB}) = -Tr(\rho_{AB}\log\rho_{AB}) \tag{2.72}$$

in many cases we will just use S_{AB} notation.

In analogy to classical relative entropy between two probability distributions, which measure how different they are from each other, we define *the quantum relative entropy* between states ρ and σ as:

$$R(\rho\|\sigma) = Tr[\rho(\log\rho - \log\sigma)] \tag{2.73}$$

where $supp(\sigma) \subseteq supp(\rho)$ with $supp(\cdot)$ denoting the subspace spanned by the eigenvectors of the corresponding density matrix.
Relative entropy is unitarily invariant, i.e. for any U, $R(U\rho U^\dagger\|U\sigma U^\dagger) = R(\rho\|\sigma)$ and positive $R(\rho\|\sigma) \geq 0$. It possess also two other important properties:
Joint convexity - for any $p \in [0,1]$ and any four states$\{\rho_a,\rho_b,\sigma_c,\sigma_d\} \in \mathscr{B}(\mathscr{H})$ there holds[8]:

$$R(p\rho_a + (1-p)\rho_b\|p\sigma_c + (1-p)\sigma_d) \leq pR(\rho_a\|\sigma_c) + (1-p)R(\rho_b\|\sigma_d) \tag{2.74}$$

Monotonicity under CP maps - for any completely positive map Λ:

$$R(\Lambda(\rho)\|\Lambda(\sigma)) \leq R(\rho\|\sigma) \tag{2.75}$$

The Holevo function $\chi(\cdot)$ is defined for any ensemble of density matrices $\mathfrak{A} = \{p_i,\rho_i\}$ with average density matrix $\rho = \sum_i p_i\rho_i$ as follows:

$$\chi(\rho) = S(\sum_i p_i\rho_i) - \sum_i p_i S(\rho_i) \tag{2.76}$$

and is a good upper bound [90, 91] on the accessible information. Whenever we use $\chi(\rho)$, we understand that the Holevo function is a function of the aforementioned ensemble $\chi(\mathfrak{A})$.

[8] An operator convex function is a function such that: $f(pA + (1-p)B) \leq pf(A) + (1-p)f(B)$, for $p \in [0,1]$, and Hermitian operators A and B (see a footnote on page 12).

Basing on the Holevo function, we derive also the observation [127] that will be later used for finding efficient reduced variants of different quantum measures:

Observation 2.7.1 *[127] For any ensemble of density matrices $\mathfrak{A} = \{\lambda_i, \rho^i_{BB'}\}$ with average density matrix $\rho_{BB'} = \sum_i \lambda_i \rho^i_{BB'}$ there holds:*

$$\chi(\rho_{BB'}) \leq \chi(\rho_B) + 2S(\rho_{B'}) \tag{2.77}$$

Proof. Basing on subadditivity[9] and concavity of quantum entropy we can easily show that:

$$\begin{aligned} & |S(\rho_{BB'}) - \sum_i p_i S(\rho^i_{BB'}) - S(\rho_B) + \sum_i p_i S(\rho^i_B)| \leq \\ \leq \; & |S(\rho_{BB'}) - S(\rho_B)| + |\sum_i p_i S(\rho^i_{BB'}) - \sum_i p_i S(\rho^i_B) \\ \leq \; & S(\rho_{B'}) + \sum_i p_i S(\rho^i_{B'}) \leq 2S(\rho_{B'}) \end{aligned}$$

which completes the proof. □

For any bipartite state ρ_{AB} one defines *the quantum mutual information*:

$$I(A:B) = S(A) + S(B) - S(AB) \tag{2.78}$$

and further, for a tripartite system ρ_{ABC} *the conditional quantum mutual information*:

$$I(A:B|C) = S(AC) + S(BC) - S(ABC) - S(C) \tag{2.79}$$

where we use the notation for entropy of X system $S(\rho_X) = S(X)$.

The coherent information for a channel Λ and a source state σ transferred through the channel is defined as:

$$I_c(\sigma, \Lambda) = I^B(I \otimes \Lambda)(|\Psi\rangle\langle\Psi|) \tag{2.80}$$

where Ψ is a pure state with reduction σ and coherent information of a bipartite state ρ_{AB} shared between Alice and Bob is defined as: $I^B(\rho_{AB}) = S(B) - S(AB)$. We will use further the following notation: $I_c(A\rangle B) = I^B(\rho_{AB})$.

[9] Quantum entropy is subadditive, i.e. for any $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$, there holds: $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$.

Chapter 3

Monogamy of quantum entanglement and Bell theorem

In this chapter we explore the concept of monogamy of quantum entanglement and its relation to symmetric extendibility. Further, we recall local realism and its violation by entangled states reflected in violation of Bell inequalities which meet the conditions for Local Hidden Variables (LHV). The chapter indicates also crucial connections between symmetric extendibility and potential violation of Bell inequalities.

3.1 Local realism and Bell inequalities

Quantum entanglement is a phenomenon which does not have any reflection in classical world and as such is a manifestation of so-called non-locality of quantum correlations. The roots of studies in this matter reach the year 1935 when the famous paper by Einstein, Podolsky and Rosen [63] discussed the so-called (EPR) pairs being in a bipartite singlet state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ shared between two spin $\frac{1}{2}$ particles. In such a case none of the subsystems can have assigned a pure state as aforementioned in the previous chapter.

In particular, many entangled states violate *local realism* and in consequence, Bell inequalities [12]. Local realism has roots in classical world-view where for particular measurement of physical quantities, one believes that the measured physical quantities for a physical object have a priori set values independent of the observers (realism) and for a bipartite setup the measurement on one site does not influence the results of the other site's measurements (locality):

Realism. The physical quantities being a subject of the measurements have definite real values which exist independent of the observation act.

Locality. The results of measurements performed by Alice do not influence the results of measurements performed by Bob.

It is worth mentioning that the experiment is arranged so that for two parties Alice and Bob, their experiments are causally disconnected. Thus, the measurement performed by Alice cannot influence the measurements done by Bob due to the light speed limit imposed by the special relativity theory.

To analyze correlations between results achieved in the experiment performed by Alice and Bob, imagine that they share a bipartite physical system consisting of two spatially separated sub-systems that could interact in the past and which will be a subject of local measurements in distant laboratories belonging to Alice and Bob respectively (*a distant lab paradigm*). Now, we can assign conditional probabilities to the measurement results $P(a,b|x,y)$ where x and y stand for measurement settings set locally by Alice and Bob respectively, and a and b for the measurement outcomes. Note that the measurement outcomes can be naturally inter-dependent, i.e. $P(a,b|x,y) \neq P(a|x)P(b|y)$ - the dependency can be created by *a local hidden variable* $\lambda \in \Lambda$ that the experimenters are not aware of. The hidden variables are a building block behind Bell inequalities and as such represent a hidden knowledge that cannot be possessed during the measurement process but influence the measurement results and correlate them. The hidden variable is obviously also pre-defined in accordance with the local realism.

Since the local measurement results are dependant only on x-settings and λ-variable for Alice, and respectively on y-settings and λ-variable for Bob in local hidden variables (LHV) model, and moreover, we assume locality, then:

$$P(a,b|x,y,\lambda) = P(a|x,\lambda)P(b|y,\lambda) \tag{3.1}$$

For discrete distribution of λ on Λ-space, after many measurement series we obtain (it reflects a random character of λ in many measurements repeated on the system):

$$P(a,b|x,y) = \sum_{\lambda\in\Lambda} p(\lambda)P(a|x,\lambda)P(b|y,\lambda) \tag{3.2}$$

For continuous distribution of λ on Λ-space, we get a local hidden variable model:

$$P(a,b|x,y) = \int_{\Lambda} p(\lambda)P(a|x,\lambda)P(b|y,\lambda)d\lambda \tag{3.3}$$

In general, every linear Bell inequality for bipartite setup $\mathbf{B}(A,B)$ of an experiment performed by Alice and Bob can be represented as a linear combination of conditional

probabilities $P(a,b|x,y)$ (R is a local realistic bound):

$$\mathbf{B}(A,B) \equiv \sum_{xy}\sum_{ab} \alpha(a,b,x,y)P(a,b|x,y) \leq R \tag{3.4}$$

and $\alpha(a,b,x,y) \geq 0$ parameters characterize the specific Bell inequality. These inequalities have to be satisfied by all classical correlations with the aforementioned probability distributions $P(a,b|x,y)$ built on LHV models.

The LHV model generates the probability vector $\overline{P} = [P(a,b|x,y)]$ having entries $0 \leq P(a,b|x,y) \leq 1$ where vectors $\overline{P}$ form a convex polytope S. The extreme points of the polytope are the extremal $\overline{B}$ vectors with $\{0,1\}$ entries. Each extreme vector $\overline{B}$ reflects a setup of the experiment where the outcomes of the measurements are determined with certainty, i.e. $B^{m,n}_{ij,kl} = \delta_{jm_i}\delta_{in_k}$ with two sets of indices $m = \{m_1,\ldots,m_{s_a}\}$ (s_a is the number of measurement settings on Alice' site and m_i indicates number of the measurement outcomes for the i-th measurement setting) and respectively for Bob $n = \{n_1,\ldots,n_{s_b}\}$.

For quantum correlations between a bipartite system in a state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ shared between Alice and Bob, the probability distribution for their measurement results is given by $P(j,l|i,k) = Tr(E^A_{ij} \otimes E^B_{kl}\rho_{AB})$. The POVM elements for Alice's i-th measurement setting (and j denotes outputs of the measurement setting) are $\{E^A_{ij} |\ E^A_{ij} \geq 0 \wedge \sum_j E^A_{ij} = \mathbb{I}\}$.

Example 3.1.1 *(CHSH inequalities) We can assume that the experiment is led between two sites shared by Alice and Bob. Assume that a source emits two particles in their directions and that Alice and Bob can perform randomly one of two dichotomic measurements $A_{1,2}$ and $B_{1,2}$ ($A_i^2 = B_i^2 = \mathbb{I}$ for $i \in \{1,2\}$ and the outcomes of the measurements are associated to projective measurements on $\mathscr{H} \cong \mathbb{C}^2$). Then for any setup of the experiment producing LHV results of the measurements, the CHSH [39] inequality can be formulated:*

$$|E(A_1B_1) + E(A_1B_2) + E(A_2B_1) - E(A_2B_2)| \leq 2 \tag{3.5}$$

where $E(A_i,B_j) = \sum_{ab} abP(ab|ij)$ is the expectation value for the measurements A_iB_j. For quantum mechanical description of the experiment, we can use the CHSH operator

$$\mathbf{B} = A_1 \otimes (B_1 + B_2) + A_2 \otimes (B_1 - B_2) \tag{3.6}$$

remembering that the expectation value, for a quantum state ρ_{AB} of those two particles, is $E(A_i,B_j) = Tr[A_i \otimes B_j\rho_{AB}]$. Then for all quantum states ρ_{AB} admitting a LHV model, there holds:

$$|Tr\mathbf{B}\rho_{AB}| \leq 2 \tag{3.7}$$

It is also very interesting to note that CHSH inequality has also its so-called *Tsirelson bound* [38] for all possible probability distributions allowed by quantum mechanics, i.e. when $E(A_i,B_j) = Tr[A_i \otimes B_j \rho_{AB}]$. Then for $\mathbf{B} = A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$, we get $\mathbf{B}^2 = 4\mathbb{I} - [A_0,A_1][B_0,B_1]$ and in result the Tsirelson bound follows:

$$|Tr\mathbf{B}\rho_{AB}| \leq 2\sqrt{2} \tag{3.8}$$

The fundamental observation about Bell inequalities is that all classical correlations met them and as observed by R. Werner [167], in general, all separable states being measured in the experiment will produce probability distributions meeting Bell inequalities:

Theorem 3.1.2 *[167] Any separable state ρ allows results of the local von Neumann measurements in agreement with a local hidden variables model.*

However, non-local correlations in general violate them. Yet, R. Werner built an important class of non-local $U \otimes U$-invariant states [1] which for some parameters can generate results with probability distribution described by LHV.

To be more precise, for any entangled state one can find a Bell inequality which will be violated but at the same time there exists a broad class of entangled states [167] that satisfy most popular Bell inequalities. In summary, when every separable state satisfy a given Bell inequality, entangled states can violate or satisfy an arbitrary chosen Bell inequality. These observations become clear when we look at the geometry of quantum states sets.

We remind now in this context a crucial Hahn-Banach theory for convex spaces [147]:

Theorem 3.1.3 *(Hahn-Banach) [Fig. 3.1] Let S be a convex subset of a vector space V, and let P be a point in V such that $P \notin S$. Then there exists a hyperplane H which separates the point P from the subset S.*

It seems now to be clear that due to convexity of the separable states set[2], any entangled state can be separated from the set of separable states by some hyperplane. Such a hyperplane in a Hilbert-Schmidt space $\mathscr{B}(\mathscr{H})$ can be defined by its normal vector which is a hermitian operator (thus, can be perceived as an observable):

Definition 3.1.4 *[99] An entanglement witness W for a state $\rho \in \mathscr{B}(\mathscr{H})$ is a hermitian operator satisfying:*

$$Tr(W\rho) < 0 \text{ and } Tr(W\rho_{sep}) \geq 0, \tag{3.9}$$

for any separable state $\rho_{sep} \in \mathscr{B}(\mathscr{H})$.

[1] Vide sec. Isotropic states.

[2] It can by immediately observed that for any two separable states $\rho = \sum_{ij} p_{ij}\rho_i \otimes \sigma_j$ and $\sigma = \sum_{kl} p'_{kl}\rho'_k \otimes \sigma'_l$, their convex combination $\alpha\rho + (1-p)\sigma$ ($p \in [0,1]$) is also separable.

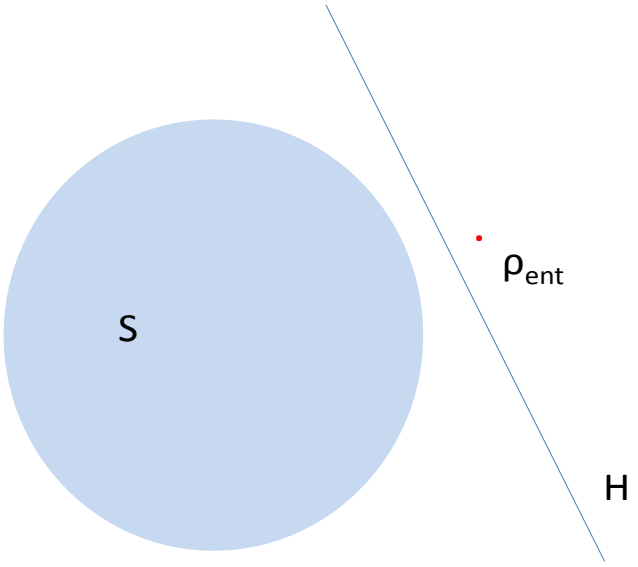

Fig. 3.1 Hyperplane H separates an entangled state $\rho_{ent} \in \mathscr{B}(\mathscr{H})$ from a convex set S of separable states in the space $\mathscr{B}(\mathscr{H})$ in accordance with the Hahn-Banach theorem.

It is now not difficult to observe that we may view Bell inequalities by prism of entanglement witnesses concept [108], where the linear inequality performs intersection of the space $\mathscr{B}(\mathscr{H})$ of quantum states and the set of separable states is included in one of the half-spaces.

As an example we can reformulate the **B** operator for CHSH inequalities as a CHSH witness which is non-negative on all LHV states [162]:

$$W_{CHSH} = 2\mathbb{I} + \mathbf{B} \tag{3.10}$$

where $\mathbb{I}$ stands for the identity operator.

It is now a very dynamic field of research to find more accurate methods of identifying if a state is separable or not, either by means of non-linear Bell inequalities (where the set of separable states is surrounded by curved hyper-surfaces in $\mathscr{B}(\mathscr{H})$) [148] or by the sets of linear Bell inequalities (they form a polytope-like structure, with facets represented by the inequalities, around the set of separable states) [144].

No-signalling

Quantum mechanics meets also the no-signalling principle having its roots in the light speed limit imposed by the special relativity theory. For Alice and Bob performing measurements

in distant labs, the choice of the measurement setting on one side (Alice or Bob) cannot influence the other's side choice due to the spatial separation. It is formulated as:

$$\begin{aligned} P(a|x) = P(a|x,y) = \sum_b P(a,b|x,y) \\ P(b|y) = P(b|x,y) = \sum_a P(a,b|x,y) \end{aligned} \tag{3.11}$$

It is interesting to observe that there exist probability distributions meeting no-signalling principle which are not allowed by quantum mechanics, like the PR-box [134]. In this sense, no-signalling theories are broader than quantum mechanics [134, 7, 8].

3.2 Quantum entanglement is monogamous

One of the fundamental questions related to quantum entanglement, as a resource shared between two parties Alice and Bob, is whether the correlations could be shared between more parties. The questions is fundamental not only due to applications in quantum computation or quantum cryptography but also due to the very nature of processing information between physical systems at different levels of complexity. It finds out that shareability of quantum correlations is bounded and it has its roots in *monogamy of entanglement*.

One can refer to a broadly used explanation [43] for spatial monogamy of entanglement between parties ABC. It states that A cannot be simultaneously fully entangled with B and C since then AB would be entangled with C having a mixed density matrix that contradicts purity of the singled state shared between A and B. It is expressed in Coffman-Kundu-Wootters (CKW) [43] monogamy inequality for three-qubit system in a state ρ_{ABC}:

$$C^2(\rho_{A|BC}) \leq C^2(\rho_{AB}) + C^2(\rho_{AC}) \tag{3.12}$$

where $C(\cdot)$ stands for the concurrence between the parties (e.g. $C^2(\rho_{A|BC})$ between A and BC subsystems). $C(\rho_{AB})$ is an entanglement monotone[3], and is defined as the averaged concurrence of an ensemble of pure states $\{p_i, |\Psi_i^{AB}\rangle\}$ corresponding to ρ_{AB} minimized over all pure decompositions of $\rho_{AB} = \sum_i p_i |\Psi_i^{AB}\rangle\langle\Psi_i^{AB}|$ [43]:

$$C(\rho_{AB}) = inf \sum_i p_i C(|\Psi_i^{AB}\rangle) \tag{3.13}$$

[3] Vide sec. Entanglement measures.

and respectively for all other states. Concurrence of a pure state is $C(|\Psi^{AB}\rangle) = \sqrt{2[1-Tr(\rho_A^2)]}$ and $\rho_A = Tr_B|\Psi^{AB}\rangle\langle\Psi^{AB}|$.

If a bipartite state is in a singlet state $\rho_{AB} = |\Psi^+\rangle\langle\Psi^+|$, then clearly the only possible tripartite extensions are of the form $\rho_{ABE} = \rho_{AB} \otimes \rho$, i.e. no symmetric extension of $|\Psi^+\rangle$ exists. That is also an immediate implication of the Schmidt decomposition for any purification of ρ_{ABE} to a state $\Psi_{ABEE'}$ which has to be decomposed to a factorized state $\Psi_{ABEE'} = |\Psi^+\rangle \otimes |\Phi_{EE'}\rangle$ if for its reduction AB one wants to get $\rho_{AB} = |\Psi^+\rangle\langle\Psi^+|$. Thus, we get at least two proofs of monogamy of entanglement, one based on entanglement measures and one based on purely geometrical considerations.

The concept of symmetric extendibility is directly related to monogamy of quantum entanglement and that phenomenon was a building block for initiation of broad studies of symmetric extendibility applications. If a bipartite state is in a singlet state $\rho_{AB} = |\Psi^+\rangle\langle\Psi^+|$, then clearly the only possible tripartite extensions are of the form $\rho_{ABE} = \rho_{AB} \otimes \rho$ as aforementioned and no symmetric extension of $|\Psi^+\rangle$ exists.

Symmetric extendibility [55, 56, 161, 128] of a given bipartite state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ (the Banach space of bounded operators) denotes that there exists a tripartite state $\rho_{ABE} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_B)$ invariant due to permutation of B and E part.

Definition 3.2.1 *(Symmetric extension) A state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is symmetrically extendible if there exists such a state $\rho_{ABE} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_B)$ ($\mathscr{H}_B = \mathscr{H}_E$) so that for permutation:*

$$P = \sum_{ijk} |ijk\rangle\langle ikj| \tag{3.14}$$

there holds $P\rho_{ABE}P^\dagger = \rho_{ABE}$ and $Tr_E\rho_{ABE} = \rho_{AB} = \rho_{AE}$.

3.3 Monogamy of Bell inequalities vs. symmetric extendibility of quantum states

We can relate violation of Bell inequalities with the existence of so-called symmetric extensions or quasi-extensions of quantum states witch is directly related to symmetric extendibility of a given quantum state [128].

In [55, 56, 161], B. Terhal, A. Doherty and D. Schwab proposed more general concept of quasi-symmetric extension H_ρ, basing on observations done by R. Werner in [169] [4]. These observations lead later to a crucial relation between symmetric extendibility and violation of any Bell inequality. H_ρ is an entanglement witness which is not necessarily positive:

[4] Vide sec. The separability problem *vs.* symmetric extendibility.

Definition 3.3.1 *[161] (Symmetric quasi-extension) Let $\pi : \mathscr{H}^{\otimes s} \to \mathscr{H}^{\otimes s}$ be a permutation of spaces $\mathscr{H}$ in $\mathscr{H}^{\otimes s}$. One defines:*

$$Sym(\rho) = \frac{1}{s!}\sum_{\pi} \pi\rho\pi^{\dagger} \tag{3.15}$$

Then ρ on $\mathscr{H}_A \otimes \mathscr{H}_B$ has a (s_a, s_b)-symmetric quasi-extension if there exists a multipartite entanglement witness H_ρ on $\mathscr{H}_A^{\otimes s_a} \otimes \mathscr{H}_B^{\otimes s_b}$ such that $Tr_{\mathscr{H}_A^{\otimes s_a-1}, \mathscr{H}_B^{\otimes s_b-1}} H_\rho = \rho$ and $H_\rho = Sym_A \otimes Sym_B(H_\rho)$.

Application of this definition leads to the observation that, if ρ_{AB} has a symmetric extension for Bob, then ρ_{AB} does not violate a Bell inequality with k settings on Bob's side and any number of settings on Alice' side which is a subject of the following general theorems:

Theorem 3.3.2 *[161] If ρ has a (s_a, s_b) symmetric quasi-extension, then ρ does not violate Bell inequalities with (s_a, s_b)-settings.*

Proof. The theorem will be proved by extraction of Local Hidden Variables model for ρ. Namely, for (s_a, s_b)-settings it should reproduce the vector $P_{ij,kl}(\rho) = Tr(E_{ij}^A \otimes E_{kl}^B \rho)$ for all possible choices of POVM measurements $\{E_{ij}^A, E_{kl}^B\}$, as a convex combination of the extremal $\overline{B}$ vectors:

$$P_{ij,kl}(\rho) = \sum_{m,n} p_{m,n}(\{E_{ij}^A, E_{kl}^B\}, \rho) B_{ij,kl}^{m,n} \tag{3.16}$$

where $p_{m,n}(\cdot) \geq 0$. If there exists a quasi-symmetric extension of ρ, then $Tr(E_{ij}^A \otimes E_{kl}^B \rho) = Tr(E_{ij}^A \otimes E_{kl}^B \otimes \mathbb{I}) H_\rho$. Now, basing on the symmetry property of H_ρ, definition of the extreme $\overline{B}$ vectors (as stated in the section *Local realism and Bell inequalities*) and properties of POVMs, we can conclude:

$$P_{ij,kl}(\rho) = Tr E_{ij}^A \otimes E_{kl}^B \rho = \sum_{m,n} (Tr \mathbb{E}_m^A \otimes \mathbb{E}_n^B H_\rho) B_{ij,kl}^{m,n} \tag{3.17}$$

where $\mathbb{E}_m^A = E_{1,m_1}^A \otimes \ldots \otimes E_{s_a,m_{s_a}}^A$ (and similarly for $\mathbb{E}_n^B$). As $H_\rho$is a quasi-extension, then $p_{m,n}(\{E_{ij}^A, E_{kl}^B\}, \rho) = Tr \mathbb{E}_m^A \otimes \mathbb{E}_n^B H_\rho$ and we get LHV model. □

It means that for a bipartite state ρ having a symmetric extension $\tilde{\rho}$ shared between Alice and Bob, instead of measuring the state ρ, Alice and Bob can build $\tilde{\rho}$. They perform one measurement with one setting for each site from s_a sites hold by Alice and s_b sites belonging to Bob. Since the measurements commute, it can be perceived as one complex measurement with a single measurement which is equivalent to LHV.

Theorem 3.3.3 *[161] If ρ has a $(1,s_b)$ symmetric quasi-extension, then ρ does not violate Bell inequalities with any number of settings on Alice' site and s_b settings for Bob.*

Proof. The proof is based on the fact that it is not possible to violate any Bell inequality if one party performs measurement with only one setting. Therefore, in such a case it is not necessary to extend such a state. Here is the LHV model for a quasi-extension H_ρ on $\mathscr{H}_A \otimes \mathscr{H}_B^{\otimes s_b}$:

$$p_{m,n}(\{E_{ij}^A, E_{kl}^B\}, \rho) = \frac{\prod_{i'=1}^{s_a} (Tr E_{i'm_{i'}}^A \otimes E_n^B H_\rho)}{(Tr \mathbb{I}_A \otimes E_n^B H_\rho)^{s_a - 1}} \tag{3.18}$$

Each $p_{m,n}$ is non-negative since H_ρ is an entanglement witness. And as in the previous proof, we obtain correct LHV values $P_{ij,kl}(\rho)$ basing on the symmetry property of H_ρ, definition of B vectors and properties of POVMs.

In this scenario Bob is the party who performs the measurement on the extension applying only one setting for each of his site, thus, achieving LHV model for his measurement results.□

We will consider now more general monogamy relation [142] basing on the previous intuitions relating Bell inequalities with symmetric extendibility but adding also insights from no-signalling principle. Let us consider an experiment [142] with $n+1$ separated parties: one Alice and n Bobs $\{B^{(1)}, B^{(2)}, \ldots, B^{(n)}\}$. For this setup we consider a Bell inequality $\mathbf{B}(A, B^{(m)}) \leq R$ for the results of measurements performed by Alice and arbitrary chosen m-th Bob. The crucial assumption is that the number of settings at each Bob's site $B^{(m)}$ is n (equal to the number of Bobs) and the number of outcomes for Alice' and Bob's measurements is arbitrary. Then there holds the monogamy inequality for n pairs of observers, each pair having a single Bob and Alice:

$$\sum_{m=1}^{n} \mathbf{B}(A, B^{(m)}) \leq nR \tag{3.19}$$

This relation holds for all non-signalling theories, including quantum mechanical results even if for a chosen pair of Alice and Bob $B^{(m)}$, a single Bell inequality $\mathbf{B}(A, B^{(m)}) \leq R$ is violated.

Chapter 4

Symmetric extendibility of quantum states

The theory of symmetric extendible states being crucial for analysis of one-way distillability and security of quantum states has still many unsolved problems. In this chapter we introduce some new concepts related to classification of all symmetric extendible states and analyze mainly composite systems including also a symmetric extendible part [128]. The key conclusions are related to behavior of multiple pairs of quantum states including the fact that it is not possible to reduce maximal extendibility of quantum states even if one acts with one-way LOCC operations on multiple states [126, 128]. We underpin those results with geometric observations about structures of multi-party settings which posses substantial symmetric extendible components in their sub-spaces [128]. It is also discussed how separability of quantum states is related to symmetric extendibility and how efficiently a symmetric extension of a quantum state can be found by means of convex optimization methods and implemented in semi-definite programming.

The key results related to geometry of symmetric extendible set, symmetric extendibility of composite systems and behavior of this property under 1-LOCC operations were published in [126, 128].

4.1 Geometry of the symmetric extendible set

The concept of symmetric extendibility of a quantum state $\rho_{AB_1} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ can be generalized to a multipartite setup of its symmetric extension $\rho_{AB_1\ldots B_kB_{k+1}} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B^{\otimes k+1})$ ($k > 1$) with a permutational invariance on B-parties:

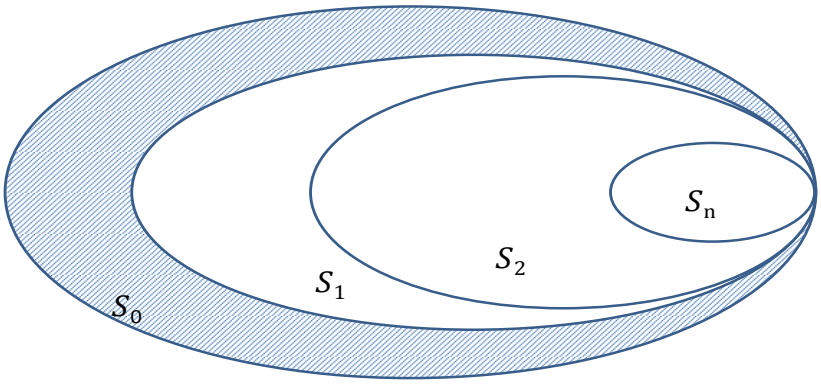

Fig. 4.1 The space of quantum states can be decomposed by the relation of k-extendibility. S_0 denotes the set of all non-extendible states (the blue area) whereas S_n the set of states having n-rank symmetric extensions.

Definition 4.1.1 *[128] A state $\rho_{AB_1} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is **k-extendible** if there exists such an extension $\rho_{AB_1\ldots B_kB_{k+1}} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B^{\otimes k+1})$ so that $\rho_{AB_i} = \rho_{AB_1}$ (for any $1 < i \leq k+1$) and $\rho_{AB_1\ldots B_kB_{k+1}} = \rho_{AB_{\pi(1)}\ldots B_{\pi(k)}B_{\pi(k+1)}}$ for any permutation π on B-parties. The state $\rho_{AB_1\ldots B_kB_{k+1}}$ is called **k-rank** symmetric extension of ρ_{AB_1}.*

By 0-extendible states we will denote those that are not symmetrically extendible at all. One could note that it might be useful to partition the set of all symmetric extendible states SE by relation of k-extendibility. If S_k denotes a convex set [126] of all states being k-extendible, then there holds the natural inclusion relation [Fig. 4.1] reflecting the fact that every 2-extendible state is also 1-extendible but the converse does not hold for all 1-extendible states etc.:

$$S_1 \supset S_2 \supset \ldots \supset S_k \tag{4.1}$$

Of a great importance is the fact that for a given $\rho_{AB} \in SE$ there may exist different k-rank symmetric extensions (i.e. extensions $\rho_{ABB_1\ldots B_k}$ invariant due to permutations on B-parties) so that the property is not unique and one could represent the set of appropriate symmetric extensions by means of equivalence classes given by the relation $\mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B) \ni \rho_{AB} \sim \rho \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B^{\otimes(k+1)})$ if and only if ρ is a k-rank symmetric extension of state ρ_{AB}.

As the trivial example note that for $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ at least the following are extensions of rank one: $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\rho = \frac{1}{2}(|000\rangle\langle 000| + |111\rangle\langle 111|)$.

For k-extendible states it might be useful to introduce an operator swapping $k+1$ particles:

$$P_\pi = \sum_{i_1 i_2 \ldots i_{k+1}} |i_1 i_2 \ldots i_{k+1}\rangle\langle \pi(i_1)\pi(i_2)\ldots\pi(i_{k+1})| \tag{4.2}$$

where swapping is performed for an arbitrary permutation π on B-part. Hence, there holds a general relation for k-extendibility that explicitly derives set S_k: $\forall_\pi\, id_A \otimes P_\pi \rho_{AB_1\ldots B_k B_{k+1}} id_A \otimes P_\pi^\dagger = \rho_{AB_1\ldots B_k B_{k+1}}$.

Example 4.1.2 *As a 1-extendible state we present* $\rho_{AB} = \frac{1}{3}|00\rangle\langle 00| + \frac{2}{3}|\Phi_+\rangle\langle\Phi_+|$ *that obviously possess 1-rank symmetric purification to W-state* $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$.

We could derive for this example a general form of n-extendible state $\Upsilon_{AB}(n)$ *that can be extended to W-like state:*

$$\Upsilon_{AB}(n) = \frac{n}{n+2}|00\rangle\langle 00| + \frac{2}{n+2}|\Phi_+\rangle\langle\Phi_+| \tag{4.3}$$

where $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

Interestingly, one can simply show that for e.g. *GHZ*-like n-partite states being a symmetric extension of $\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ there holds $\rho_{AB} = \lim_{n\to\infty}\rho_{AB}(n)$ that is in agreement with theorems [161] stating implicitly that ρ is separable if and only if it is ∞-extendible (where $\rho_{AB}(n)$ is derived from n-partite GHZ state by tracing out all parties beside A and B).

In the following, we present two different approaches to the problem of representation of symmetric extensions in the extended spaces. The first approach is widely used in previous papers (see [55, 56, 161]) on extendibility of quantum states. Every bipartite state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ where $\mathscr{H}_A = \mathbb{C}^m$ and $\mathscr{H}_B = \mathbb{C}^n$ can be represented in the basis of generators of group $SU(m)\otimes SU(n)$ as follows:

$$\begin{aligned} \rho_{AB} &= \gamma\sigma_A^0\otimes\sigma_B^0 + \sum_{i>0}\alpha_i\sigma_A^0\otimes\sigma_B^i + \\ &+ \sum_{j>0}\beta_j\sigma_A^j\otimes\sigma_B^0 + \sum_{i,j\neq 0}\zeta_{ij}\sigma_A^i\otimes\sigma_B^j \end{aligned} \tag{4.4}$$

where σ_B^i are basis elements of $SU(n)$ and respectively σ_A^i for $SU(m)$. The coefficients are real and elements of the basis satisfy relations: $Tr[\sigma_S^i\sigma_S^j] = \eta_S\delta_{ij}$ and $Tr[\sigma_S^i] = \delta_{1i}$ with

$S = \{A, B\}$. Therefore, one could derive a general representation of all 1-rank symmetric extensions which results also from the completeness of the aforementioned basis:

$$\begin{aligned} \rho_{AB_1B_2} &= \sum_{i,j} \alpha_{ij} \sigma_A^i \otimes \sigma_{B_1}^j \otimes \sigma_{B_2}^j + \\ &+ \sum_{ijk, j<k} \beta_{ijk} (\sigma_A^i \otimes \sigma_{B_1}^j \otimes \sigma_{B_2}^k + \sigma_A^i \otimes \sigma_{B_1}^k \otimes \sigma_{B_2}^j) \end{aligned} \tag{4.5}$$

and further, for general case of k-extendibility:

$$\begin{aligned} \rho_{AB_1\ldots B_{k+1}} = \sum_{i,j} \alpha_{ij} \sigma_A^i \otimes \sigma_{B_1}^j \otimes \ldots \otimes \sigma_{B_{k+1}}^j + \\ \sum_{i, i_1 < i_2 < \ldots < i_{k+1}} \sum_{\sigma} \beta_{i i_1 \ldots i_{k+1}} \sigma_A^i \otimes \sigma_{B_1}^{\sigma(i_1)} \otimes \ldots \otimes \sigma_{B_{k+1}}^{\sigma(i_{k+1})} \end{aligned} \tag{4.6}$$

The latter approach that we will utilize in this thesis is based on partitioning a space on which Bobs' states operate into a symmetric and antisymmetric subspace.

In the following, we will prove some lemmas about Schmidt decomposition of k-rank pure symmetric states that support more powerful theorem about properties of symmetric extendible states in due course.

Lemma 4.1.3 *[128] Let $\rho_{AB_1} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_{B_1})$ be symmetrically extendible to a k-rank pure extension $|\Psi_{AB_1\ldots B_{k+1}}\rangle \in \mathscr{H}_A \otimes \mathscr{H}_{B_1}^{\otimes k+1}$ ($k \geq 1$) then there exists a Schmidt decomposition:*

$$|\Psi_{AB_1\ldots B_{k+1}}\rangle = \sum_i \alpha_i |\phi_i^{AB_1}\rangle |\psi_i^{B_{2\ldots k+1}}\rangle \tag{4.7}$$

where $\{|\phi_i^{AB_1}\rangle\}, \{|\psi_i^{B_{2\ldots k+1}}\rangle\}$ are orthonormal sets and $|\psi_i^{B_{2\ldots k+1}}\rangle \in Sym^k(\mathscr{H}_{B_1}) \bigoplus Asym^k(\mathscr{H}_{B_1})$ (where Sym stands for the symmetric and Asym for the antisymmetric sub-space respectively).

Proof. Since $I_{AB_1} \otimes P_\pi |\Psi_{AB_1\ldots B_{k+1}}\rangle\langle\Psi_{AB_1\ldots B_{k+1}}| I_{AB_1} \otimes P_\pi^\dagger = |\Psi_{AB_1\ldots B_{k+1}}\rangle\langle\Psi_{AB_1\ldots B_{k+1}}|$ and $|\Psi_{AB_1\ldots B_{k+1}}\rangle$ is a pure symmetric extension, then:

$$\forall_\pi \; I_{AB_1} \otimes P_\pi |\Psi_{AB_1\ldots B_{k+1}}\rangle = \pm |\Psi_{AB_1\ldots B_{k+1}}\rangle$$

where P_π operates only on $B_2 \ldots B_{k+1}$ of the system, which implies $\sum_i \alpha_i |\phi_i^{AB_1}\rangle P_\pi |\psi_i^{B_{2\ldots k+1}}\rangle = \pm \sum_i \alpha_i |\phi_i^{AB_1}\rangle |\psi_i^{B_{2\ldots k+1}}\rangle$. However, since the state is a symmetric extension, the above Schmidt decomposition is invariant due to any permutation on B-part and $|\phi_i^{AB_1}\rangle$ indexes uniquely the $|\psi_i^{B_{2\ldots k+1}}\rangle$ states so P_π transforms $|\psi_i^{B_{2\ldots k+1}}\rangle$ onto itself. Therefore, the second multiplicands

of Schmidt decomposition represent either symmetric or antisymmetric orthonormal states. □

While the spectral conditions for 1-rank symmetric extensions were stated in [123], we derive general statements about spectral conditions for k-extendible states basing on the observation about decomposition of symmetric states:

Observation 4.1.4 *[128] Every pure normalized state $|\Psi\rangle \in Sym^{k+1} \bigoplus Asym^{k+1}(\mathscr{H}_{B_1})$ of k+1-partite system can be decomposed to the following Schmidt form:*

$$\forall_{1<l<k} |\Psi\rangle = \sum_i |\phi_i^{B_1 \ldots B_l}\rangle |\phi_i^{B_{l+1} \ldots B_{k+1}}\rangle$$

where the multiplicands form respectively symmetric or antisymmetric orthonormal sets.

Proof. One can conduct the proof similarly to (4.1.3). Since $\forall_\pi P_\pi |\Psi\rangle\langle\Psi| P_\pi = |\Psi\rangle\langle\Psi|$, then for all possible permutations the operation cannot change Schmidt decomposition of $\sum_i |\phi_i^{B_1 \ldots B_l}\rangle |\phi_i^{B_{l+1} \ldots B_{k+1}}\rangle$. Furthermore, due to assumed symmetry property of $|\Psi\rangle$, a state of any l-subsystem $B_1 \ldots B_l$ represented by the first multiplicand is permutationally invariant and the same is applied to the second multiplicand. □

This observation with application of lemma 4.1.3 can be effectively used to generate k-extendible states.

Observation 4.1.5 *Let ρ_{AB_1} be k-extendible to a pure symmetric state $|\Psi_{AB_1 \ldots B_{k+1}}\rangle$ then for ordered vectors of eigenvalues of ρ_{AB_1} and $\rho_{B_2 \ldots B_{k+1}}$ there holds*[1]*:*

$$\lambda^{\downarrow}(\rho_{AB_1}) = \lambda^{\downarrow}(\rho_{B_2 \ldots B_{k+1}}) \tag{4.8}$$

Proof. The proof is immediate applying Schmidt decomposition and results of (4.1.3). □

Symmetric extendibility of composite systems

In this section we explore symmetric extendibility of complex systems consisting of multiple pairs of quantum states. Thus, all following statements are vital for protocols acting on such quantum systems.

One may state a non-trivial question if it is feasible to achieve symmetric extendibility of a composition of quantum states when at least one of them is not-symmetric extendible. The result of this question is crucial both for quantum security applications and measuring quantum entanglement. The following lemma casts some light on this field:

[1] For a vector $\bar{x}$, we order its components in decreasing order, i.e.: $x_1 \geq x_2 \geq \ldots \geq x_n$ and then write $x^{\downarrow}$.

Lemma 4.1.6 *[128] If $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A^N \otimes \mathscr{H}_B^M)$ is not symmetrically extendible state then there does not exist any such a state $\rho_{A'B'} \in \mathscr{B}(\mathscr{H}_{A'}^K \otimes \mathscr{H}_{B'}^L)$ that $\rho_{AB} \otimes \rho_{A'B'}$ would be symmetrically extendible in respect to BB' subsystem.*

Proof. Conversely, let $\rho_{ABA'B'} = \rho_{AB} \otimes \rho_{A'B'}$ be a symmetrically extendible state acting on $\mathscr{B}(\mathscr{H}_A^N \otimes \mathscr{H}_B^M \otimes \mathscr{H}_{A'}^K \otimes \mathscr{H}_{B'}^L)$. Therefore, one notes that $\rho_{ABA'B'}$ after swapping to $\rho_{AA'BB'}$ can be represented by method (4.5) in an appropriate basis including generators of group $SU(N) \otimes SU(K) \otimes SU(M) \otimes SU(L)$ and further, can be extended to a 1-rank symmetric extension $\rho_{AA'BB'\widetilde{B}\widetilde{B'}}$ where we extend BB' part as follows:

$$\begin{aligned} \rho_{AA'BB'\widetilde{B}\widetilde{B'}} &= \sum_{ijkl} \alpha_{ijkl} T_{ijklkl} + \\ &+ \sum_{ijklmn} \beta_{ijklmn} (T_{ijklmn} + T_{ijmnkl}) \end{aligned} \tag{4.9}$$

with tensors $T_{ijklmn} = \sigma^i \otimes \sigma^j \otimes \sigma^k \otimes \sigma^l \otimes \sigma^m \otimes \sigma^n$. We derive the state $\rho_{AB\widetilde{B}}$ of system $AB\widetilde{B}$ tracing out that of $A'B'\widetilde{B'}$. For the fact that $Tr[\sigma^i \otimes \sigma^j \otimes \sigma^k] = Tr(\sigma^i)Tr(\sigma^j)Tr(\sigma^k)$ and $Tr[\sigma^i] = \delta_{0i}$ after tracing out only elements with $\sigma^0 = I$ remain, namely, one obtains:

$$\begin{aligned} \rho_{AB\widetilde{B}} &= \sum_{ik} \alpha_{i1k1} T_{i1k1k1} + \\ &+ \sum_{ikm} \beta_{i1k1m1} (T_{i1k1m1} + T_{i1m1k1}) \end{aligned} \tag{4.10}$$

Hence, $\rho_{AB\widetilde{B}}$ is 1-rank symmetric extension of ρ_{AB} that is in contradiction with the assumption that the latter is not symmetrically extendible. □

Corollary 4.1.7 *[128] If $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A^N \otimes \mathscr{H}_B^M)$ is at most k-extendible state then there does not exist any such a state $\rho_{A'B'} \in \mathscr{B}(\mathscr{H}_{A'}^K \otimes \mathscr{H}_{B'}^L)$ that $\rho_{AB} \otimes \rho_{A'B'}$ would be k+1- extendible in respect to BB' subsystem.*

Lemma 4.1.8 *[128] Assume that $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ is not symmetric extendible and there exists a local operation $\mathbb{F}$ acting on A-part such that $\sigma_{AB} = (\mathbb{F} \otimes id)\rho_{AB}(\mathbb{F}^\dagger \otimes id)/Tr[(\mathbb{F} \otimes id)\rho_{AB}(\mathbb{F}^\dagger \otimes id)]$ is a symmetric extendible state.*

Then for any local operations $\mathbb{A}$ and $\mathbb{B}$ acting on A and B part of the system:

$$\mathbb{A} = U \begin{pmatrix} \alpha_0 & & & \\ & \alpha_1 & & \\ & & \ddots & \\ & & & \alpha_i \end{pmatrix} U^\dagger \tag{4.11}$$

$$\Lambda(\rho_{AB}) = \frac{\mathbb{A}\otimes\mathbb{I}\rho_{AB}\mathbb{A}^\dagger\otimes\mathbb{I}}{Tr(\mathbb{A}\otimes\mathbb{I}\rho_{AB}\mathbb{A}^\dagger\otimes\mathbb{I})} \tag{4.12}$$

where for all i ($0 \leq i \leq \dim\mathscr{H}_A$*),* $0 < \alpha_i \leq 1$ *and U denotes an unitary operation (*$\mathbb{B}$ *has a corresponding structure), there exists a local operation* $\widetilde{\mathbb{F}}$ *such that* $\widetilde{\sigma}_{AB} = (\widetilde{\mathbb{F}}\otimes\mathbb{B}^{-1})\Lambda(\rho_{AB})(\widetilde{\mathbb{F}}^\dagger\otimes\mathbb{B}^{\dagger-1})/Tr[(\widetilde{\mathbb{F}}\otimes\mathbb{B}^{-1})\Lambda(\rho_{AB})(\widetilde{\mathbb{F}}^\dagger\otimes\mathbb{B}^{\dagger-1})]$ *is symmetric extendible and* $rank\mathbb{F} = rank\widetilde{\mathbb{F}}$.

Proof. To prove this lemma, it suffices to note that $\mathbb{A} = UDU^\dagger$ with a diagonal matrix D. Further, we observe that $\widetilde{\mathbb{F}} = \mathbb{F}\circ UD^{-1}U^\dagger$ where $D^{-1}D = id$. The latter is possible due to the condition that for all i there holds: $0 < \alpha_i \leq 1$ and we easily observe that $\mathbb{F} = \widetilde{\mathbb{F}}\circ\mathbb{A}$. This brings us to conclusion that $(\widetilde{\mathbb{F}}\otimes id)\Lambda(\rho_{AB})(\widetilde{\mathbb{F}}^\dagger\otimes id)$ is a symmetric extendible operator (after normalization becoming a physical state). If Bob acts in the process with a local operation $\mathbb{B}$, to ensure that the final state $\widetilde{\sigma}_{AB}$ is symmetric extendible, he has to act with a reversed local operation $\mathbb{B}^{-1}$ on his site (we ensured that the local operation $\mathbb{B}$ is also reversible). □

Remark. It casts some light on a fact that local operations on Alice's side actually do not change the amount of symmetric extendibility embedded in a state.

This lemma is of a great importance for private security and entanglement distillation studies, as we can always build a symmetric extension Γ_{ABE} of a state $\widetilde{\sigma}_{AB}$ which means that Eve potentially has a state $\rho_E = \rho_B = Tr_A\widetilde{\sigma}_{AB}$ and operates on such a space. To support this statement one can further derive the corollary about extendibility of any quantum state with a proposal of new extendible number of a quantum state:

Definition 4.1.9 *[128] For any* ρ_{AB}, $\eta_{SE}(\rho_{AB}) = \max_{\mathbb{F}} rank\mathbb{F}$ *is called the extendible number of a state* ρ_{AB} *where* $(\mathbb{F}\otimes id)\rho_{AB}(\mathbb{F}^\dagger\otimes id)$ *is a symmetric extendible operator and* $\mathbb{F}$ *is a local operation acting on A (*$\dim\mathbb{F}$ *states for the dimension of the image of* $\mathbb{F}$*).*

Corollary 4.1.10 *[128] Any state* $\rho_{AB}\in\mathscr{B}(\mathscr{H}_A\otimes\mathscr{H}_B)$ *with extendible number* η_{SE} *can be extended to a state* $\rho_{ABE}\in\mathscr{B}(\mathscr{H}_A\otimes\mathscr{H}_B\otimes\mathscr{H}_E)(\dim\mathscr{H}_\mathscr{B} = \dim\mathscr{H}_\mathscr{E})$ *for which there exists a filtering operation* $\mathbb{F}$ *on A so that* $(\mathbb{F}\otimes id)\rho_{ABE}(\mathbb{F}^\dagger\otimes id)$ *is invariant due to permutation of B and E.*

Naturally, there holds: if $\eta_{SE}(\rho_{AB}) = rank(\rho_A)$, then the state is symmetric extendible.

4.2 Set of symmetric extendible states is closed under 1-LOCC

We will present now a generalized version of a lemma [126] up to k-extendible maps stating that no matter what one-way operations Alice and Bob perform, the symmetric state shared between Alice and Bob will keep its symmetric extendibility.

Note that the set of extendible states is convex and compact which can be obviously obtained from the extendibility of any convex combination of extendible states. Subsequently, we show that the set is closed under local operations and one-way classical communication (1-LOCC) in the following lemma:

Lemma 4.2.1 *[126] The set $\mathscr{E}_{AB}$ of symmetrically extendible states is mapped under* 1*-LOCC for $\Lambda : \mathscr{B}(\mathscr{H}_{AB}) \to \mathscr{B}(\mathscr{H}_{\widetilde{A}\widetilde{B}})$ into the set of symmetrically extendible states $\mathscr{E}_{\widetilde{A}\widetilde{B}}$.*

Proof.

$$\begin{aligned}\rho_{AB} \subset \mathscr{E}_{AB} \Rightarrow \exists_{\rho_{ABB'}}\, \rho_{ABB'} = \rho_{AB'B} \wedge Tr_{B'}\rho_{ABB'} = \rho_{AB} \\ \Rightarrow Tr_{\widetilde{B}'}\Lambda(\rho_{ABB'}) = \rho_{\widetilde{A}\widetilde{B}} \subset \mathscr{E}_{\widetilde{A}\widetilde{B}}\end{aligned}$$

where

$$\begin{aligned}\Lambda(\rho_{ABB'}) \;=\; & \sum_{i,j=1}^{K,L} (I_2^{\widetilde{A}} \otimes W_{ji}^{B\to\widetilde{B}} \otimes W_{ji}^{B'\to\widetilde{B}'}) \\ & \times (V_i^{A\to\widetilde{A}} \otimes I_1^B \otimes I_1^{B'})\rho_{ABB'} \\ & \times (V_i^{A\to\widetilde{A}\dagger} \otimes I_1^B \otimes I_1^{B'}) \\ & \times (I_2^{\widetilde{A}} \otimes W_{ji}^{B\to\widetilde{B}\dagger} \otimes W_{ji}^{B'\to\widetilde{B}'\dagger})\end{aligned}$$

and operations acting on Bob's side are trace-preserving due to the necessity of non-breaking the property of extendibility. □

Namely, it is not possible to reduce the maximal extendibility [2] of a quantum state by means of 1-LOCC even if the operation is performed on multiple copies (cf. [126]). The following lemma indicates a fact that one cannot produce maximally k-extendible state from maximally n-extendible state (when $n > k$) by means of 1-LOCC $\Lambda_{\to}(\cdot)$ on any number of pairs and is a generalization of the above one:

[2] A maximal symmetric extension of a state ρ_{AB_1} stands for such a $\rho_{AB_1\ldots B_n}$ $(n > 1)$ so that there does not exist any symmetric extension $\rho_{AB_1\ldots B_k}$ where $k > n$.

Lemma 4.2.2 *[128] Let $\Lambda_{\rightarrow}$ be a 1-LOCC quantum operation (not necessarily trace-preserving):*

$$\Lambda_{\rightarrow}(\rho) = \sum_{ij}(I \otimes B_{ij})(A_i \otimes I)\rho(A_i \otimes I)^{\dagger}(I \otimes B_{ij})^{\dagger}$$

where $\sum_i A_i^{\dagger} A_i \leq I$ and $\sum_j B_{ij}^{\dagger} B_{ij} = I$ for all i since Bob cannot communicate the outcome of a probabilistic operation back to Alice. If ρ is maximally k-extendible state then $\Lambda_{\rightarrow}(\rho)$ is n-extendible and $n \geq k$.

One may raise further a very important question how to create the property of symmetric non-extendibility both in case of single states and collective systems using only local operations or additionally one-way communication that naturally will have implications for distillability and capacities of corresponding states and channels.

Lemma 4.2.3 *[128] Let $\rho_{AB} \in \mathscr{B}(\mathscr{H}_{AB})$ be a state possessing at most k-rank symmetric extension where $k < \infty$ then there does not exist any 1-LOCC protocol represented by $\Lambda_{A\rightarrow BC} : \mathscr{B}(\mathscr{H}_{ABC}) \rightarrow (\widetilde{\mathscr{H}_{ABC}})$ (not necessarily trace-preserving):*

$$\Lambda_{A\rightarrow BC}(\rho_{AB} \otimes \sigma_C) = \widetilde{\rho}_{ABC} \tag{4.13}$$

so that $\widetilde{\rho}_{ABC}$ is a symmetric extension of ρ_{AB} and $\sigma_C \in \mathscr{B}(\mathscr{H}_C)$ is an additional resource on Bob's side, i.e. $Tr_C \widetilde{\rho}_{ABC} = \rho_{AB}$.

Proof. Since ρ_{AB} is k-extendible, one can assume that its symmetric extension is realized to $\rho_{ABB_1 \ldots B_k}$ but $B_1 \ldots B_K$-part is possessed by Eve. Obviously no communication between Eve and Bob in such a scenario is allowed so that Bob cannot detect locally Eve and further, since the set of symmetric extendible states is closed under $1-LOCC$ operations [126] even if Alice and Bob had engaged one-way communication they cannot break symmetric extendability of ρ_{AB} and so cannot eliminate Eve if the symmetric extension had been realized.

Therefore, assuming that on the contrary $\Lambda_{A\rightarrow BC}$ enables creation of a symmetric extension:

$$\Lambda_{A\rightarrow BC} \otimes id_{B_1 \ldots B_k}(\rho_{ABB_1 \ldots B_k} \otimes \sigma_C) = \Omega \tag{4.14}$$

resulting state Ω would be k+1-symmetric extension of ρ_{AB} that contradicts the lemma's assumption about extendibility of this state and completes the proof. □

Remark. The aforementioned statements for n copies of symmetric extendible states holds as well in asymptotic regime for $n \rightarrow \infty$ due to the results of 4.1.6 that can be extended for an infinite case.

As a result of the above lemmas we can conclude that in general for creation of any symmetric extension one needs to engage two-way communication. However, it is interesting to note that LOCC operations with finite bidirectional communication can be simulated with stochastic local operations by including the expected communication bits in the shared randomness, and succeeding only when these shared random bits and the to-be-communicated bits coincide [120]. In this context, it might be a subject of further research to analyze how symmetric extendibility behaves under such stochastic operations and how easily the extensions can be created. These results will be vital for cryptographic applications.

4.3 The separability problem *vs.* symmetric extendibility

It is easy to note that a separable state $\rho_{AB} = \sum_i p_i \rho_i^A \otimes \sigma_i^B$ can be symmetrically extended to n Bobs $\rho_{AB}^n = \sum_i p_i \rho_i^A \otimes (\sigma_i^B)^{\otimes n}$ for any $n \geq 1$, i.e. any separable state is ∞-extendible. Thus, one can presume that there is a strong relation between the concept of symmetric extendibility and separability of a quantum state. It is based on the intuition that for the pair of quantum states $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ and $\sigma_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ where maximal extendibility of σ_{AB} is greater than that of ρ_{AB}, the state σ_{AB} is less entangled than ρ_{AB} (in terms of an appropriate entanglement measure, e.g. based on a distance to the separability states set).

Although it is easy to observe that every separable state is ∞-extendible, it is not obvious in the asymptotic regime if every ∞-extendible state is separable. The positive answer to this question for an asymptotic regime is a conclusion of the theorem proved by R. Werner, M. Fannes et al. in [67, 138] and is based on observations arose on the basis of the famous de Finetti theorem [45].

The classical de Finetti theorem states that for any symmetric probability distribution on m random variables $P_{X_1 X_2 \ldots X_m}$ which is infinitely exchangeable (i.e. it can be extended to n-partite distribution for all $n > m$ and is invariant under any permutation π of the random variables $P_{\pi(X_1)\pi(X_2)\ldots\pi(X_m)} = P_{X_1 X_2 \ldots X_m}$), one can find an expansion:

$$P_{X_1 X_2 \ldots X_m} = \int P_X^m d\mu(P_X) \tag{4.15}$$

where $d\mu$ is a measure on the set of probability distributions of one variable P_X.

We present now a quantum analogue of de Finetti theorem [160, 93, 133, 29, 72, 73]. A state $\rho_m \in \mathscr{B}(\mathscr{H}^{\otimes m})$ is *exchangeable* if it is invariant under any permutation π_m on m copies of $\mathscr{H}$ (i.e. $\pi_m \rho_m \pi_m^\dagger = \rho$) and for any n, there exists an extended state $\rho_{m+n} \in \mathscr{B}(\mathscr{H}^{\otimes m+n})$ which is permutationally invariant under π_{m+n} and: $\rho_m = Tr_n \rho_{m+n}$ (a partial trace over n additional systems).

Theorem 4.3.1 *(Quantum de Finetti Theorem) Let $\rho_m \in \mathscr{B}(\mathscr{H}^{\otimes m})$ be an exchangeable density matrix, then there exists a unique probability distribution $P(\rho)$ over the space S of quantum states on $\mathscr{H}$ so that:*

$$\rho_m = \int_S \rho^{\otimes m} P(\rho) d\mu(\rho) \tag{4.16}$$

where $P(\rho) \geq 0$ and the probability distribution is normalized $\int_S P(\rho) d\mu(\rho) = 1$ with $d\mu(\rho)$ being a suitable measure on the space S.

Exchangeable states ρ_m create a specific sequence of states $\{\rho_m\}_{m=1}^{+\infty}$ called sometimes *exchangeable de Finetti sequence*. We can easily observe that for the exchangeable states the above expansion results in a convex combination of product states, hence, we can proceed to the following strong statement:

Theorem 4.3.2 *[67, 138] A state $\rho_{AB_1} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_{B_1})$ is separable if and only if it has symmetric extensions $\rho_{AB_1\ldots B_n} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_{B_1} \otimes \ldots \otimes \mathscr{H}_{B_n})$ for any $n = 2, 3, \ldots, \infty$ (i.e. is ∞-extendible).*

Since every separable state is PPT (as discussed in previous sections, it is easy to observe that for every separable state $\Gamma_B(\rho_{AB}) = \sum_i p_i \rho_i^A \otimes (\sigma_i^B)^T = \sum_i p_i \rho_i^A \otimes \sigma_i^B = \rho_{AB}$), sometimes it might be useful to introduce the concept of PPT symmetric extensions [55, 56]. PPT symmetric extension of ρ_{AB_1} is such a symmetric extension $\rho_{AB_1\ldots B_{k+1}}$ that $\Gamma_{\{B_i\}}(\rho_{AB_1\ldots B_{k+1}}) \geq 0$, i.e. is positive under any partial transposition of any subset of its sub-systems.

In a natural way, one can build a hierarchy of symmetric extensions:

Theorem 4.3.3 *Let $\rho_{AB_1} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_{B_1})$ has a PPT symmetric extension $\rho_{AB_1\ldots B_n} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_{B_1}^{\otimes n})$ to n copies of B-subsystem. Then ρ_{AB_1} has a PPT symmetric extension to $(n-1)$ copies of B.*

Proof. For any state $\rho_{AB_1\ldots B_{n-1}} = Tr_B \rho_{AB_1\ldots B_n}$ (reduction over one of the copy of B), it is easy to observe that $\rho_{AB_1\ldots B_{n-1}}$ inherits the property of being a symmetric extension.

Now, we will consider PPT-property of that state, assume that $\rho_{AB_1\ldots B_{n-1}}$ is not PPT. Then there is such a subset S of the subsystems that $\Gamma_S(\rho_{AB_1\ldots B_{n-1}}) < 0$. Let $|\phi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_{B_1}^{\otimes n-1}$ be the eigenvector with a corresponding negative eigenvalue of this PPT problem and let $\{|i\rangle\}_{i=1}^{d_B}$ be the basis for the system B which was traced out from $\rho_{AB_1\ldots B_n}$. Since $\rho_{AB_1\ldots B_n}$ is PPT, then for all i: $\langle\phi|\langle i|\Gamma_S(\rho_{AB_1\ldots B_n})|i\rangle|\phi\rangle \geq 0$ and one gets immediately:

$$\sum_{i=1}^{d_B} \langle\phi|\langle i|\Gamma_S(\rho_{AB_1\ldots B_n})|i\rangle|\phi\rangle = \langle\phi|Tr_B[\Gamma_S(\rho_{AB_1\ldots B_n})]|\phi\rangle \geq 0 \tag{4.17}$$

which contradicts the assumption that $\Gamma_S(\rho_{AB_1\ldots B_{n-1}}) < 0$. □

4.4 Hierarchy of separability tests

Basing on the findings of the previous section we can build in a natural way a hierarchy of separability tests [55, 56] searching for PPT k-rank symmetric extensions as a PPT modification [Fig. 4.2] of the algorithm searching for k-rank symmetric extension for an input state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$.

Namely, the first test verifies if the state is PPT. If no, then the state ρ_{AB} is entangled. If yes, the state can be separable or entangled and it runs the second test to check if there exists PPT symmetric extension (in a standard algorithm that would be just search for 2-rank symmetric extension) $\rho_{ABB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B^{\otimes 2})$. If no, then the state naturally is entangled etc. The n-th test searches for PPT symmetric extension $\rho_{AB\ldots B} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B^{\otimes n})$. It is immediate to observe that each iteration is at least as powerful as all the preceding ones in detecting entanglement [55, 56].

As mentioned, one could just look for symmetric extensions of quantum states without verifying PPT-property of the extension, yet, as proved in [55, 56] introducing this condition gives better operational results due to the strength of this additional condition.

The hierarchy of separability tests can be implemented as a semi-definite program (SDP) by means of convex optimization methods. Moreover, it was also proved that the hierarchy is complete, i.e. for any entangled state ρ_{AB}, the algorithm finishes with a positive result at a finite n. We will use these methods further[3] to find a whole class of symmetric extensions of isotropic states and building new entanglement monotone basing on them after modification of this SDP.

However, in this context we cannot forget that solving separability problem is of NP-hard class (i.e. it is at least as difficult as solving any non-deterministic polynomial-time problem - NP - in terms of computational complexity) which is also the case of the aforementioned algorithm, scaling polynomially with the dimensions of the subsystems but finishing at unknown step n.

4.5 Convex optimization for searching symmetric extensions

Searching for symmetric extensions of a given state is actually a particular type of a convex optimization problem, that can be implemented in semi-definite programming (SDP). A typical SDP is one of the convex optimization [22] form subjected to a linear matrix inequality:

[3] Vide sec. Symmetric extendibility of isotropic states.

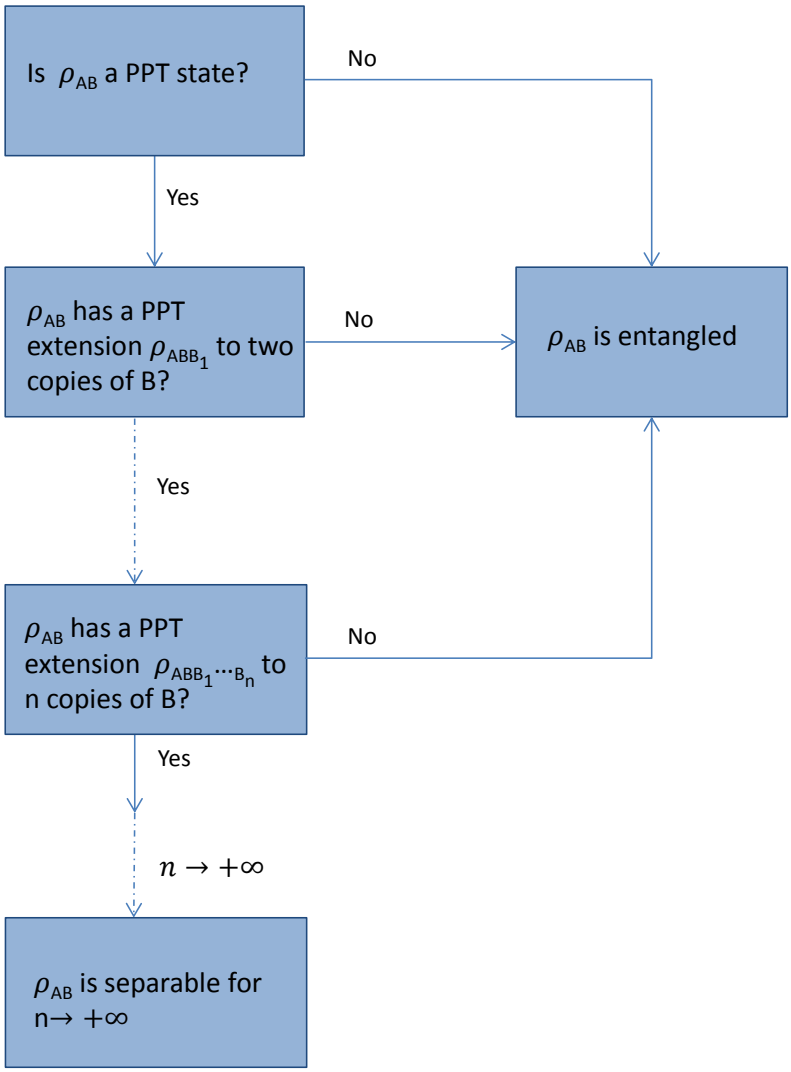

Fig. 4.2 The hierarchy of separability tests algorithm looking at each step for PPT symmetric extension of n-rank for a state ρ_{AB}. If a state fails a particular step, it is entangled.

$$\begin{aligned} &\textit{minimize } c^T\mathbf{x} \\ &\textit{subject to } F(\mathbf{x}) \geq 0, \end{aligned} \tag{4.18}$$

where c is a given vector, $\mathbf{x} = (x_1, \ldots, x_n)$ and $c^T\mathbf{x}$ creates the objective convex function. The positive semi-definite matrix $F(\mathbf{x}) = F_0 + \sum_i x_i F_i$ (F_i are hermitian matrices) put constraints on the optimization problem. The minimization is performed over vectors $\mathbf{x}$ and the set of solutions of the problem is convex.

We will show now how to construct [55, 56] SDP for symmetric extensions. As discussed previously[4], any bipartite state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ can be represented in the basis $\{\sigma_i^A \otimes \sigma_j^B\}$ as $\rho_{AB} = \sum_{ij} \rho_{ij} \sigma_i^A \otimes \sigma_j^B$ where $\rho_{ij} = \alpha_A^{-1}\alpha_B^{-1} Tr[\rho_{AB}\sigma_i^A \otimes \sigma_j^B]$ ($Tr[\sigma_i^X \sigma_j^X] = \alpha_X \delta_{ij}$ for $X = \{A, B\}$). The algorithm performs search for an extension $\rho_{ABB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_B)$:

$$\rho_{ABB} = \sum_{ijk,,i<k} \rho_{ijk}\{\sigma_i^B \otimes \sigma_j^A \otimes \sigma_k^B + \sigma_k^B \otimes \sigma_j^A \otimes \sigma_i^B\} + \sum_{kj} \rho_{kjk} \sigma_k^A \otimes \sigma_j^B \otimes \sigma_k^A \tag{4.19}$$

To ensure that ρ_{ABB} is a symmetric extension of ρ_{AB}, we require additionally: $Tr_B \rho_{ABB} = \rho_{AB}$. Due to the relations between $\{\sigma_i\}$ operators we get $\rho_{ij1} = \rho_{ij}$. Now the linear constraints for the optimization problem comes from the requirement that the partial transposes and the symmetric extension are positive semi-definite. Let us define:

$$\begin{aligned} F_0 &= \sum_j \rho_{1j} \sigma_1^B \otimes \sigma_j^A \otimes \sigma_1^B + \sum_{i=2,j=2} \rho_{ij}(\sigma_i^B \otimes \sigma_j^A \otimes \sigma_1^B + \sigma_1^B \otimes \sigma_j^A \otimes \sigma_i^B) \\ F_{iji} &= \sigma_i^B \otimes \sigma_j^A \otimes \sigma_i^B \; i \geq 2, \\ F_{ijk} &= (\sigma_i^B \otimes \sigma_j^A \otimes \sigma_k^B + \sigma_k^B \otimes \sigma_j^A \otimes \sigma_i^B) \; k > i \geq 2, \end{aligned} \tag{4.20}$$

and we can re-write the linear constraint $\rho_{ABB} \geq 0$ of our SDP (we put all the indexes $\{ijk\}$ under J-index) in a more compact form:

$$F(\mathbf{x}) = F_0 + \sum_J x_J F_J \geq 0 \tag{4.21}$$

and the coefficients ρ_{ijk} build the vector $\mathbf{x}$.

Since the matrix ρ_{ABB} is a symmetric extension over B-parties, we require that $\Gamma_A(\rho_{ABB}) \geq 0$ and $\Gamma_B(\rho_{ABB}) \geq 0$ (PPT conditions), and in conclusion we can put the final condition for

[4] Vide sec. Geometry of symmetric extendible set.

SDP:

$$M = \rho_{ABB} \oplus \Gamma_A(\rho_{ABB}) \oplus \Gamma_B(\rho_{ABB}) \geq 0. \tag{4.22}$$

and we actually resolve *a feasibility problem* $M \geq 0$ (4.22) with an objective function equal zero (i.e. $c = 0$ and $c^T \mathbf{x} = 0$) [22, 55, 56] that is a modification of standard convex optimization problem.

For higher levels of the hierarchy, the algorithm generates the symmetric matrices F_J of higher dimension and then builds the block diagonal matrix M for which the optimization is performed so it searches for an appropriate k-rank symmetric extension and verify if it has PPT-property.

Example 4.5.1 *As a special example of application of these observations we use below bipartite state ρ_{AB} that is extendible for $F \leq \frac{1}{2}$, moreover, notice that in this range the state may be quite strongly entangled [126]:*

$$\rho_{AB} = \frac{F}{3} P_+ + \frac{1-F}{3}(|01\rangle\langle 01| + |20\rangle\langle 20| + |21\rangle\langle 21|) \tag{4.23}$$

Note that filtering on Bob's side the state ρ_{AB}, and in general any such a state, does not change the extendibility, what may be simply proved. Applying filtering with $W = diag\left[1, \frac{1}{\sqrt{F}}, \frac{1}{\sqrt{2-F}}\right]$ we get a state $\widetilde{\rho}_{AB}$ and a maximally mixed state $\widetilde{\rho_A}$ on Alice's side:

$$\widetilde{\rho}_{AB} = \frac{W \otimes I \rho_{AB} W^\dagger \otimes I}{Tr\{W \otimes I \rho_{AB} W^\dagger \otimes I\}}, \; \widetilde{\rho}_A = \frac{I}{3} \tag{4.24}$$

$$\widetilde{\rho}_{AB} = \begin{pmatrix} \frac{F}{3} & 0 & 0 & 0 & \frac{\sqrt{F}}{3} & 0 & 0 & 0 & \frac{F}{3\sqrt{2-F}} \\ 0 & \frac{1-F}{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{\sqrt{F}}{3} & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & \frac{\sqrt{F}}{3\sqrt{2-F}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1-F}{3(2-F)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1-F}{3(2-F)} & 0 \\ \frac{F}{3\sqrt{2-F}} & 0 & 0 & 0 & \frac{\sqrt{F}}{3\sqrt{2-F}} & 0 & 0 & 0 & \frac{F}{3(2-F)} \end{pmatrix} \tag{4.25}$$

For any of the above states, the extension can be found by means of linear optimisation with help of SEDUMI module [157]. We have found the extension of ρ_{AB} very easily, in fact

we have for $F \leq \frac{1}{2}$ the following spectral decomposition of the extension ρ_{BAB}:

$$\begin{cases} |\varphi_0\rangle = |020\rangle \text{ and } \lambda_0 = \frac{1-F}{6} \\ |\varphi_1\rangle = |001\rangle + |100\rangle + |111\rangle + |122\rangle + |221\rangle \text{ and } \lambda_1 = \frac{F}{3} \\ |\varphi_2\rangle = |021\rangle \text{ and } \lambda_2 = \frac{1-2F}{6} \\ |\varphi_3\rangle = |101\rangle \text{ and } \lambda_3 = \frac{1-2F}{3} \\ |\varphi_4\rangle = |120\rangle \text{ and } \lambda_4 = \frac{1-F}{6} \\ |\varphi_5\rangle = |121\rangle \text{ and } \lambda_5 = \frac{1-2F}{6} \end{cases} \tag{4.26}$$

where generally eigenvalues have to fulfil the following conditions so that after tracing out Brigitte we obtain ρ_{AB}:

$$\begin{cases} \lambda_0 + \lambda_4 = \frac{1-F}{3} \\ \lambda_2 + \lambda_5 = \frac{1-2F}{3} \end{cases} \tag{4.27}$$

According to these constructions, we may find another state ρ_{BAB} that is nearest (in the set of states constructed on the above eigenvectors) to singlet in a sense of maximizing fidelity ($\mathscr{F} = \langle\Psi_+|\rho_{AB}|\Psi_+\rangle$) of its local reduction ρ_{AB}:

$$\begin{cases} \rho_{BAB} = \frac{1}{5}|\varphi_1\rangle\langle\varphi_1| \\ \rho_{AB} = \frac{3}{5}P_+ + \frac{1}{5}|01\rangle\langle 01| + \frac{1}{5}|21\rangle\langle 21| \end{cases} \tag{4.28}$$

As a generalization of such states, we construct states extreme in the above sense for arbitrary dimension:

$$\Upsilon = \frac{d}{2d-1}P_+ + \frac{1}{2d-1}\sum_{i=1}^{d-1}|i\,0\rangle\langle i\,0| \tag{4.29}$$

We state now the following question as a natural conclusion of above analysis:
Question: What is the maximal possible value of fidelity of ρ that we may obtain from states for which $Q_\rightarrow = 0$ (a zero one-way quantum channel capacity[5])?

[5] Vide chap. Quantum Channels

Chapter 5

Isotropic states and their symmetric extensions

In this chapter we present analytically derived symmetric extensions of isotropic states which are important for further definition of new entanglement measures based on symmetric extendibility, due to the fact that every state can be transformed under $U \otimes U^*$ - *twirling* into an isotropic state and for maximally entangled singlets, the nearest symmetric extendible states from the set of symmetric extendible states set are the isotropic states [126]. Furthermore, we define a new entropic measure [126] based on a normalized relative entropy distance to the set of symmetric extendible states in analogy to the relative entropy of entanglement.

5.1 Isotropic states

In this section we present a unique class of quantum states - Werner states and isotropic states. R. Werner [168] analyzed bipartite quantum states $\rho \in \mathscr{B}(\mathscr{H} \otimes \mathscr{H})$ which do not changes their structure if their subsystems are exposed to the same local unitary operations:

$$\rho = U \otimes U \rho U^\dagger \otimes U^\dagger \tag{5.1}$$

The structure of the Werner states is as follows:

$$\rho_W(\alpha) = \frac{I + \alpha P}{d^2 + \alpha d} \tag{5.2}$$

where $P = \sum_{i,j=0}^{d-1} |ij\rangle\langle ji|$. The state is separable for $1 \geq \alpha \geq -\frac{1}{d}$ (i.e. it is separable if and only if it is PPT), NPT for $-\frac{1}{d} > \alpha \geq 1$ and two-way 1-distillable[1] for $-\frac{1}{2} > \alpha \geq -1$. For a

[1] Vide sec. Distilling quantum entanglement.

bipartite qubit state $\rho_W \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, we get [135]:

$$\rho_W = \alpha |\Psi_-\rangle\langle\Psi_-| + (1-\alpha)\frac{I}{4} \tag{5.3}$$

where $-\frac{1}{3} \leq \alpha \leq 1$ and $|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

The states are so specific due to the following property. Namely, any state ρ, subjected to random bilocal unitary transformations of the form $U \otimes U$, becomes a Werner state. The random unitary operations are called *twirling operations*:

$$\rho_W = \int dU U \otimes U \rho U^\dagger \otimes U^\dagger \tag{5.4}$$

The second class of states considered in this thesis creates so-called isotropic states [139]. These are the only states invariant under $U \otimes U^*$ transformation. We can derive them as a higher-dimensional generalization of $\rho_W \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, interchanging $|\Psi_-\rangle$ with $|\Psi_+\rangle$ [101]:

$$\rho(\alpha, d) = \alpha P_+ + (1-\alpha)\frac{I}{d^2} \tag{5.5}$$

where $-\frac{1}{d^2-1} \leq \alpha \leq 1$. If we are interested in the question of how much singlet fraction $F = TrP_+\rho$ is embedded in this state, we get the following broadly used form:

$$\rho(d, F) = \frac{d^2}{d^2-1}[(1-F)\frac{I}{d^2} + (F - \frac{1}{d^2})P_+] \tag{5.6}$$

The state is a mixture of a singlet state $P_+ = |\Psi_+\rangle\langle\Psi_+|$ and a pure noise with a representation $\rho_{noise} = I/d^2$. It is the only state invariant under $U \otimes U^*$ transformation. The state is NPT if $F > \frac{1}{d}$ and the parameter F is invariant under $U \otimes U^*$ twirling.

Finally, in analogy to $U \otimes U$ twirling, any state exposed to $U \otimes U^*$ twirling becomes an isotropic state ρ_{iso}:

$$\rho_{iso} = \int dU U \otimes U^* \rho U^\dagger \otimes U^{*\dagger}. \tag{5.7}$$

5.2 Symmetric extendibility of isotropic states

Using techniques [62], we show [126] that the nearest state to a singlet in an arbitrary dimension is a state $\rho(d, F_{max})$ from a subset of isotropic states $\rho(d, F)$ [101] with fidelity $F \leq F_{max}$ for which those are symmetrically extendible:

$$F_{max} = \frac{d+1}{2d} \tag{5.8}$$

$$\rho(d,F) = \frac{d^2}{d^2-1}[(1-F)\frac{I}{d^2} + (F - \frac{1}{d^2})P_+] \tag{5.9}$$

Indeed, following [62] one needs to analyze operators from a six dimensional non-commutative $\mathbf{C}^*$-algebra that are $\overline{U} \otimes U \otimes U$-invariant and $V_{(23)}$-invariant. Such operators S will be represented as a linear combination of the basis elements of the algebra: $B = \{S_+, S_-, S_0, S_1, S_2, S_3\}$ where for the trace condition one obtains [62] conditions for factors of the combination: $s_2 = s_3 = 0$ and, further, from positivity: $s_0 = 1 - s_+ - s_-$.

$$S = s_+ S_+ + s_- S_- + s_0 S_0 + s_1 S_1 \tag{5.10}$$

The matter of interest is now the tetrahedron in three-dimensional euclidian space of parameters (s_+, s_-, s_1) confined by the hyperplanes [62]: $\{h_1', h_2', h_3', h_4'\}$ in which exists the state Ω_{ABE} giving the searched symmetric extendible reduction ρ_{AB}. For maximizing the distance of the unknown state ρ_{AB} to singlet it suffices [126] to find the maximization over fidelity $\widetilde{F}$ between the symmetric extension represented as Ω_{ABE} and virtually extended unnormalized operator $\rho_{ABB'} = P_+ \otimes I$ as $\widetilde{F}_{max} = Tr[P_+ \otimes I\, \Omega_{ABE}] = Tr[P_+\, \rho_{AB}] = F_{max}$:

$$\begin{cases} F_+ = Tr[(P_+ \otimes I)\, S_+]/Tr[S_+^2] = 0 \\ F_- = Tr[(P_+ \otimes I)\, S_-] = 0 \\ F_0 = Tr[(P_+ \otimes I)\, S_0]/Tr[S_0^2] = d/2d \\ F_1 = Tr[(P_+ \otimes I)\, S_1]/Tr[S_1^2] = 1/2d \end{cases} \tag{5.11}$$

$$\begin{cases} \widetilde{F} = F_0 + \overrightarrow{s} \circ \overrightarrow{f} \\ \widetilde{F}_{max} = \max_{\overrightarrow{s} \in \Delta} \widetilde{F} \end{cases} \tag{5.12}$$

where Δ denotes the tetrahedron bounded by mentioned hyperplanes, $\overrightarrow{f} = [F_+ - F_0, F_- - F_0, F_1]$ and $\overrightarrow{s} = [s_+, s_-, s_0]$. Normalization of parameters F_i inherits from the commutation relations [62] between operators S_i. Maximization results in $\overrightarrow{s} = [0,0,1]$ that relates to the found aforementioned isotropic states $\rho_{AB} = \rho(d, F_{max})$. The explicit form of the tripartite symmetric extension of isotropic states $\rho(d, F_{max})$ in the border of extendibility is [126]:

$$\Omega_{ABE} = \frac{1}{2d}(S_0 + S_1) \tag{5.13}$$

where [62]:

$$\begin{cases} S_0 = \frac{1}{d^2-1}(d(X + VXV) - (XV + VX)) \\ S_1 = \frac{1}{d^2-1}(d(XV + VX) - (X + VXV)) \end{cases} \tag{5.14}$$

for

$$|\Phi\rangle = \sum_i |ii\rangle \ , \ X = |\Phi\rangle\langle\Phi| \otimes I \ , \ V = V_{(23)} = \sum_{ijk} |ijk\rangle\langle ikj|. \tag{5.15}$$

It is important to notice that the same results can be obtained numerically by means of linear programming methods that we have utilized to find the broad class of symmetric extendible states.

5.3 Relative entropy and distance to the set of symmetric extendible states

Distance measures are introduced to quantify generally distances between quantum states or between a state and a specific subset of quantum states but they also bring more operational application related to statistical distinguishability of quantum states. In particular, a fundamental issue relates to the distance of a given quantum state $\rho \in \mathscr{B}(\mathscr{H})$ to the nearest (in a sense of a chosen metric) separable state $\sigma \in \mathscr{B}(\mathscr{H})$ from a set S of separable states in this space $S \subset \mathscr{B}(\mathscr{H})$, which is compact and convex.

This distance relates directly to the strength of entanglement shared between subsystems of a system in a state ρ and we will find out in the following chapter that distance measures are good candidates to quantify quantum entanglement. This concept is based on the intuition that the closer to separable states a multipartite quantum state is localized, the less entanglement it stores and for any separable state, its entanglement $E(\sigma) = 0$ [2]. On the other hand, we predict that the states, which are close to each other, will generate similar statistical results for the measurements performed on them.

There are many different proposals of distance measures introduced in quantum information theory but we present below the most popular. For a given set of separable states $S \subset \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$, the distance of a state $\rho \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ to the nearest separable state can be assessed by [13]:

Bures distance $D_{Bures}(\rho) = min_{\sigma \in S} D_{Bures}(\rho, \sigma)$, where $D^2_{Bures}(\rho, \sigma) = 2[1 - \sqrt{F(\rho, \sigma)}]$ with fidelity defined as: $F(\rho, \sigma) = [Tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$.

Hilbert-Schmidt distance $D_{HS}(\rho) = min_{\sigma \in S} D_{HS}(\rho, \sigma)$, where $D_{HS}(\rho, \sigma) = \sqrt{Tr(\rho - \sigma)^2}$.

Trace distance $D_{Tr}(\rho) = min_{\sigma \in S} D_{Tr}(\rho, \sigma)$, where $D_{Tr}(\rho, \sigma) = \frac{1}{2} Tr|\rho - \sigma|$.

[2] Vide sec. Entanglement measures.

The trace distance between ρ and σ is actually the variational distance of the probability distributions generated by POVMs on these states:

$$D_{Tr}(\rho,\sigma) = \max_V D_{Tr}(P,S) \tag{5.16}$$

where maximization is over all POVMs V on ρ and σ (which generates the probability distributions P and S). As an application, one could try to decide if an unknown state equals σ if no prior knowledge is given and only POVMs could be performed. As in case of other measures, it is interesting to note that the trace distance is monotonic under CPTP maps Λ: $D_{Tr}(\Lambda(\rho),\Lambda(\sigma)) \leq D_{Tr}(\rho,\sigma)$ and reflects also the strong convexity: $D_{Tr}(\sum_i p_i\rho_i, \sum_i q_i\sigma_i) \leq D_{Tr}(P,S) + \sum_i p_i D_{Tr}(\rho_i,\sigma_i)$.

Another very popular measure, directly related with the Bures distance, is *the fidelity* quantifying an overlap of two quantum states. For pure states $|\Psi\rangle$ and $|\Phi\rangle$, the fidelity equals the probability of passing the test by $|\Psi\rangle$ whether it is $|\Phi\rangle$, and it reads:

$$F(P_{|\Psi\rangle}, P_{|\Phi\rangle}) = |\langle\Psi|\Phi\rangle|^2 \tag{5.17}$$

In general, for mixed states ρ and σ:

$$F(\rho,\sigma) = [Tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2 \tag{5.18}$$

and if one of the states is pure, then $F(|\psi\rangle\langle\psi|,\sigma) = Tr(|\psi\rangle\langle\psi|\sigma)$. Fidelity is also monotonic under action of CPTP channels Λ:

$$F(\Lambda(\rho),\Lambda(\sigma)) \geq F(\rho,\sigma) \tag{5.19}$$

and moreover, there holds a very interesting property for pure extensions $|\psi\rangle$ and $|\phi\rangle$ of mixed states ρ and σ respectively:

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\phi\rangle} |\langle\psi|\phi\rangle|^2 \tag{5.20}$$

In this context, the next quantity - the relative entropy of entanglement is not a distance (as it is not symmetric, i.e. $R(\rho\|\sigma) \neq R(\sigma\|\rho)$), however, it is also used to quantify entanglement of quantum states since it can be used to distinguish a given state ρ from the nearest separable state:

$$D_R(\rho) = min_{\sigma\in S} R(\rho\|\sigma) \tag{5.21}$$

It is interesting to notice the relation between relative entropy and the trace distance [13]:

$$R(\rho\|\sigma) \geq 2D_{Tr}(\rho,\sigma)^2 \tag{5.22}$$

and as we will see further, the relative entropy of entanglement is an efficient upper bound on distillable entanglement which is one of the key reason for such an interest in this matter. Basing on these insights and monogamy of quantum entanglement, we introduced and developed in [126] the concept of a distance of a quantum state to the nearest symmetric extendible state which is also a new upper bound on one-way distillable entanglement (vide sec. 'New upper bounds on one-way distillable entanglement'). As we will find out, in similarity to a standard case of separable state where $D_R(\rho) = 0$ if the state ρ is separable, we propose an entropic measure which gives a zero value for states being symmetrically extendible [126]. This is a crucial for all states being a subject of 1-LOCC distillation and cryptographic protocols.

We define the measure of this distance to the set of symmetric extendible states based on the definition of relative entropy:

Definition 5.3.1 *[126] Assume that a convex set $\mathscr{E}_{AB}$ is a set of extendible states, i.e.*

$$\mathscr{E}_{AB} = \{\sigma_{AB} : \exists_{\Psi_{ABB'C}}\ \sigma_{AB} = \sigma_{AB'} = \\ = Tr_{CB}[|\Psi_{ABB'C}\rangle\langle\Psi_{ABB'C}|]\}$$

Then the distance of a state ρ_{AB} on $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$ with $\dim \mathscr{H}_A = d_A$ and $\dim \mathscr{H}_B = d_B$ to the set of extendible states $\mathscr{E}_{AB}$ of $d \otimes d$ type where $d = \max[d_A, d_B]$ is defined by

$$R_{\mathscr{E}_{AB}}(\rho_{AB}) = \delta_{AB} \inf_{\sigma_{AB}\in\mathscr{E}} R(\widetilde{\rho}_{AB}\|\sigma_{AB}) \tag{5.23}$$

where $\forall_{\rho,\sigma}\ R(\rho\|\sigma) = Tr[\rho\log\rho - \rho\log\sigma]$ and $\delta = -\frac{\log d}{\log\frac{(d+1)}{2d}}$ with $d = \max[d_A, d_B]$ due to normalization of this function on maximally entangled states. In the formula (5.23) $\widetilde{\rho}_{AB}$ is taken as a state of $d \otimes d$ type (after embedding ρ_{AB} into $d \otimes d$ space).

Normalization of this symmetric extendible relative entropy is derived in such a way that for maximally entangled states: $R_{\mathscr{E}_{AB}}(|\Psi_+\rangle\langle\Psi_+|) = \log d$ and for all symmetric extendible states σ, $R_{\mathscr{E}_{AB}}(\sigma) = 0$. It becomes clear in next chapter that by such a formulation we can derive new upper bounds on one-way distillable entanglement. Such a formula would be not possible without a derivation of exact symmetric extensions of isotropic states and their relation to singlet states.

5.4 Symmetric extendibility of bipartite qubit states

Every bipartite state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ (where $\dim \mathscr{H}_A = m$ and $\dim \mathscr{H}_B = n$) can be represented in the so-called Fano form [66], decomposed in the product group basis $SU(m) \otimes SU(n)$ as:

$$\rho_{AB} = \frac{1}{mn}(\mathbb{I}_A \otimes \mathbb{I}_B + \sum_{i=1}^{m^2-1} \beta_i^A \sigma_i \otimes \mathbb{I}_B + \sum_{j=1}^{n^2-1} \beta_j^B \mathbb{I}_A \otimes \sigma_j + \sum_{i=1}^{m^2-1} \sum_{j=1}^{n^2-1} \gamma_{ij}^{AB} \sigma_i \otimes \sigma_j) \tag{5.24}$$

where $\overline{\beta}^A$ and $\overline{\beta}^B$ can be interpreted as real Bloch vectors of the reduced states $\rho_A = Tr_B \rho_{AB}$ and $\rho_B = Tr_A \rho_{AB}$ respectively. Further, $[\gamma_{ij}^{AB}]$ can be represented as a real $(m^2-1) \times (n^2-1)$ matrix of correlation parameters γ_{ij}^{AB}.

It is interesting to analyze this structure in case of bipartite qubit systems in a state $\rho_{AB} \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. Then the Fano representation is:

$$\rho_{AB} = \frac{1}{4}(\mathbb{I}_A \otimes \mathbb{I}_B + \sum_{i=1}^{3} \beta_i^A \sigma_i \otimes \mathbb{I}_B + \sum_{j=1}^{3} \beta_j^B \mathbb{I}_A \otimes \sigma_j + \sum_{i,j=1}^{3} \beta_{ij}^{AB} \sigma_j \otimes \sigma_j) \tag{5.25}$$

where $\{\sigma_1, \sigma_2, \sigma_3\}$ denote the Pauli matrices and the real parameters are (we project the state ρ_{AB} onto a basis vectors of a Hilbert-Schmidt space $\mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$):

$$\beta_i^A = Tr(\rho_{AB} \sigma_i \otimes \mathbb{I}_B) \tag{5.26}$$

$$\beta_j^B = Tr(\rho_{AB} \mathbb{I}_A \otimes \sigma_j) \tag{5.27}$$

$$\beta_{ij}^{AB} = Tr(\rho_{AB} \sigma_i \otimes \sigma_j) \tag{5.28}$$

$$\tag{5.29}$$

Furthermore, any two-qubit state having the reduced density matrices $\rho_A = \rho_B = \mathbb{I}/2$ can be transformed to the Bell diagonal representation by means of local unitary operations U_A and U_B acting on the qubits A and B which diagonalize the correlation matrix $[\beta_{ij}^{AB}]$, i.e.:

$$\rho_{AB} = \sum_{ij=0}^{1} \alpha_{ij} |\Phi_{ij}\rangle\langle\Phi_{ij}| \tag{5.30}$$

with the Bell states $|\Phi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0i\rangle + (-1)^i |1 \oplus j\rangle)$ and the corresponding eigenvalues:

$$\alpha_{ij} = \frac{1}{4}(1 + (-1)^i x - (-1)^{i+j} y + (-1)^j z) \tag{5.31}$$

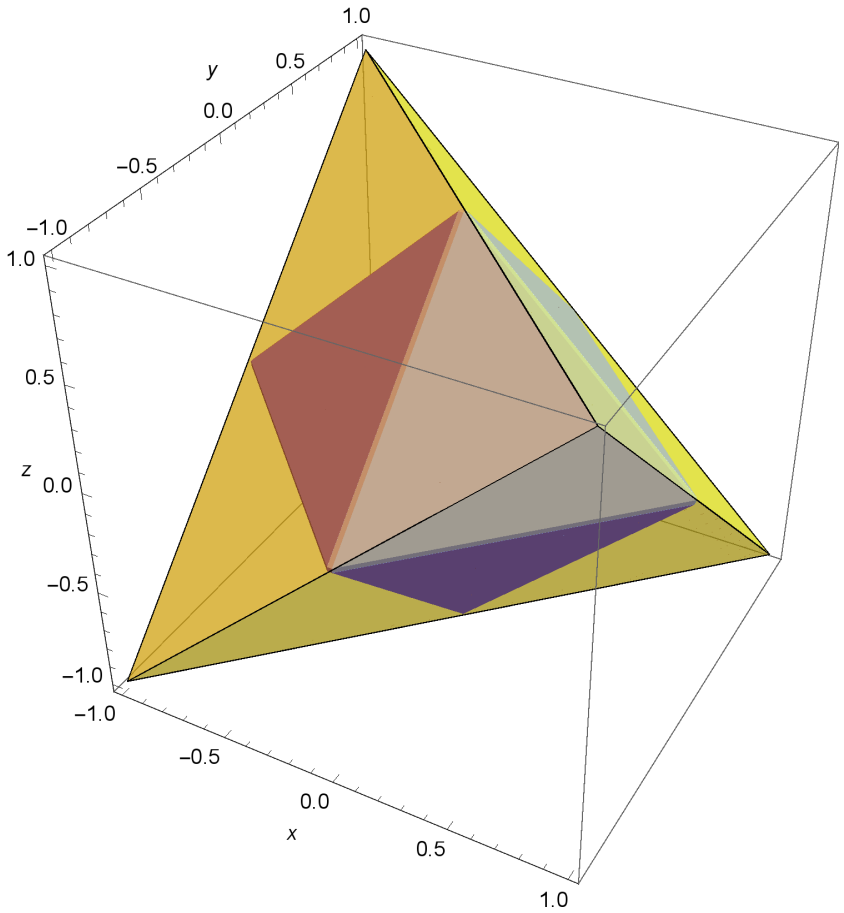

Fig. 5.1 All Bell diagonal two-qubit states are represented by the tetrahedron with the extreme points (vertices of the tetrahedron) $\{(1,1,-1),(-1,-1,-1),(1,-1,1),(-1,1,1)\}$ representing the Bell states. The octahedron represents all separable two-qubit states diagonal in the Bell basis.

Therefore, such states can be represented by means of vectors $\tau = [x,y,z]$ [Fig. 5.1] (the eigenvalues α_{ij} are non-negative and the density matrix is normalized).

It is now an open question what are the general conditions for symmetric extendibility of general bipartite states although the conditions are known for all two-qubit states. This condition is a subject of the following theorem proved recently in [112]:

Theorem 5.4.1 *A two qubit state ρ_{AB} is symmetric extendible if and only if:*

$$Tr(\rho_B^2) \geq Tr(\rho_{AB}^2) - 4\sqrt{det\rho_{AB}} \tag{5.32}$$

where $\rho_B = Tr_A\rho_{AB}$.

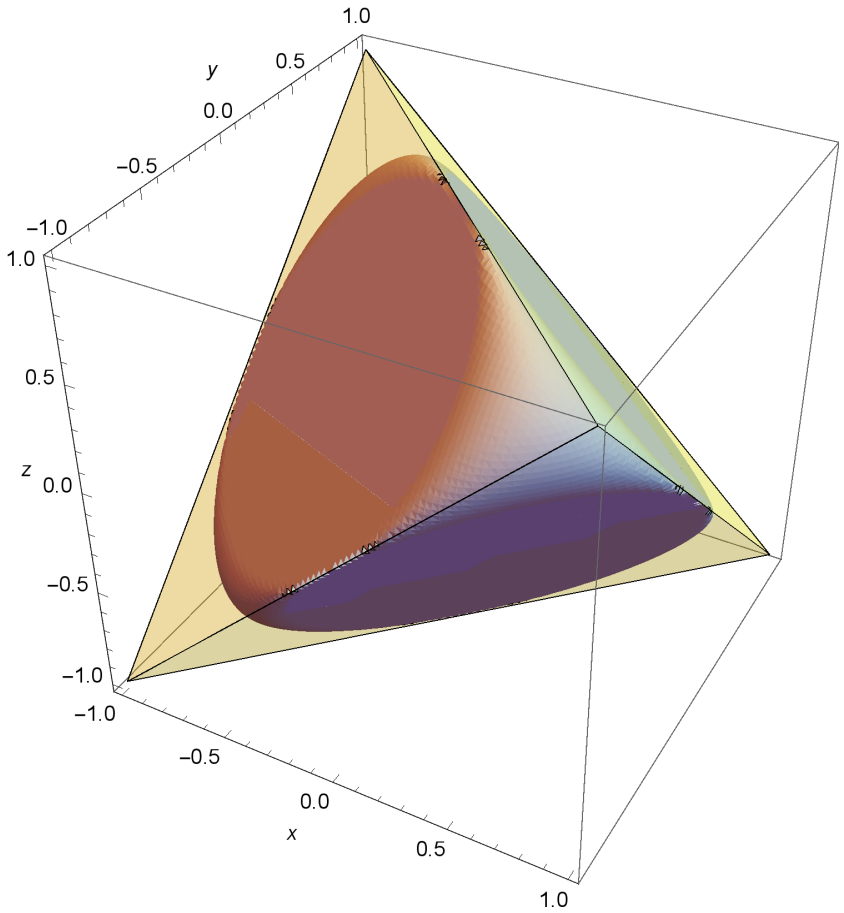

Fig. 5.2 Symmetric extendible states ρ_{AB} which are diagonal in the Bell basis are represented as the region $\mathscr{R} = \{\rho_{AB} : Tr(\rho_B^2) \geq Tr(\rho_{AB}^2) - 4\sqrt{det\rho_{AB}}\}$ inside the tetrahedron of Bell diagonal states.

The region of symmetric extendible bipartite qubit states on $\mathbb{C}^2 \otimes \mathbb{C}^2$, which are diagonal in the Bell basis, is represented in the Fig. 5.2. Since the reduced matrices of such states are maximally entangled, the simplified condition for such states reads:

$$4\sqrt{det\rho_{AB}} \geq Tr(\rho_{AB}^2) - \frac{1}{2} \tag{5.33}$$

Chapter 6

Distillation of entanglement and entanglement measures

6.1 Distilling quantum entanglement

The concept of entanglement distillation has its roots in classical communication theory where an initial message is sent through a noisy channel and then a receiver tries to recover an initial message by local operations and classical communication with the sender. Actually, the two engaged parties apply a communication protocol that in a natural way can include also error correction mechanism preventing the final message from disturbance of the environment when sent throughout the channel and cryptographic mechanisms protecting their communication from an influence of the adversary Eve. Thus, in quantum analogy Alice and Bob can consider a noisy quantum state of a shared systems as a resource that they would like to utilize for reliable communication under condition that they can transform their systems into strongly entangled pairs.

The distillable entanglement is a measure responding to the question: how much pure entanglement (in terms of singlets $P_- = |\Psi_-\rangle\langle\Psi_-|$) can Alice and Bob extract from n copies of a system in a state ρ_{AB} (globally in a state $\rho_{AB}^{\otimes n}$) by means of only local operations and classical communication (LOCC)? The two parties try to transform (distill) n pairs of systems in a state ρ_{AB} into k singlets $|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. The maximal possible rate $D(\rho_{AB}) = lim_{n\to\infty}\frac{k}{n}$ of this process is called distillable entanglement [Fig. 6.1].

One can consider different variations of entanglement distillation process basing on allowable types of classical communication between two parties (let us say Alice and Bob) sharing the system.

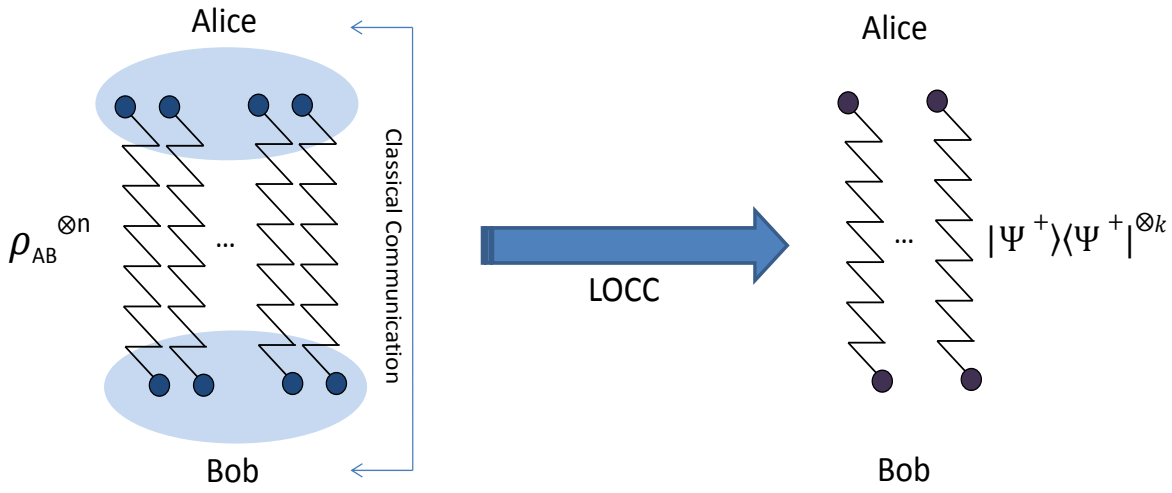

Fig. 6.1 Spatially separated Alice and Bob share n pairs of quantum states ρ_{AB}. They operate on the pairs with local quantum operations and engage also a classical channel of communication, e.g. a mobile, to communicate classically. After action of this quantum protocol, they achieve k pairs of strongly entangled states $|\Psi_+\rangle$.

Namely, the most popular and historically first scheme is based on local quantum operations and bidirectional communication between Alice and Bob, so called 2-LOCC or two-way entanglement distillation, for which one considers the rate $D_{\leftrightarrow}$.

If only one-directional communication is allowed in the distillation protocol (either from Alice to Bob or only from Bob to Alice), then we say about 1-LOCC or one-way entanglement distillation (and one-way distillable entanglement rate $D_{\rightarrow}$ respectively).

In case of no classical communication allowed (only quantum local operations allowed), we consider so called zero-way or 0-LOCC entanglement distillation protocols (and $D_{\emptyset}$). Since protocols using zero-way communication are a subset of a set of protocols using one-way classical communication, and the latter are a subset of 2-LOCC protocols, it is an immediate observation that in general for any ρ_{AB} there holds:

$$D_{\emptyset}(\rho_{AB}) \leq D_{\rightarrow}(\rho_{AB}) \leq D_{\leftrightarrow}(\rho_{AB}) \tag{6.1}$$

A formal definition of the process is as follows:

Definition 6.1.1 *[98, 137] For a bipartite state $\rho_{AB} \in \mathscr{B}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ consider a sequence P_n of LOCC operations such that $P_n(\rho_{AB}^{\otimes n}) = \rho_n$ where $\rho_n \in \mathscr{B}([\mathbb{C}^2 \otimes \mathbb{C}^2]^{\otimes k_n})$. Then the set $\mathscr{P} = \bigcup_{n=1}^{\infty}\{P_n\}$ is called a distillation protocol of the state ρ_{AB} if:*

$$\lim_{n\to\infty} \|\rho_n - P_-^{\otimes k_n}\| = 0. \tag{6.2}$$

For a chosen distillation protocol $\mathscr{P}$, its rate is defined as:

$$R(\mathscr{P}) = \lim_{n\to\infty} \sup \frac{k_n}{n} \tag{6.3}$$

Then the entanglement distillation of the state ρ_{AB} is defined as:

$$D(\rho_{AB}) = \sup_{\mathscr{P}} R(\mathscr{P}), \tag{6.4}$$

where supremum is over all possible distillation protocols $\mathscr{P}$.

Therefore, we recalled also a definition of a rate of a given quantum protocol (even such for which $\mathscr{R}(P) = 0$) and we take supremum over all accessible protocols to Alice and Bob to find the most optimal one which extracts a maximal possible number of pure singlets $P_- = |\Psi_-\rangle\langle\Psi_-|$ (if any).

There exists a dual concept to the distillable entanglement engaging in some sense reverse scheme, so called *entanglement cost* E_C. In general, it measures how many singlets has to be utilized by Alice and Bob minimally to produce n output copies of a state ρ_{AB}. Thus,

$E_C(\rho_{AB}) = lim_{n\to\infty}\frac{k}{n}$ where k stands for the number of bipartite systems in a singlet state $|\Psi_-\rangle$ needed in this process.

Definition 6.1.2 *[98, 137] For a bipartite state $\rho_{AB} \in \mathscr{B}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ consider a sequence P_n of LOCC operations such that $P_n(|\Psi_-\rangle\langle\Psi_-|^{\otimes n}) = \rho_n$ where $\rho_n \in \mathscr{B}([\mathbb{C}^2 \otimes \mathbb{C}^2]^{\otimes k_n})$. Then the set $\mathscr{P} = \bigcup_{n=1}^{\infty}\{P_n\}$ is called a formation protocol of the state ρ_{AB} if:*

$$\lim_{n\to\infty} \|\rho_n - \rho_{AB}^{\otimes k_n}\| = 0. \tag{6.5}$$

For a chosen formation protocol $\mathscr{P}$, its rate is defined as:

$$R(\mathscr{P}) = \lim_{n\to\infty} \sup \frac{n}{k_n} \tag{6.6}$$

Then the entanglement cost of a state ρ_{AB} is defined as:

$$E_C(\rho_{AB}) = \sup_{\mathscr{P}} R(\mathscr{P}), \tag{6.7}$$

where supremum is over all possible protocols $\mathscr{P}$ of ρ_{AB} formation.

Calculation of distillable entanglement for any state ρ is extremely difficult due to the considered asymptotic region and non-classical behavior of quantum entanglement for many pairs (e.g. activation of bound entanglement or general non-additivity of entanglement). Thus, one cannot just scale the behavior of entanglement for a couple of entangled pairs into the infinite regime. Basing on that, of a great importance become all efficient lower and upper bounds on distillable entanglement (in all LOCC variants), especially those operationally easy to calculate or verify in labs.

We say that a state is non-distillable if $D(\rho_{AB}) = 0$, i.e. there does not exist any such a protocol that the output state ρ_{out} is in a singlet state. To assess capabilities of the engaged protocol to distill entanglement, we can recall the fidelity measure as $F(\rho_{out}) = TrP_+^{\otimes k}\rho_{out}$ to assess the overlap between the output state and the expected number of singlets as we will see in the example below.

Example 6.1.3 *(BBPSW Distillation Protocol [17])*
We assume that Alice and Bob starts the protocol sharing multiple pairs of ρ_{AB} state. The fidelity fraction for these states is $F(\rho_{AB}) = TrP_+\rho_{AB} > 1/2$. As proved in [17], only then the protocol is able to distill a smaller number of pairs with higher singlet fraction. We repeat the following steps and with each iteration the fidelity for output states grows:

1. Alice and Bob take two pairs of the initial state ρ_{AB} and apply $U \otimes U^*$ twirling operation achieving isotropic states (as observed in the previous chapter) - i.e. two realize twirling, Alice engages one-way classical communication to communicate to Bob which random unitary operation U he should apply:

$$\rho_{AB} \otimes \rho_{AB} \longrightarrow \rho_F \otimes \rho_F \tag{6.8}$$

2. Then they apply locally U_{XOR} operation at each pair they possess locally, where the first qubit is called a source qubit and the second as a target qubit:

$$U_{XOR} = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \tag{6.9}$$

3. The target qubits of Alice and Bob are measured locally in a computational basis $\{|0\rangle, |1\rangle\}$. If Alice and Bob have the same result (they have to engage at this stage two-way classical communication to verify the results), they keep the source pair $\widetilde{\rho}_{AB}$. Otherwise, they discard the source pair and can repeat with other pairs.
One can calculate now the improved singlet fraction $\widetilde{F}$ for the remaining pairs $\widetilde{\rho}_{AB}$:

$$\widetilde{F}(\widetilde{\rho}_{AB}) = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} \tag{6.10}$$

With a huge number of pairs Alice and Bob can obtain arbitrary high F, yet still not $F = 1$, as the asymptotic rate of this protocol is convergent to zero. Therefore, at a next stage we have to engage so-called 'hashing protocol' [47–49] which enables final distillation of singlet pairs by means of one-way distillation protocol for pairs where coherent information is positive $I_C(A\rangle B) > 0$.

In general, for any state ρ_{AB}, one can state the following necessary and sufficient condition for distillability of any bipartite quantum state:

Theorem 6.1.4 *[100] Any state ρ_{AB} on $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ is distillable if and only if there exist two-dimensional projectors $P : \mathscr{H}_A^n \to \mathbb{C}^2$ and $Q : \mathscr{H}_B^n \to \mathbb{C}^2$, such that for some n the state:*

$$\widetilde{\rho}_{AB} = (P \otimes Q)\rho_{AB}^{\otimes n}(P \otimes Q)^\dagger \tag{6.11}$$

is entangled.

As a consequence, we observe that all NPT two-qubit states $\rho_{AB} \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ are two-way distillable and in general, all NPT states $\rho_{AB} \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^3)$ are two-way distillable. Furthermore, it implies the following powerful statement:

Theorem 6.1.5 *[100] If a state ρ_{AB} is PPT, then it cannot be distilled.*

There exist a broad class of so-called *bound entangled states* [100], from which no entanglement can be distilled. The initially discovered class of bound entangled states was of PPT type due to the above theorem stating that PPT states cannot be distilled even if they are entangled. However, there is a big open problem in quantum information theory still unresolved, whether there exist non-distillable NPT entangled states. As we observed previously that any state can be transformed by twirling to Werner states, this problem can be reduced to the issue of finding non-distillable Werner states as follows:

Theorem 6.1.6 *[101] The following statements are equivalent:*
1. Any NPT state is distillable.
2. Any entangled Werner state ρ_W is distillable.

Example 6.1.7 *(Bound Entangled State [100]) A state $\rho_a \in \mathscr{B}(\mathbb{C}^3 \otimes \mathbb{C}^3)$ is PPT bound entangled for $a \in (0,1)$ and separable for $a = 0$ or $a = 1$:*

$$\rho_a = \frac{1}{8a+1}\begin{pmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{pmatrix} \tag{6.12}$$

One-way entanglement distillation

In [50, 51, 49], I. Devetak and A. Winter proved that one-way distillable entanglement $D_{\rightarrow}$ of a state ρ_{AB} can be represented as regularization of one-copy formula engaging coherent information. The proof of this theorem was possible only due to the proof of a very powerful *hashing inequality* [49] which to date is one of the strongest results in domain of one-way quantum protocols.

A one-way entanglement distillation protocol consists of:

1. A quantum instrument $\mathbf{T} = (T_l)_{l=1}^{L}$ for Alice which is a set of quantum operations

performed by Alice.
2. For each l (communicated by Alice to Bob via a classical channel), there exists a quantum operation R_l performed by Bob (R_l are trace-preserving completely positive maps).

We call it an (n,ε)-protocol [49] if it acts on n copies of the state shared between Alice and Bob and produce a maximally entangled state:

$$|\Psi_N\rangle = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} |n_A\rangle \otimes |n_B\rangle \tag{6.13}$$

with fidelity $1-\varepsilon$:

$$F(|\Psi_N\rangle, \sum_{l=1}^{L} (T_l \otimes R_l)\rho_{AB}) \geq 1-\varepsilon \tag{6.14}$$

Then there holds a hashing inequality for any state ρ_{AB}:

Theorem 6.1.8 *[49] For any state ρ_{AB}, there holds:*

$$D_{\rightarrow}(\rho_{AB}) \geq I_C(A\rangle B) \tag{6.15}$$

where $I_C(A\rangle B) = S(B) - S(AB)$.

And these results lead to more general formula for one-way entanglement distillation in terms of coherent information:

Theorem 6.1.9 *[49] For any bipartite state ρ_{AB}:*

$$D_{\rightarrow}(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} D^{(1)}_{\rightarrow}(\rho_{AB}^{\otimes n}) \tag{6.16}$$

with

$$D^{(1)}_{\rightarrow}(\rho_{AB}) = \max_{\boldsymbol{T}} \sum_{l=1}^{L} \lambda_l I_c(A\rangle B)_{\rho_l} \tag{6.17}$$

where the maximization is over quantum instruments $T = \{T_1, \ldots, T_L\}$ on Alice's system, $\lambda_l = TrT_l(\rho_A)$, T_l is assumed to have one Kraus operator $T_l(\rho) = A_l \rho A_l^{\dagger}$ and $\rho_l = \frac{1}{\lambda_l}(T_l \otimes id)\rho_{AB}$. Moreover, it is assumed that l is bounded by dimension of A system as $L \leq d_A^2$.

Generally for two-way LOCC, I. Devetak and A. Winter proved a very interesting result [49]:

Theorem 6.1.10 *For any state ρ_{AB}:*

$$D(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} \sup_{V} I_C(A'\rangle B')_{\omega} \tag{6.18}$$

with any two-way LOCC operations V and the coherent information refers to the output state $\omega = V(\rho_{AB}^{\otimes n})$.

Since the concept of the coherent information is fundamental for definitions of distillable entanglement and quantum channel capacity, we recall below the observation about a multipartite system ABB' where BB' part is initially possessed by Bob (Alice possesses A-subsystem) and Bob can transfer B'-subsystem to Eve:

Observation 6.1.11 *[127] For a bipartite state* $\rho_{ABB'} \in B(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_{B'})$ *shared between Alice and Bob (B and B' system) there holds:*

$$I_c(A\rangle BB') \leq I_c(A\rangle B) + 2S(B') \tag{6.19}$$

Proof. One can easily observe that for subadditivity of entropy $S(BB') \leq S(B) + S(B')$ and for the Araki-Lieb inequality $|S(AB) - S(B')| \leq S(ABB')$, the left hand side can be bounded as follows: $S(BB') - S(ABB') \leq S(B) + S(B') - S(AB) + S(B') = I_c(A\rangle B) + 2S(B')$ which completes the proof. □

As observed, there are two classes of quantum states which cannot be generally distilled by means of two-way LOCC protocols: separable states and bound entangled states that we elaborate on further. If we consider now a domain of one-way distillation, we have to add one more class of all symmetric extendible states [126], from which no entanglement can be distilled by means of one-way LOCC. That is a subject of the following observation [126]:

Observation 6.1.12 *If any bipartite state* ρ_{AB} *has a symmetric extension* $\rho_{ABB'}$*, so that* $\rho_{ABB'} = \rho_{AB'B}$ *and* $\rho_{AB} = Tr_{B'}\rho_{ABB'}$*, then for the one-way distillable entanglement there holds:*

$$D_{\rightarrow}(\rho_{AB}) = 0. \tag{6.20}$$

Proof of the above theorem is immediate and follows from quantum entanglement monogamy (cf. [26, 30]). If Alice sends classical information to Bob and they distill singlet in the protocol then the state can not have symmetric extension since Bob's colleague, say Brigitte (corresponding to index B') could also receive the same message from Alice and finally share the singlet with Alice too. But Alice's particle cannot be maximally entangled with two different particles at the same time (this is just the entanglement monogamy property). So a symmetric extendible state can not have one-way distillable entanglement nonzero.

Basing on theory of entanglement distillability we state the following conjecture in domain of one-way communication linking it directly with symmetric extendibility of quantum states:

Conjecture 6.1.13 *[128] Any state ρ_{AB} on $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ is one-way distillable if and only if there exists a two-dimensional projector $P : \mathscr{H}_A^n \to \mathbb{C}^2$ such that for some $n \geq 1$ the state:*

$$\widetilde{\rho}_{AB} = (P \otimes id)\rho_{AB}^{\otimes n}(P \otimes id)^{\dagger} \tag{6.21}$$

is not symmetrically extendible.

For a potential proof, it is an immediate observation that one-way distillable quantum states cannot be symmetric extendible [126], yet it is an open question if there exists a two-qubit state that is not at the same time symmetric extendible nor one-way distillable. Since we know conditions for symmetric extendibility of two-qubit states [123, 112], this conjecture if true would simplify analysis of entanglement of two-qubit states and capacity of channels acting on such spaces substantially. On the contrary, if there exist two-qubit states that are neither symmetric extendible nor one-way distillable then they would be one-way counterparts of bound entangled states for two-way distillability in higer dimensions. An analysis of this subject seems to be of a great importance for further studies on quantum secure protocols and structure of entanglement.

As an example, it is worth mentioning Werner states [167] and the hypothesis about NPT (non-positive trace-preserving) bound entangled states [53, 59]. As discussed in a previous chapter, the structure of the Werner states is as follows:

$$\rho_W(\alpha) = \frac{id + \alpha\mathbb{P}}{d^2 + \alpha d} \tag{6.22}$$

where $\mathbb{P} = \sum_{i,j=0}^{d-1} |ij\rangle\langle ji|$. The state is separable for $1 \geq \alpha \geq -\frac{1}{d}$, NPT for $-\frac{1}{d} > \alpha \geq 1$ and two-way 1-distillable for $-\frac{1}{2} > \alpha \geq -1$. Applying the conditions for symmetric extendibility [112], we found that for $d = 2$, the state is non-symmetric extendible for $-0.8 \geq \alpha \geq -1$.

We analyzed potential one-way distillability of the state for the region of non-symmetric extendible Werner states with non-positive coherent information, namely for $-0.8 \geq \alpha > \cong -0.85559$. The latter condition excludes all those states being distilled by well-known one-way hashing protocol.

The analysis was performed for two-copies of the state and over 10^8 random filtering operations on Alice' side and random unitary operations on Bob's side. However, the protocol was not able to distill states with positive coherent information which suffices to distill entanglement with the hashing protocol.

Therefore, it is *an open question* if the state is one-way distillable in the region $-0.8 \geq \alpha > \cong -0.85559$ or it is one-way 'bound entangled' which would be a counterpart of bound entanglement concept in two-way communication domain.

6.2 Entanglement measures

As we could already observe, of profound importance is the method of quantifying entanglement which is a subject of entanglement measures theory.

All entanglement measures $E : \mathscr{B}(\mathscr{H}) \longrightarrow \mathbb{R}_{\geq 0}$ have to meet the following necessary conditions although there are still discussions which conditions they should meet [98, 13]:
1. *Monotonicity* under action of any LOCC operation Λ:

$$E(\rho_{AB}) \geq E(\Lambda(\rho_{AB})) \tag{6.23}$$

Its strong monotonicity version assumes that one can apply probabilistic LOCC (i.e. after action of probabilistic LOCC on the state ρ_{AB}, one gets the state ρ_{AB}^i with probability p_i) and then we require:

$$E(\rho_{AB}) \geq \sum_i p_i E(\rho_{AB}^i) \tag{6.24}$$

2. *Vanishing on separable states*, i.e. for any separable state ρ_{AB}, it is required that:

$$E(\rho_{AB}) = 0 \tag{6.25}$$

In this context, there are some additional postulates related to entanglement measures which support to a great extent analysis of entanglement properties:
3. *Normalization* on singlet states: $E(|\Psi_+\rangle\langle\Psi_+|) = \log d$.
4. *Asymptotic continuity:*

$$\|\rho_n - \sigma_n\|_1 \to 0 \Longrightarrow \frac{|E(\rho_n) - E(\sigma_n)|}{\log d_n} \to 0, \tag{6.26}$$

where $\rho_n, \sigma_n \in \mathscr{B}(\mathscr{H}_n)$ and $\dim \mathscr{H}_n = d_n$.
5. *Convexity* for any ensemble of states $\{p_i, \rho_i\}$:

$$E(\sum_i p_i \rho_i) \leq \sum_i p_i E(\rho_i). \tag{6.27}$$

Some measures can possess also additivity property for any two states:

$$E(\rho \otimes \sigma) = E(\rho) + E(\sigma) \tag{6.28}$$

but in general they are either sub-additive ($\leq$) or super-additive ($\geq$). For such cases as we will see further, it is convenient to consider a *regularized measure* $E^{\infty}(\rho_{AB})$:

$$E^{\infty}(\rho_{AB}) = \lim_{n\to\infty} \frac{E(\rho_{AB}^{\otimes n})}{n} \tag{6.29}$$

In general, as defined by G. Vidal [166], any function $E : \mathscr{B}(\mathscr{H}) \longrightarrow \mathbb{R}_{\geq 0}$ which is just monotonic under LOCC operations is called *an entanglement monotone*. To be more precise, we expect that any entanglement monotone (and any entanglement measure) is invariant under local unitary operations and does not increase under action of LOCC and this is why we restrict our attention only to the non-increasing monotones (under action of LOCC), and in particular, to one-way entanglement monotones (non-increasing under 1-LOCC). It can be assumed that [166] an entanglement monotone is non-increasing 'on average' under action of LOCC (which is a more restrictive version of monotonicity), i.e.:

$$E(\rho) \geq \sum_i p_i E(\rho_i) \tag{6.30}$$

where after action of probabilistic LOCC on the state ρ, one gets the state ρ_i with probability p_i. In the following, the new entanglement monotone based on the best symmetric extendible approximation in is an example meeting such a condition.

We have already considered *geometric measures of entanglement* like the trace distance measure, the Bures measure, the Hilbert-Schmidt measure and the fidelity of entanglement or relative entropy of entanglement. All are related by direct connections with geometry of analyzed states and its geometric distance or similarity to either separable states or symmetric extendible states. The latter is considered as far as the subject of analysis includes action of 1-LOCC operations [126].

Further, both aforementioned distillable entanglement and entanglement cost are examples of *operational measures of entanglement* [13]. They are defined implicitly due to the asymptotic regime considered and are operational due to the direct relation to operations LOCC that form engaged quantum protocols $\mathscr{P}$ in a laboratory by Alice and Bob in order to distill entanglement or engage entanglement into production of requested quantum states.

We invoke another measure built directly on a concept of extendibility where for a given state ρ_{AB}, one searches for its tripartite extensions.

Squashed entanglement [32] is defined as:

$$E_{sq}(\rho_{AB}) = \inf_{\rho_{ABE}} \frac{1}{2}[S_{AE} + S_{BE} - S_E - S_{ABE}] \tag{6.31}$$

where the infimum is taken over all extensions ρ_{ABE} so that $\rho_{AB} = Tr_E \rho_{ABE}$ and S_X stands for the von Neumann entropy of the system X. Squashed entanglement is monotone, vanishes on separable states and is convex.

In what follows, we show how new upper bounds on one-way entanglement distillation and new entanglement monotones can be built applying the above theorems and the concept of symmetric extendibility.

Symmetric extendible component in quantum states

In this section we consider vulnerability of quantum states to the loss [128] of non-symmetric extendibility property asking how easily the quantum state becomes symmetric extendible by distraction of its sub-system or how much of symmetric extendibility can be extracted from the state. When the former recalls lockability of entanglement measures, the latter relates to the best symmetric approximation subject responding to the question: how much of non-symmetric extendible component has to be mixed with symmetric extendible state so that it becomes non-symmetric extendible?

The general idea of locking a property of a quantum state relates to the loss or decrease of this property subjected to a measurement or discarding of one qubit. It has been shown [103, 32] that entanglement of formation, entanglement cost and logarithmic negativity are lockable measures which manifests as an arbitrary decrease of those measures after measuring one qubit.

Herewith, we analyze in fact locking of non-symmetric extendibility in sense that discarding one qubit from the quantum state that is not symmetric extendible leads to the loss of this property. Further, we derive implications for quantum security applying one-way communication between engaged parties Alice and Bob.

We shall show now that the property of non-symmetric extendibility of an arbitrary state ρ_{AB} can be destroyed by measurement of one qubit and in result, it presents how easily a quantum state can be removed of one-way distillability and security.

Let us consider bipartite quantum state shared between Alice and Bob on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B \cong \mathbb{C}^{d+2} \otimes \mathbb{C}^{d+2}$

$$\rho_{AB} = \frac{1}{2d-1} \begin{bmatrix} dP_+ & 0 & 0 & \mathscr{A} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathscr{A}^\dagger & 0 & 0 & \sigma \end{bmatrix} \tag{6.32}$$

where P_+ is a maximally entangled state on $\mathbb{C}^d \otimes \mathbb{C}^d$, $\sigma = \sum_{i=1}^{d-1} |i\,0\rangle\langle i\,0|$ and $\mathscr{A}$ is an arbitrary chosen operator so that ρ_{AB} represents a correct quantum state. This state is represented in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ held by Alice and Bob and possess a singlet-like structure. Whenever one party (Alice or Bob) measures the state in the local computational basis, the state decoheres and off-diagonal elements vanish which leads to a symmetric extendible state [126]:

$$\Upsilon_{AB} = \frac{d}{2d-1} P_+ + \frac{1}{2d-1} \sum_{i=1}^{d-1} |i\,0\rangle\langle i\,0| \tag{6.33}$$

from which no entanglement nor secret key can be distilled by means of one-way communication and local operations. Clearly this example shows that from a non-symmetric extendible state possessing large entanglement cost and non-zero one-way secret key one can easily obtain a symmetric structure by discarding small part of the whole system destroying possibility of entanglement distillation and secret key generation by means of 1-LOCC.

Thus, it is interesting to consider how much of symmetric extendibility is embedded in a given state ρ_{AB} as it can be expected that the more symmetric extendibility is hidden in a state, the less vulnerable for losses of one-way distillable entanglement and security it is [128]. Besides analysis of symmetric structures in projected subspaces, we will also propose to perform this task by means of *the best symmetric extendible approximation* [122, 113] that decomposes the state into a symmetric extendible component σ_{ext} and non-symmetric extendible component σ_{next}:

$$\rho_{AB} = \max_{\lambda} \lambda\,\sigma_{ext} + (1-\lambda)\sigma_{next} \tag{6.34}$$

We denote by $\lambda_{max}(\rho)$ the maximum weight of extendibility [122] of ρ_{AB} where $0 \leq \lambda_{max}(\rho) \leq 1$,thus, all symmetric extendible states have the weight $\lambda_{max} = 1$ and due to the maximization of λ over all potential decompositions of ρ into a symmetric extendible and non-symmetric extendible component, the state σ_{next} does not contain any symmetric extendible component, i.e. $\lambda_{max}(\sigma_{next}) = 0$. It is proved in [124, 122] that in case of one-way protocols only the non-symmetric extendible component can be effectively utilized for generation of a secret key and it confirms that the notion of symmetric extendibility is crucial for consideration of one-way entanglement and key distillation [Fig. 6.2].

However, we show that there exist states which do not possess any symmetric extendible component in the aforementioned decomposition but there can be a large symmetric extendible component embedded in them. An example of such a state is given above (8.40) and one can derive the following statement about general structure of such states:

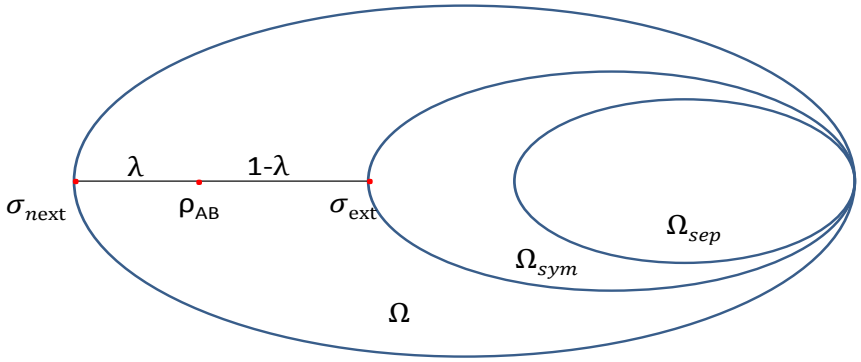

Fig. 6.2 Best symmetric extendible approximation of a state $\rho_{AB} = \max_\lambda \lambda\sigma_{ext} + (1-\lambda)\sigma_{next}$. Ω_{sep} denotes the set of separable states, Ω_{sym} denotes the set of symmetric extendible states and Ω stands for the set of quantum states. There holds a natural inclusion relation: $\Omega_{sep} \subset \Omega_{sym} \subset \Omega$.

Lemma 6.2.1 *[128] Consider a state γ on $\mathscr{H}_{AA'BB'} = \mathscr{H}_A \otimes \mathscr{H}_{A'} \otimes \mathscr{H}_B \otimes \mathscr{H}_{B'} \sim \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$:*

$$\gamma = \rho \otimes \sigma \tag{6.35}$$

being a composition of an arbitrary chosen state $\sigma \in B(\mathscr{H}_{A'} \otimes \mathscr{H}_{B'})$ and a non-symmetric extendible state $\rho \in B(\mathscr{H}_A \otimes \mathscr{H}_B)$ with no symmetric extendible component $\lambda_{max}(\rho) = 0$. Then for the best extendible approximation of γ there holds $\lambda_{max}(\gamma) = 0$, i.e. there is no symmetric extendible component in $\gamma \in B(\mathscr{H}_{AA'BB'})$.

Proof.

Conversely, assume that there exists decomposition of $\gamma_{AA'BB'}$ with non-zero symmetric extendible component, i.e. $\lambda \neq 0$:

$$\gamma_{AA'BB'} = \lambda\sigma_{ext} + (1-\lambda)\rho_{ne} \tag{6.36}$$

then both components would be supported on $\mathscr{H}_{AA'BB'}$ and one can search for a decomposition of $\gamma_{AA'BB'}$ after tracing out A'B'-part. Due to linearity of a partial trace operation $\Gamma_X(\cdot) =$

$Tr_X(\cdot)$ we obtain:

$$\Gamma_{A'B'}(\gamma_{AA'BB'}) = \lambda\Gamma_{A'B'}(\sigma_{ext}) + (1-\lambda)\Gamma_{A'B'}(\rho_{ne}) \tag{6.37}$$

and, further, basing on a symmetric extendibility property of composite systems [126] one derives that tracing out $A'B'$ from σ_{ext} does not destroy its symmetric extendibility and produces symmetric extendible state $\widetilde{\sigma}_{ext}$ ($\widetilde{\rho}_{ne}$ results from tracing out A'B' from ρ_{ne}):

$$\rho = \lambda\widetilde{\sigma}_{ext} + (1-\lambda)\widetilde{\rho}_{ne} \tag{6.38}$$

Thus, the initial assumption would imply existence of a non-zero symmetric extendible component of the state ρ that contradicts the aforementioned decomposition. □

In the following, one can make an immediate observation about any private quantum state[1] [103]:

Corollary 6.2.2 *[128] Any private quantum state $\gamma_{ABA'B'} \in B(\mathscr{H}_{ABA'B'})$:*

$$\gamma_{ABA'B'} = \frac{1}{2}\sum_{i,j=0}^{1} |ii\rangle\langle jj| \otimes U_i\rho_{A'B'}U_j^{\dagger}, \tag{6.39}$$

where U_i and U_j are arbitrary unitary transformations, does not possess symmetric extendible component, i.e. $\lambda_{max} = 0$.

Remark. The proof is conducted in analogy to the proof of 6.2.1 but this state represents a twisted composition of singlet and an arbitrary chosen state $\rho_{A'B'}$ where AB-part is the key part of the state and is not symmetric extendible due to the observation that secure states cannot be symmetric extendible [122].

Basing on previous studies of entanglement measures and importance of symmetric extendible states, we introduce the following one-way *best symmetric approximated entanglement monotone* (as a counterpart of BSA - best separable approximation in [113]):

Definition 6.2.3 *[128] For any $\rho \in B(\mathscr{H}_A \otimes \mathscr{H}_B)$ having best symmetric decomposition $\rho_{AB} = \max_\lambda \lambda\sigma_{ext} + (1-\lambda)\sigma_{next}$, the best symmetric approximated entanglement monotone is defined as:*

$$E^{ss}(\rho) = 1 - \lambda_{max}(\rho) \tag{6.40}$$

[1] Vide sec. Quantum private states and secret key.

Proof. (We will prove that the quantity meets the conditions to become an entanglement monotone.)
1. If ρ is separable, i.e. also symmetric extendible, then $\lambda_{max} = 1$ and $E^{ss}(\rho) = 1 - \lambda_{max} = 0$.
2. $E^{ss}(\rho)$ is invariant under local unitary operations since application of local operations U_A and U_B on σ_{ext} leaves it extendible to the third part B', i.e. $E^{ss}(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger) \geq E^{ss}(\rho)$ and vice versa.
3. For any bi-local operations $V_i(\cdot)$ (with allowed one-way communication, where $V_i(\cdot) = A_i(\cdot)A_i^\dagger \otimes \Lambda_i(\cdot)$, $\sum_i A_i A_i^\dagger = \mathbb{I}$ and A_i denotes local POVMs on Alice's side and $\Lambda_i(\cdot)$ denotes completely positive trace-preserving map on Bob's side), there holds:

$$\begin{aligned} E^{ss}(\rho) = 1 - \lambda_{max}(\rho) &\geq \sum_i (1 - \lambda_i^{\max}(\rho_i) Tr(V_i(\rho))) \\ &\geq \sum_i E^{ss}(\rho_i) Tr(V_i(\rho))) \end{aligned}$$

and $\rho_i = V_i(\rho)/Tr(V_i(\rho))$. To achieve this result we followed the reasoning in [113] and the fact that the set of symmetric extendible states is closed under 1-LOCC operations which means that any bi-local operations associated with one-way communication cannot generate non-symmetric extendible state from a symmetric extendible state so they can only increase the symmetric extendible component in the output state, i.e.:

$$V_i(\rho) = V_i(\lambda \sigma_{ext} + (1-\lambda)\sigma_{next}) \to \rho_i = \lambda_i \sigma_i^{ext} + (1-\lambda_i)\sigma_i^{next}, \tag{6.41}$$

and we observe that $\lambda_i \geq \lambda$ as the local operations can still operate on the state σ_{next} in such a way that the output state can possess some symmetric extendible component but not vice versa (we recall the observation that initially, σ_{next} does not contain any symmetric extendible component). □

It is interesting to notice that for two-qubit states on $\mathbb{C}^2 \otimes \mathbb{C}^2$ there holds a non-trival observation about best symmetric approximated decomposition:

$$\rho = \lambda \sigma_{ext} + (1-\lambda)|\Psi\rangle\langle\Psi| \tag{6.42}$$

with σ_{ext} being a symmetric extendible component that appears in ρ with highest probability. The proof of this observation can be based on BSA with separable components [113] where $\rho = \alpha\sigma_{sep} + (1-\alpha)|\Psi\rangle\langle\Psi|$ (remembering that $\rho \in \mathscr{B}(\mathbb{C}^2 \otimes \mathbb{C}^2)$). As set of separable states is a subset of the convex set of symmetric extendible states, then for any dimension $\alpha \leq \lambda$. Further, due to the fact that any two-qubit state has best separable decomposition into a separable and projective entangled component, we conclude that $\lambda\sigma_{ext} = \alpha\sigma_{sep} + \beta|\Psi\rangle\langle\Psi|$ for arbitrary chosen β.

These propositions can simplify potentially many research problems like analysis of *CHSH* regions vs. symmetric extendibility of states [121] represented in the steering ellipsoid formalism or just further analysis on security and distillability of all $\mathbb{C}^2 \otimes \mathbb{C}^2$ states.

A. Sanpera and R. Quesada pointed out in [141] that there is a strong relation between the best separable approximation and the max-relative entropy. The max-relative entropy can be defined as: $D_{\max}(\sigma \parallel \rho) \equiv \log \min\{\lambda : \sigma \leq \lambda\rho\}$ and $\mathrm{supp}\sigma \subseteq \mathrm{supp}\rho$ and it is interpreted as a probability of finding a component σ in decompositions of ρ. Then for the best separable approximation of a state ρ, $D_{\max}(\sigma_{sep} \parallel \rho)$ is interpreted as the maximal probability of finding σ_{sep} in the best separable decomposition of ρ.

Following these results, we can immediately propose a similar max-relative entropy monotone based on the best symmetric extendible decomposition, i.e. $D_{\max}(\sigma_{ext} \parallel \rho)$ where σ_{ext} stands for the extendible component in a state ρ. This leads immediately to $\lambda = \max(2^{-D_{\max}(\sigma_{ext}\|\rho)})$ where maximization is over the set of symmetric extendible states such that $\mathrm{supp}\sigma_{ext} \subseteq \mathrm{supp}\rho$.

An open problem [128] is, whether for one-way distillable entanglement we can state that $D_{\rightarrow}(\rho) \leq (1 - \lambda_{max}(\rho))D_{\rightarrow}(\sigma_{next})$? If the answer is negative, then it would be interesting to analyze a general relation between $D_{\rightarrow}$ and $D_{\rightarrow}(\sigma_{next})$. This issue seems to be substantial for bounding the one-way distillable entanglement for a state ρ in terms of the one-way distillable entanglement of its maximal non-extendible component.

6.3 New upper bounds on one-way distillable entanglement

We analyze now if similarly to the distance from separable states one can construct an appropriate entanglement measure basing on (5.23) [126]. The normalized distance from the set of extendible states does not satisfy though all necessary conditions [163, 164] that every measure of one-way distillable entanglement has to satisfy: introduction of the normalization factor δ_{AB} causes that $R_{\mathscr{E}_{AB}}(\rho)$ becomes explicitly dependant on the dimension of the system AB, therefore, for protocols increasing dimension of the input state the parameter is not a monotone [126]:

A1. If σ_{AB} is separable then $R_{\mathscr{E}_{AB}}(\sigma_{AB}) = 0$ due to the fact that every separable state is extendible.

A2. Local unitary operations leave $R_{\mathscr{E}_{AB}}(\sigma_{AB})$ invariant that is satisfied due to invariancy of distance measures under local unitary transformations, i.e. $R_{\mathscr{E}_{AB}}(\sigma_{AB}) = R_{\mathscr{E}_{AB}}(U_A \otimes U_B\sigma_{AB}U_A^{\dagger} \otimes U_B^{\dagger})$.

A3. (Restricted 1-LOCC monotonicity.) The parameter $R_{\mathscr{E}_{AB}}(\sigma_{AB})$ of one-way distillable entanglement does not increase under non-increasing dimension 1-LOCC, i.e. $\Lambda : B(\mathscr{H}_{AB}) \to B(\mathscr{H}_{\widetilde{A}\widetilde{B}})$ with $n_{AB} = \max[d_A, d_B]$, $n_{\widetilde{A}\widetilde{B}} = \max[d_{\widetilde{A}}, d_{\widetilde{B}}]$ for $n_{AB} \geq n_{\widetilde{A}\widetilde{B}}$, then

$$R_{\mathscr{E}_{\widetilde{A}\widetilde{B}}}(\Lambda(\sigma_{AB})) \leq R_{\mathscr{E}_{AB}}(\sigma_{AB}) \tag{6.43}$$

This condition may be simply proved due to non-increasing of $R(\rho\|\sigma)$ under a subclass of 1-LOCC operations Λ that is stated in the lemma 4.2.1, i.e. the set of symmetric extendible states $\mathscr{E}_{AB}$ is mapped under 1-LOCC into a set of symmetric extendible states $\mathscr{E}_{\widetilde{A}\widetilde{B}}$. Namely, because $\Lambda(\mathscr{E}_{AB}) \subset \mathscr{E}_{\widetilde{A}\widetilde{B}}$ and the relative entropy is monotonic under CP maps, and assuming that σ^* is an extendible state that realizes the minimal value in eq.(5.23) we have:

$$\begin{aligned} R_{\mathscr{E}_{AB}}(\rho) &= \delta_{AB} R(\rho\|\sigma^*) \geq \delta_{\widetilde{A}\widetilde{B}} R(\Lambda\rho\|\Lambda\sigma^*) \\ &\geq \delta_{\widetilde{A}\widetilde{B}} \inf_{\sigma\in\mathscr{E}_{\widetilde{A}\widetilde{B}}} R(\Lambda\rho\|\sigma) = R_{\mathscr{E}_{\widetilde{A}\widetilde{B}}}(\Lambda\rho) \end{aligned}$$

where $n_{AB} \geq n_{\widetilde{A}\widetilde{B}}$ derives the condition $\delta_{AB} \geq \delta_{\widetilde{A}\widetilde{B}}$ (the parameter δ_{AB} is defined in 5.23).

However, we show further that the entanglement parameter can be utilized for bounding one-way entanglement of distillation due to preparation of the measure in asymptotic regime.

In general, every entanglement parameter of type $E(\sigma) = \alpha \inf_{\rho\in\Delta} \mathscr{D}(\sigma\|\rho)$ where $\mathscr{D}(\sigma\|\rho)$ is appropriate distance between σ and ρ, Δ denotes the characteristic set to which the distance is measured and α normalizes the parameter so that $E(|\Psi_+\rangle\langle\Psi_+|) = \log d$ is not monotonic, i.e. $\exists_\Lambda\, E(\sigma) > E(\Lambda(\sigma))$. For $R_{\mathscr{E}_{AB}}$ unitary injection of input state ρ_{AB} into higher dimensional space gives $R_{\mathscr{E}_{AB}}(\rho) > R_{\mathscr{E}_{\widetilde{A}\widetilde{B}}}(\Lambda(\rho))$.

Additionally, following analysis in [98, 58], we show that the entanglement parameter satisfies:

B1. (Continuity on isotropic states.) We may simply show that this parameter is continuous on isotropic states $\rho(d_n, F_n)$ with $F_n \to 1, d_n \to \infty$ that means

$$\frac{R_{\mathscr{E}}(\rho(d_n, F_n))}{\log d_n} \to 1$$

as then $R_{\mathscr{E}}(\rho(d_n, F_n)) \to \log d_n$ that is easy to check.

Following the papers [98, 102] and the above definition we define the distance in the asymptotic regime as follows [126]:

$$R^{\infty}_{\mathscr{E}_{AB}}(\rho_{AB}) = \limsup_{n\to\infty} \frac{R_{\mathscr{E}_{AB}}(\rho_{AB}{}^{\otimes n})}{n} \tag{6.44}$$

Having defined above regularized parameter $R^{\infty}_{\mathscr{E}_{AB}}(\rho_{AB})$, we are able now to determine an upper bound on the one-way distillable entanglement. In [49] Devetak and Winter have proved a very powerful conjecture (discussed above) called "hashing inequality"

$$D_{\rightarrow} \geq S(\rho_B) - S(\rho_{AB})$$

from which one may find particular states of non-zero $D_{\rightarrow}$. For the very features of measures that bound the distillable entanglement $D_{\rightarrow}$, defined in [98, 58], where was shown that monotonicity and continuity on isotropic states are sufficient for any properly regularised function to be upper bound for $D_{\rightarrow}$, we may prove now the following theorem exploiting only distillation protocols in the line of the proof:

Theorem 6.3.1 *[126] For any bipartite state ρ_{AB} there holds:*

$$D_{\rightarrow}(\rho_{AB}) \leq R^{\infty}_{\mathscr{E}_{AB}}(\rho_{AB}) \tag{6.45}$$

Proof. Any one-way distillation protocol can be reduced to the distillation protocol [98, 58, 102] where the input is $\rho^{\otimes n}$ and the output is a family of the states $\rho(d_n, F_n)$ with $\lim_{n\to\infty} \frac{\log d_n}{n} = D_{\rightarrow}(\rho)$ and $F_n \to 1$.

We may always put $d_n \leq n^n_{AB}$ for $n_{AB} = \min[d_A, d_B]$ since there holds $D_{\rightarrow}(\rho) \leq \log n_{AB}$. Thus, we can consider only 1-LOCC non-increasing dimensions of input and so monotonicity of $R_{\mathscr{E}_{AB}}$ holds.

By analogy with the theorem put in [98, 58, 102] the properties (A3) and (B1) imply that $R^{\infty}_{\mathscr{E}_{AB}}(\rho_{AB})$ is an upper bound for $D_{\rightarrow}$. The regularisation (6.44) with supreme value enables the upper bound of $D_{\rightarrow}$. □

6.4 Reduced one-way distillable entanglement

We can now propose a new bound on distillation of entanglement by means of one-way LOCC. This result is based on the aforementioned observation [50, 51] that one-way distillable entanglement $D_{\rightarrow}$ of a state ρ_{AB} can be represented as regularization of one-copy formula: $D^{(1)}_{\rightarrow}(\rho_{AB}) = \max_{\mathbf{T}} \sum_{l=1}^{L} \lambda_l I_c(A\rangle B)_{\rho_l}$ where the maximization is over quantum instruments

$T = \{T_1, \ldots, T_L\}$ on Alice's system, $\lambda_l = TrT_l(\rho_A)$, T_l is assumed to have one Kraus operator $T_l(\rho) = A_l \rho A_l^\dagger$ and $\rho_l = \frac{1}{\lambda_l}(T_l \otimes id)\rho_{AB}$. Basing on the results of Observation 6.1.11, we derive a general formula for the bound on one-way distillable entanglement applying the reduced quantity:

Definition 6.4.1 *[127] For a bipartite state $\rho_{ABB'} \in B(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_{B'})$ shared between Alice and Bob (B and B' system) the reduced one-way distillable entanglement is defined as:*

$$D_{\rightarrow}^{(1)} \downarrow (\rho_{ABB'}) = \inf_{\mathscr{U}} [D_{\rightarrow}^{(1)}(\mathscr{U}(\rho_{AB})) + \Delta_{D_{\rightarrow}}] \tag{6.46}$$

where $\mathscr{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve, i.e. $\mathscr{U}(\rho_{AB}) = Tr_{B'}(I \otimes U_{BB'})\rho_{ABB'}$ for some unitary $U_{BB'}$. $\Delta_{D_{\rightarrow}} = 2S(\widetilde{\rho}_{B'})$ denotes the defect parameter related to increase of entropy produced by the transfer of B'-subsystem from Bob's side to Eve and $\widetilde{\rho}_{B'} = Tr_{AB}(I \otimes U_{BB'})\rho_{ABB'}$.

Remark. It is substantial to note that in a case of an odd dimension of the space of the system possessed by Bob, i.e. $dim\mathscr{B}(\mathscr{H}_{BB'}) = 2k+1$ for some $k \in \mathbb{N}$, we can always perform isometric embedding $E : \mathscr{B}(\mathscr{H}_{BB'}) \rightarrow \mathscr{B}(\mathscr{H}_{\widetilde{BB'}})$ of the space to make it even on Bob's side, which can be done e.g. be adding an ancillary system $\rho_{ancilla} = |0\rangle\langle 0|$ to Bob, also of an odd dimension and then perform a local unitary operation on Bob's side. After this operation Bob can always split his system which show that the definition can be always applied for the bipartite state shared between Alice and Bob, for any dimension on Bob's side. Since such an isometric embedding on Bob's side is a local operation, it does not change distillable entanglement for the system shared between Alice and Bob. Thus, in general, $D_{\rightarrow}(\rho_{ABB'}) = D_{\rightarrow}(\rho_{\widetilde{ABB'}})$. In a consequence, one can always generate $D_{\rightarrow}^{(1)} \downarrow (\rho_{\widetilde{ABB'}})$ We can apply this reasoning to all following statements about the reduced one-way distillable entanglement.

Theorem 6.4.2 *[127] For a bipartite state $\rho_{ABB'} \in B(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_{B'})$ shared between Alice and Bob (B and B' system) there holds:*

$$D_{\rightarrow}(\rho_{ABB'}) \leq D_{\rightarrow} \downarrow (\rho_{ABB'})$$

where $D_{\rightarrow} \downarrow (\rho_{ABB'}) = \lim_n D_{\rightarrow}^{(1)} \downarrow (\rho_{ABB'}^{\otimes n})/n$ denotes regularized version of reduced one-way distillable entanglement for one copy. Particularly, for identity operation $\mathscr{U} = id$ on Bob's side one obtains: $D_{\rightarrow}(\rho_{ABB'}) \leq D_{\rightarrow}(\rho_{AB}) + \Delta_{D_{\rightarrow}}$ where $\Delta_{D_{\rightarrow}} = 2S(\rho_{B'})$.

The left inequality is an immediate implication of the following lemma for the one-copy formula [127]:

Lemma 6.4.3 *[127] For every bipartite state $\rho_{ABB'}$ there holds:*

$$D^{(1)}_{\rightarrow}(\rho_{ABB'}) \leq D^{(1)}_{\rightarrow} \downarrow (\rho_{ABB'}) \tag{6.47}$$

Proof. It suffices to use results of Observation 6.1.11. to notice that for a chosen set of instruments **T** on Alice side for calculation of $D^{(1)}_{\rightarrow}(\rho_{ABB'})$ the inequality holds as extension of inequality from Observation 6.1.11. by multiplicands λ_l on the left and right side. However, if in case of calculating $D^{(1)}_{\rightarrow}(\rho_{AB})$ there exists a set **T'** maximizing $D_{\rightarrow}(\rho_{AB})$ better than **T**, then right hand side of the inequality can be only greater. □

To prove the inequality asymptotically it suffices to notice that statements of this lemma hold also for the arbitrary chosen state $\rho_n = \rho^{\otimes n}$. Let $\rho_n^{ABB'}$ be a state maximizing $D_{\rightarrow}(\rho_{ABB'})$ as an asymptotic regularization of coherent information (cf. def. 6.1.9).

Basing on Observation 6.1.11, one can immediately derive for the maximizing state $\rho_n^{ABB'}$: $\frac{1}{n} I_c(A\rangle BB') \leq \frac{1}{n}[I_c(A\rangle B) + 2S(\rho_n^{B'})]$. Since the maximization over quantum instruments **T** is on Alice's side, we can perform this operation on both sides of the inequality which completes the proof.

It is crucial to notice that the 'defect' parameters Δ for the reduced quantities are subadditive and hence, can be exploited in case of composite systems and regularization:

Corollary 6.4.4 *[127] For the reduced quantities of $\{K_{\rightarrow}, P, Q_{\rightarrow}, D_{\rightarrow}\}$ for composite systems there holds: $\Delta_X(\rho \otimes \sigma) \leq \Delta_X(\rho) + \Delta_X(\sigma)$ and $\Delta_Y(\Lambda \otimes \Gamma) \leq \Delta_Y(\Lambda) + \Delta_Y(\Gamma)$ where $X = \{K_{\rightarrow}, D_{\rightarrow}\}$ stands for states[2] and $Y = \{Q_{\rightarrow}, P\}$ for channels[3] respectively.*

To prove the above corollary it suffices to use subadditivity of entropy for composite systems since Bob can act with a unitary operation before he discards some part of his subsystem. This property of the parameters enables regularization in the asymptotic regime of the reduced quantities for large systems $\rho^{\otimes n}$.

Example 6.4.5 *(Activable multi-qubit bound entangled states)*

As an example illustrating this bound we consider an activated bound entangled state ρ_{II} [46] which is distillable if the parties (Alice and Bob) form two groups containing between 40% *and* 60% *of all parties of the system in the state ρ_{II}.*

If Alice or Bob posses less than 40% *of the system or system is shared between more than two parties, then the state becomes un-distillable. This state for large amount of particles can manifest features characteristic for 'macroscopic entanglement' with no 'microscopic entanglement'.*

[2] Vide chap. Quantum Privacy.
[3] Vide chap. Quantum Channels.

For definition of the state, let us consider the family ρ_N of N-qubit states:

$$\rho_N = \sum_{\sigma=\pm} \lambda_0^\sigma |\Psi_0^\sigma\rangle\langle\Psi_0^\sigma| + \sum_{k\neq 0} \lambda_k (|\Psi_k^+\rangle\langle\Psi_k^+| + |\Psi_k^-\rangle\langle\Psi_k^-|) \tag{6.48}$$

where $|\Psi_k^\pm\rangle = \frac{1}{\sqrt{2}}(|k_1k_2\ldots k_{N-1}0\rangle \pm |\bar{k}_1\bar{k}_2\ldots\bar{k}_{N-1}1\rangle)$ are GHZ-like states with $k = k_1k_2\ldots k_{N-1}$ being a chain of $N-1$ bits and $k_i = 0,1$ if $\bar{k}_i = 1,0$, thus, the state is parameterized by 2^{N-1} coefficients. The states $|\Psi_0^\pm\rangle = \frac{1}{\sqrt{2}}(|00\ldots0\rangle \pm |11\ldots1\rangle)$ denote the standard GHZ states.

Let us consider now a bipartite splitting $\mathscr{P}$ where Alice takes $0.6N$ of qubits and Bob takes the other $0.4N$ qubits. We can immediately show that:

$$D_\rightarrow(\rho_{II}) \leq -2(\lambda_0^+ + \lambda_0^- + 2\sum_k \lambda_k)\log(\lambda_0^+ + \lambda_0^- + 2\sum_k \lambda_k) \tag{6.49}$$

since for Bob transferring one qubit to the environment, we obtain undistillable state ρ_{N-1} and $D_\leftrightarrow(\rho_{N-1}) = 0$ which obviously implies $D_\rightarrow(\rho_{N-1}) = 0$. It is noticeable that even for a large macroscopic system with $N \to \infty$:

$$D_\rightarrow(\rho_{II}) \leq -2(\lambda_0^+ + \lambda_0^- + 2\sum_k \lambda_k)\log(\lambda_0^+ + \lambda_0^- + 2\sum_k \lambda_k). \tag{6.50}$$

It can be easily shown that with the same method it is possible to achieve an upper bound on one-way quantum channel capacity $Q_\rightarrow$ which is a subject of analysis in the next chapter.

Chapter 7

Quantum channels

7.1 Types of quantum channel capacities

Quantum channel capacity $Q(\Lambda)$ of a channel Λ is a measure of reliability of a channel in transmitting quantum information from a sender to the receiver and has its roots in classical coding theorem by Shannon [151, 152] who analyzed transmission of classical information over noiseless and noisy channels respectively. We focus in this section on recalling the most fundamental approach to defining the quantum version of this concept [9, 10, 125].

Namely, let us define a quantum source [9, 10] $\Omega = (\mathscr{H}_s, \Gamma)$ generating a sequence $\Gamma = \{\rho_s^1, \rho_s^2, \ldots, \rho_s^n\}$ where the state ρ_s^1 acts on $\mathscr{H}_s$, ρ_s^2 acts on $\mathscr{H}_s^{\otimes 2}$ and ρ_s^n on $\mathscr{H}_s^{\otimes n}$ respectively. Then, the entropy of a source Ω is defined as:

$$S(\Omega) = \limsup_{n\to\infty} \frac{S(\rho_s^{(n)})}{n} \tag{7.1}$$

A coding protocol (or scheme) consists of a sequence of trace-preserving encoding maps $\mathscr{E}_n$ and respectively, decoding maps $\mathscr{D}_n$:

$$\mathscr{E}_n : \mathscr{B}(\mathscr{H}_s^{\otimes n}) \to \mathscr{B}(\mathscr{H}_c^{\otimes n}) \tag{7.2}$$

$$\mathscr{D}_n : \mathscr{B}(\mathscr{H}_o^{\otimes n}) \to \mathscr{B}(\mathscr{H}_s^{\otimes n}) \tag{7.3}$$

The code space $\mathscr{H}_c^{\otimes n}$ is a space of a code $\mathscr{C}_n$ onto which the initial states are encoded in a direct analogy to the classical space of codewords. Further, a channel $\Lambda^{\otimes n}$ acts on the encoded state and produce a state on the $\mathscr{H}_o^{\otimes n}$ which will be finally decoded by $\mathscr{D}_n$ to a state on $\mathscr{H}_s^{\otimes n}$ [Fig. 7.1].

.

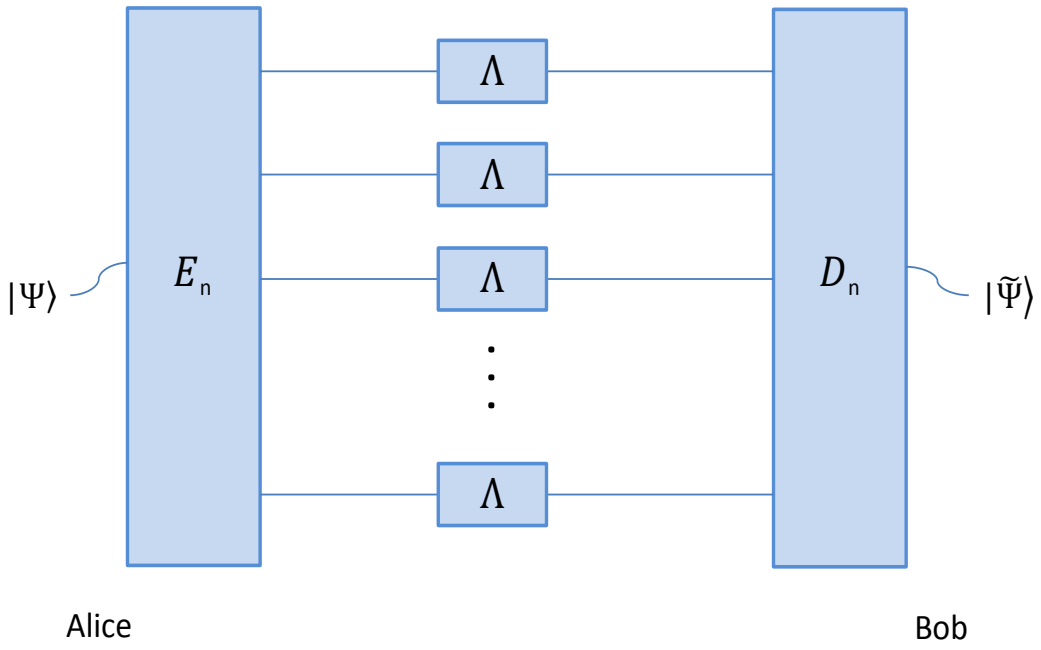

Fig. 7.1 Alice encodes her state with an encoding operation $\mathscr{E}_n$ which generates a state $|\Psi\rangle \in \mathscr{C}_n$ of a code $\mathscr{C}_n$, that she sends through n uses of the channel Λ. Then Bob applies decoding operation to decode the state $|\tilde{\Psi}\rangle$ with high fidelity. The rate of the code $\mathscr{C}_n$ is $R = \frac{1}{n}\log\dim\mathscr{C}_n$ and the quantum capacity of a quantum channel Λ is an optimal rate over all possible codes.

As observed, the model of a coding scheme is in direct analogy to the classical coding theorem, where a message sent by a sender Alice is firstly encoded (it can be performed on multiple copies of the message in parallel) by her, then sent via a noisy channel which introduces some errors to the encoded information and at the final stage, it is decoded by Bob who tries to retrieve an original message.

Basing on the definition of the encoding and decoding operations, one can define the (n,ε)-code as such a coding scheme which meets the following condition for the fidelity:

$$\min_{|\phi\rangle\in\mathscr{H}_s^{\otimes n}} F(|\phi\rangle\langle\phi|, \mathscr{D}_n \circ \Lambda^{\otimes n} \circ \mathscr{E}_n(|\phi\rangle\langle\phi|)) \geq 1-\varepsilon \tag{7.4}$$

The rate of the code is defined as:

$$R = \frac{1}{n}\log dim\mathscr{H}_s^{\otimes n} \tag{7.5}$$

The source Ω can be sent reliably over a quantum channel Λ if there exists a coding scheme so that:

$$\lim_{n\to\infty} \min_{|\phi\rangle\in\mathscr{H}_s^{\otimes n}} F(|\phi\rangle\langle\phi|, \mathscr{D}_n \circ \Lambda^{\otimes n} \circ \mathscr{E}_n(|\phi\rangle\langle\phi|)) = 1 \tag{7.6}$$

and we call the rate R for transmission over the channel Λ achievable if there exists a sequence of subspaces $\mathscr{H}_n$ in $\mathscr{H}_c^{\otimes n}$ such that:

$$R = \lim_{n\to\infty} \sup \frac{\log dim\mathscr{H}_n}{n} \tag{7.7}$$

Then, the quantum capacity of the quantum channel [9, 10] (called also *the subspace transmission capacity of a quantum channel*) is defined as a supremum over all achievable rates R of all possible codes on the input states which is in analogy to definitions of distillable entanglement and quantum key:

$$Q(\Lambda) = sup\{R : R\, achievable\}. \tag{7.8}$$

Intuitively it responses to the question: how many qubits can we sent faithfully through n uses of the channel (where the inputs can be entangled)? It is worth mentioning the alternative approach to this definition of a quantum channel capacity which is based on entanglement transmission over the channel. Namely, the alternative definition of the rate $\widetilde{R}$ is built on the entanglement fidelity definition:

$$\widetilde{R} = \max_{\rho_n\in\mathscr{B}(\mathscr{H}_s^{\otimes n})} \{S(\rho_n) : F_e(\rho, \mathscr{D}_n \circ \Lambda^{\otimes n} \circ \mathscr{E}_n) \geq 1-\varepsilon\} \tag{7.9}$$

where the entanglement fidelity F_e is defined for a bipartite system where one part of the system is sent through the channel Λ:

$$F_e(\rho,\Lambda) = F(|\Psi\rangle\langle\Psi|,(I\otimes\Lambda)(|\Psi\rangle\langle\Psi|)) \tag{7.10}$$

where $|\Psi\rangle$ is a purification of ρ and F_e is not dependant on the choice of this purification. The rate $\widetilde{R}$ is achievable for the channel Λ if there exists a source Ω (and entropy $S(\Omega)$) that can be sent reliably via Λ channel, i.e. $\lim_{n\to\infty} F_e(\rho_n, \mathscr{D}_n \circ \Lambda^{\otimes n} \circ \mathscr{E}_n) = 1$.

The quantum channel capacity defined as a supremum over the aforementioned achievable rates $\widetilde{R}$ is also called *the entanglement transmission capacity of a quantum channel* $\widetilde{Q}(\Lambda)$. It is proved that both quantities are equal [9]:

$$Q(\Lambda) = \widetilde{Q}(\Lambda) \tag{7.11}$$

If the transmission process is assisted by a classical communication between parties Alice and Bob we talk about either one-way quantum channel capacity $Q_{\rightarrow}(\Lambda)$ (one direction communication) or two-way quantum channel capacity $Q_{\leftrightarrow}(\Lambda)$ (bidirectional communication) (or zero-way when no classical communication is exchanged between the parties).

The above definitions of quantum channel capacities reflects the process of transmission of quantum states through the channel, however, due to the very definitions endowed with infinities, they are not operationally very useful for direct estimation of the quantities. Therefore, of a great importance are alternative definitions or bounds on the quantum channel capacities.

In particular, the quantum capacity of a quantum channel can be defined in terms of coherent information which is one of the best known definitions of the quantum capacity. It can be formulated by means of the coherent information even when the communication is assisted by one-way or two-way classical communication between Alice and Bob:

Theorem 7.1.1 *[48, 49] Let $\Lambda : \mathscr{B}(\mathscr{H}_A) \to \mathscr{B}(\mathscr{H}_B)$ be a quantum channel, then:*

$$Q_{\emptyset}(\Lambda) = Q_{\rightarrow}(\Lambda) = \lim_{n\to\infty} \frac{1}{n} \max_{|\psi^{A'A^n}\rangle} I_c(A'\rangle B^n)_{\omega} \tag{7.12}$$

where $|\psi^{A'A^n}\rangle$ denotes a pure state of the system $A'A^{\otimes n}$, i.e. n copies of A together with a reference system A', and the state $|\omega\rangle$ results from sending the subsystem A^n through n copies of the channel:

$$\omega = \mathbb{I}\otimes\Lambda^{\otimes n}(|\psi^{A'A^n}\rangle\langle\psi^{A'A^n}|) \tag{7.13}$$

For two-way quantum channel capacity, there holds:

$$Q_{\leftrightarrow}(\Lambda) = \lim_{n\to\infty} \frac{1}{n} \max_{|\psi^{A'A^n}\rangle, O} I_c(A'\rangle B^n)_\omega \tag{7.14}$$

with ω resulting from action of n copies of a channel Λ and two-way LOCC operations $\mathbb{O}$ on the system $A'A^n$:

$$\omega = \mathbb{O}[\mathbb{I} \otimes \Lambda^{\otimes n}(|\psi^{A'A^n}\rangle\langle\psi^{A'A^n}|)] \tag{7.15}$$

Noteworthily, a quantum channel assisted by forward communication (one-way classical communication) has the same quantum capacity as a quantum channel unassisted by such communication (zero-way classical communication) and there holds:

$$Q_{\emptyset}(\Lambda) = Q_{\rightarrow}(\Lambda) \leq Q_{\leftrightarrow}(\Lambda) \tag{7.16}$$

We also know that a single-letter formula for quantum channel capacity is in general smaller than the asymptotically regularized version:

$$Q_{\emptyset}^{(1)}(\Lambda) = Q_{\rightarrow}^{(1)}(\Lambda) = \max_{|\psi^{A'A}\rangle} I_c(A'\rangle B)_\omega \leq Q_{\emptyset}(\Lambda) \tag{7.17}$$

where we consider only one copy of A. The system AA' is in a state $|\psi^{A'A}\rangle$, over which the maximization is considered and $\omega = \mathbb{I} \otimes \Lambda(|\psi^{A'A}\rangle\langle\psi^{A'A}|)$ - the system A is sent through the channel Λ. Further, since $Q_{\emptyset}(\Lambda) = Q_{\rightarrow}(\Lambda)$, we will use the simplified notation for quantum channel capacity $Q(\Lambda)$ assuming that it can be assisted by one-way communication which does not change its value. This notation has been also used widely in literature during recent years.

In a context of this discussion, we have to recall the observation that one can analyze a classical content of the final output states after decoding the quantum states which can be performed by collective POVM operations performed by Bob. This leads us to the definition of *the classical capacity of a quantum channel* and its famous Holevo formulation:

Theorem 7.1.2 *[92, 150] The classical capacity $C(\Lambda)$ of a quantum channel Λ is:*

$$C(\Lambda) = \lim_{n\to\infty} \frac{C^{(1)}(\Lambda^{\otimes n})}{n} \tag{7.18}$$

where the Holevo capacity stands for:

$$C^{(1)}(\Lambda) = \max_{\{p_i,\rho_i\}} \chi_{\{p_i,\rho_i\}}(\Lambda) = \max_{\{p_i,\rho_i\}} [S(\sum_i p_i \Lambda(\rho_i)) - \sum_i p_i S(\Lambda(\rho_i))] \tag{7.19}$$

with $\chi(\cdot)$ denoting the Holevo function, $\{p_i, \rho_i\}$ an ensemble of quantum signal states, $\sum_i p_i = 1$ and $p_i > 0$. Every ρ_i is an input signal state to the channel sent with probability p_i.

It is fundamental to note that the Holevo function $\chi_{\{p_i,\rho_i\}}(\Lambda)$ can be interpreted as the amount of classical information sent through the Λ channel from Alice to Bob. Alice prepares the signal states ρ_i with a priori probability p_i and sends them through the channel. Bob finally tries to recognize which signal state was sent by Alice, by means of collective measurements on his side and he analyzes classical information after his measurements.

For the Holevo capacity $C^{(1)}(\Lambda)$, it is assumed that Alice prepares the input state as a product state $\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$ with each ρ_i as a potential signal state for a single use of the channel Λ. Thus, no entanglement between the input states is allowed in this formula although Bob can apply measurements entangled on his received states. That is also the reason for consideration of more general scheme where the input states can be entangled and it results in necessity of using the regularized version of this capacity as: $C(\Lambda) = \lim_{n\to\infty} \frac{C^{(1)}(\Lambda^{\otimes n})}{n}$.

The subject of regularization of both quantities as $C(\Lambda) = \lim_{n\to\infty} \frac{C^{(1)}(\Lambda^{\otimes n})}{n}$ and $Q(\Lambda) = \lim_{n\to\infty} \frac{Q(\Lambda^{\otimes n})}{n}$ relates to the question of additivity of classical capacity and quantum capacity of quantum channels, i.e. whether $Q(\Lambda_1 \otimes \Lambda_2) = Q(\Lambda_1) + Q(\Lambda_2)$ and $C^{(1)}(\Lambda_1 \otimes \Lambda_2) = C^{(1)}(\Lambda_1) + C^{(1)}(\Lambda_2)$. The answer to this question is negative and for many years was a big open question of the quantum information theory since for classical channels the information theoretic quantities are additive, e.g. if a channel Λ_1 and Λ_2 are classical then $C^{(1)}(\Lambda_1 \otimes \Lambda_2) = C^{(1)}(\Lambda_1) + C^{(1)}(\Lambda_2)$ and in a result $C^{(1)}(\Lambda) = C(\Lambda)$.
For general quantum channels, M. Hastings proved in 2009 [84] that classical capacity of quantum channels is non-additive:

$$C^{(1)}(\Lambda_1 \otimes \Lambda_2) > C^{(1)}(\Lambda_1) + C^{(1)}(\Lambda_2) \tag{7.20}$$

and as we will see further, there are also existential proofs of this property in case of quantum channel capacity of quantum channels [153]:

$$Q(\Lambda_1 \otimes \Lambda_2) > Q(\Lambda_1) + Q(\Lambda_2) \tag{7.21}$$

It is also substantial to note that in general, there holds:

$$C(\Lambda) \geq Q(\Lambda) \tag{7.22}$$

In the following sections, we focus on the class of quantum capacities of quantum channels assisted by one-way classical communication between Alice and Bob which is directly related to the application of symmetric extendibility of quantum channels.

7.2 Simple test for quantum channel capacity

As we could observe, it has been proven [15] that there is a strong connection between entanglement distillation [17] and quantum channel capacities. No-cloning principle has been used to prove that for some region quantum depolarising channel has zero capacity even if does not destroy entanglement [26].

Following the idea [26] developing restriction on qubit depolarising channel from approximate quantum cloning we shall utilise general notion of symmetric extensions of quantum states (see [55, 56, 161]) to provide a general rule and examples of channels with zero one-way capacity. We show that every state $\rho_{AB}(\Lambda)$ which has a symmetric extension $\rho_{ABB'}$ has special featured one-way distillable entanglement $D_{\rightarrow}$ and quantum channel capacity Q according to its quantum channel implied by Jamiolkowski isomorphism.

Combining the observation from a previous chapter that any symmetric extendible state has zero one-way distillable entanglement with Choi-Jamiolkowski isomorphism between states and channels we get immediately the following:

Observation 7.2.1 *[126] A sufficient condition for quantum capacity of a given quantum channel Λ to vanish is symmetric extendibility of the state $\rho_{AB}(\Lambda)$ isomorphic to the channel.*

Proof. Proof of the above theorem is immediate and follows again from quantum entanglement monogamy (cf. [26, 30]) and the fact that the set of symmetric extendible states is closed under 1-LOCC operations. If the state ρ_{AB}, being Choi-Jamiolkowski isomorphic with the quantum channel Λ, is symmetric extendible (which means that Λ is an extendible channel) then for n copies of ρ_{AB} (isomorphic with n copies of Λ), one still gets a symmetric extendible state $\rho_{AB}^{\otimes n}$ and so $\Lambda^{\otimes n}$ is still symmetric extendible. Even if one would add any additional 1-LOCC operations between the parties engaged in the coding-encoding protocol, then the output state is still symmetric extendible (in accordance with the 1-LOCC closeness of the set of symmetric extendible states) and one still cannot achieve any singlet states from the output states so the channel capacity is zero $Q(\Lambda) = 0$.

Conversely, assume that the quantum capacity of the channel is positive $Q(\Lambda) > 0$. Then, in accordance with the definition of the quantum channel capacity, the coherent information on the output state $\rho_{AB}^{\otimes n}$ is positive and there exists a protocol, i.e. "the hashing protocol", which from the state $\rho_{AB}^{\otimes n}$ isomorphic with the channel (even in the asymptotic regime, $n \rightarrow \infty$) is able to distill k copies of singlet states $|\Psi_+\rangle\langle\Psi_+|$, for some $k > 0$. But we know that the set of symmetric extendible states is closed under 1-LOCC operations and "the hashing protocol" cannot produce k singlets from a symmetric extendible state. This implies that $\Gamma_{AB}^{n} = \rho_{AB}^{\otimes n}$ could not be symmetric extendible. The last statement holds due to the fact that

$\sigma^{\otimes n}$ is symmetric extendible if σ is symmetric extendible (for any n), as already proved in the chapter 4. □

In the following, we present a special classes of channels which are directly related to the concept of symmetric extendibility which proves a great importance of that concept for quantum channels theory.

(Anti)degradable channels

We recall now the degradable channels and anti-degradable channels [52] basing on the Stinespring dillation for a given quantum channel. We already mentioned in the introductory chapters treating of quantum channels that a channel Λ acting on a state ρ_A can be represented by a unitary operation U acting on the system in this state and ancillary system of the environment E:

$$\Lambda(\rho_A) = Tr_E[U(\rho_A \otimes |0\rangle_E\langle 0|)U^\dagger] \tag{7.23}$$

Then *the complementary channel* (or a dual channel) Λ_C acts on the environment, i.e.:

$$\Lambda_C(\rho_A) = Tr_A[U(\rho_A \otimes |0\rangle_E\langle 0|)U^\dagger]. \tag{7.24}$$

Then we call the channel Λ *degradable* if there exists another channel Λ_D which is able to transform (degrade) the channel Λ into its complementary channel Λ_C when acts on the output of that channel:

$$\Lambda_C = \Lambda_D \circ \Lambda. \tag{7.25}$$

Further, a channel Λ is anti-degradable if there exists such a channel Λ_{Ad} which transforms the complementary channel Λ_C into Λ:

$$\Lambda = \Lambda_{Ad} \circ \Lambda_C. \tag{7.26}$$

We can find an immediate relation of anti-degradability of quantum channels with symmetric extendibility:

Lemma 7.2.2 *[123] A channel Λ is anti-degradable if and only if its Choi-Jamiolkowski representation $\rho_\Lambda = \frac{1}{d}\sum_{i,j=0}^{d-1}|i\rangle\langle j| \otimes \Lambda(|i\rangle\langle j|)$ is symmetrically extendible.*

As a natural consequence of this fact, one finds that for all anti-degradable channels Λ_{Ad}, there holds $Q(\Lambda_{Ad}) = 0$. Moreover, all necessary and sufficient conditions for symmetrically extendible states hold also for anti-degradable channels isomorphic with them by means of the Choi-Jamiolkowski isomorphism.

Entanglement breaking and k-extendible channels

A special class of channels are those which always generate separable states, i.e. if Alice possesses two maximally entangled particles in a state $|\Psi_+\rangle_{AB}$ and sends one of the particles to Bob via the entanglement breaking channel Λ, then they will share a separable state in the output:

Definition 7.2.3 *[105] A channel Λ is called entanglement breaking if $\rho_{AB} = [I \otimes \Lambda]|\Psi_+\rangle\langle\Psi_+|$ is a separable state where $|\Psi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.*

It is worth mentioning that such channels have very simple Kraus representation with rank-one operators V, i.e. $\Lambda(\rho) = \sum_i V_i \rho V_i^\dagger$. Further, it can be represented in a so-called *Holevo form* :

$$\Lambda(\rho) = \sum_k R_k Tr(F_k \rho) \tag{7.27}$$

where R_k are density matrices and F_k are POVMs on ρ. In this scenario the sender Alice performs POVM measurements F_k on the state and send the outcome k via the classical channel to Bob who basing on that prepare the output state R_k. In a result, all such channels have zero two-way capacity $Q_\leftrightarrow(\Lambda_{EBreak}) = 0$. It is also noticeable that for any channel Λ and an entanglement breaking channel Λ_{EBreak} there holds:

$$Q_\leftrightarrow(\Lambda_{EBreak} \otimes \Lambda) = Q_\leftrightarrow(\Lambda) \tag{7.28}$$

which means that assistance of entanglement breaking channel does not change capacity of a quantum channel.

A next class of channels with zero two-way capacity generates bound entangled states:

Definition 7.2.4 *[106] A channel $\Lambda : M_m \longrightarrow M_n$ is binding entanglement if $\rho = [I \otimes \Lambda]P_+$ ($\rho \in \mathscr{B}(\mathbb{C}^m \otimes \mathbb{C}^n)$) is a bound entangled state.*

As we will see later, in contrary to the case of entanglement breaking channels, binding entanglement channels (for which $Q(\Lambda_{EBind}) = 0$) can activate entanglement in the assisted state. Thus, in general for this class $Q(\Lambda_{EBind} \otimes \Lambda) \neq Q(\Lambda) + Q(\Lambda_{EBind})$ (which is a an example of non-additivity of quantum channel capacities).

As already observed, quantum channels generating symmetric extendible states have zero one-way quantum channel capacities, such channels are called symmetric side channels or symmetric extendible channels:

Definition 7.2.5 *A channel Λ is called k-extendible if $\rho_{AB} = [I \otimes \Lambda]|\Psi_+\rangle\langle\Psi_+|$ is a k-extendible state where $|\Psi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.*

An example of such a channel can be $\frac{1}{2}$-erasure channel: $\Lambda_{erasure}(\rho) = \frac{1}{2}\rho + \frac{1}{2}\mathbb{I}$ generating symmetric extendible state from a singlet when one of its subsystems is sent through. Thus, in accordance with the above definitions, every entanglement breaking channel is ∞-extendible channel.

7.3 New upper bounds on one-way quantum channel capacity

The best known derivation of the one-way quantum channel capacity $Q(\Lambda)$ [18, 11] is expressed as an asymptotic regularization of coherent information (as an analogue to def. 6.1.9):

$$Q(\Lambda) = \lim_{n\to\infty} \frac{1}{n} \sup_{\rho_n} I_c(\rho_n, \Lambda^{\otimes n}) \tag{7.29}$$

with parallel use of N copies of Λ channel. Coherent information for a channel Λ and a source state σ transferred through the channel is defined as: $I_c(\sigma,\Lambda) = I^B(I\otimes\Lambda)(|\Psi\rangle\langle\Psi|)$ where Ψ is a pure state with reduction σ and coherent information of a bipartite state ρ_{AB} shared between Alice and Bob is defined as: $I^B(\rho_{AB}) = S(B) - S(AB)$. We will use further the following notation: $I^B(\rho_{AB}) = I_c(A\rangle B)$.

Motivated by the reduced quantity of the one-way distillable entanglement rate and the observation 6.1.11, we derive further the reduced version of quantum channel capacity [Fig. 7.2] and show that it is a good bound on quantum channel capacity (we remember also that $Q_\emptyset(\Lambda) = Q_\rightarrow(\Lambda)$ which is not the case for distillable entanglement):

Definition 7.3.1 *[127] For a one-way quantum channel $\Lambda_{BB'} : B(\mathscr{H}_{BB'}) \rightarrow B(\mathscr{H}_{\widetilde{B}\widetilde{B'}})$ the reduced one-way quantum channel capacity is defined as:*

$$Q^{(1)}\downarrow(\Lambda_{BB'}) = \inf_{\mathscr{U}}[Q^{(1)}(\mathscr{U}(\Lambda_{BB'})) + \Delta_Q] \tag{7.30}$$

where $\mathscr{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve after action of $\Lambda_{BB'}$ channel, i.e. $\mathscr{U}(\Lambda_{BB'}(\rho_{BB'})) = Tr_{B'}U_{BB'}\Lambda_{BB'}(\rho_{BB'})$ for some unitary $U_{BB'} : B(\mathscr{H}_{\widetilde{B}\widetilde{B'}}) \rightarrow B(\widetilde{\mathscr{H}_{\widetilde{B}\widetilde{B'}}})$. $\Delta_Q = 2\sup_{\rho_{BB'}} S(Tr_B U_{BB'}\Lambda_{BB'}(\rho_{BB'}))$ denotes the defect parameter related to increase of entropy produced by the potential transfer of B'-subsystem from Bob's side to Eve.

.

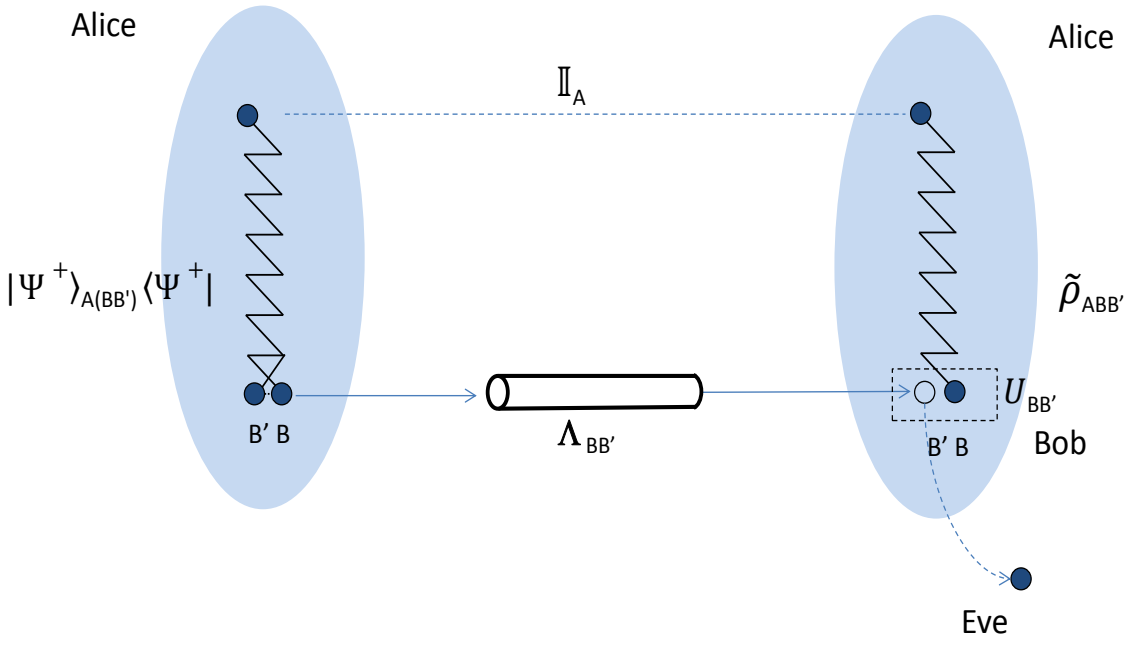

Fig. 7.2 Alice sends BB' part of the singlet state $|\Psi^+_{A(BB')}\rangle\langle\Psi^+_{A(BB')}|$ through the channel $\Lambda_{BB'}$. After this action, Bob can locally act with a unitary operation $U_{BB'}$ on BB'-subsystem and transfer the part B' to the environment possessed by Eve.

Theorem 7.3.2 *[127] For any one-way quantum channel $\Lambda_{BB'} : B(\mathscr{H}_{BB'}) \to B(\mathscr{H}_{\widetilde{B}\widetilde{B'}})$ there holds:*

$$Q(\Lambda_{BB'}) \leq Q\downarrow(\Lambda_{BB'}) \tag{7.31}$$

where $Q\downarrow(\Lambda_{BB'}) = \lim_n Q^{(1)}\downarrow(\Lambda_{BB'}^{\otimes n})/n$ denotes the reduced quantum capacity.

To prove this inequality for regularized quantum capacity and its reduced version it is sufficient to derive the below lemma for a single copy case:

Lemma 7.3.3 *For any one-way quantum channel $\Lambda_{BB'} : B(\mathscr{H}_{\mathscr{B}\mathscr{B}'}) \to \mathscr{B}(\mathscr{H}_{\widetilde{\mathscr{B}}\widetilde{\mathscr{B}'}})$ there holds:*

$$Q^{(1)}(\Lambda_{BB'}) \leq Q^{(1)}\downarrow(\Lambda_{BB'}) \tag{7.32}$$

Proof. The proof of this lemma is straightforward with application of the observation 6.1.11 that for a state $\rho_{BB'}$ maximizing coherent information on the left hand side of the observation the above formula holds also for a possible transfer of B' to the environment. It is worth recalling that an action of the unitary operator on a state does not change its entropy and in a result the coherent information for any partition of the system.□

Further, one can complete the proof of the theorem in the asymptotic regime:

Proof. To prove the inequality of Theorem 7.3.2 asymptotically it suffices to notice that statements of Lemma 7.3.3 hold also for the arbitrary chosen state $\rho_n = \rho^{\otimes n}$. Let $\rho_n^{BB'}$ be a state maximizing $Q(\Lambda_{BB'})$ as an asymptotic regularization of coherent information, i.e. $Q(\Lambda_{BB'}) = \lim_{n\to\infty}\frac{1}{n}I_c(\rho_n^{BB'}, \Lambda_{BB'}^{\otimes n})$ which one can represent as $I_c(A\rangle BB')$ for the aforementioned Choi-Jamiolkowski isomorphism between states and channels.

Basing on Observation 6.1.11, one can immediately derive for the maximizing state $\rho_n^{BB'}$: $\frac{1}{n}I_c(A\rangle BB') \leq \frac{1}{n}[I_c(A\rangle B) + 2S(\rho_n^{B'})]$ where $I_c(A\rangle B) = I_c(Tr_{B'}\rho_n^{BB'}, \Lambda_{BB'}^{\otimes n})$ and $\rho_n^{B'} = Tr_B\Lambda_{BB'}^{\otimes n}(\rho_n^{BB'})$.

However, if there exists a state σ_n^B for which $I_c(\sigma_n^{BB'}, \Lambda_{BB'}^{\otimes n}) > I_c(Tr_{B'}\rho_n^{BB'}, \Lambda_{BB'}^{\otimes n})$, then it proves that right hand side of the inequality in the lemma can be only larger than in case of the chosen state $\rho_n^{BB'}$ which completes the proof.

Finally, the subadditivity of entropy can be applied to verify that in case of the regularized one-way quantum channel capacity its defect parameter cannot be larger than $\Delta_Q = 2\sup_{\rho_{BB'}} S(Tr_B\Lambda_{BB'}(\rho_{BB'}))$, since $\sup_{\sigma_{BB'}} S(Tr_B\Lambda_{BB'}^{\otimes n}(\sigma_{BB'})) \leq \sup_{\rho_{BB'}^n} S(Tr_{B^n}\Lambda_{BB'}^{\otimes n}(\rho_{BB'}^n)) \leq n\sup_{\rho_{BB'}} S(Tr_B\Lambda_{BB'}(\rho_{BB'})$. □

Example 7.3.4 *Let us consider the graph state [88] $|\mathscr{G}\rangle$ of a $3n+1$-qubit system associated with a mathematical graph $\mathscr{G} = \{\mathscr{V}, \mathscr{E}\}$, composed of a set $\mathscr{V}$ of $3n+1$ vertices and a set $\mathscr{E}$*

of edges $\{i, j\}$ connecting each vertex i with some other j:

$$|\mathscr{G}\rangle = \bigotimes_{i,j\in\mathscr{E}} CZ_{ij}|\mathscr{G}_0\rangle \tag{7.33}$$

where $3n+1$ qubits are initialized in the product state $|\mathscr{G}_0\rangle = \bigotimes_{i\in\mathscr{V}} |\psi_i\rangle$ with $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|0_i\rangle + |1_i\rangle)$. Afterwards, one applies a maximally-entangling control-Z (CZ) gate to all pairs $\{i, j\}$ of qubits joined by an edge:

$$CZ_{ij} = |0_i0_j\rangle\langle 0_i0_j| + |0_i1_j\rangle\langle 0_i1_j| + |1_i0_j\rangle\langle 1_i0_j| - |1_i1_j\rangle\langle 1_i1_j|. \tag{7.34}$$

If Alice takes no more than n qubits from the graph system that will use to establish communication with Bob who uses other n qubits in this graph state, then the state ρ_{2n}^{AB} (with n qubits on Alice side and n qubits on Bob's side) is symmetric extendible to a state ρ_{3n}^{AB} which means that the channel isomorphic with this state has a zero capacity. A natural symmetric extension of ρ_{2n}^{AB} is a state $\rho_{3n}^{AB} = Tr_{B'}|\mathscr{G}\rangle\langle\mathscr{G}|$ resulting from tracing out an arbitrary chosen qubit B' from graph $\mathscr{G}$. However, if Alice takes n qubits and Bob takes $n+1$ qubits from the graph system, the resulting state ρ_{2n+1}^{AB} is not symmetric extendible anymore.

Now we will search for the one-way quantum channel capacity of a channel $\Lambda_{BB'}$, isomorphic due to the Choi-Jamiolkowski isomorphism, with a state $\rho_{2n+1}^{ABB'} = (I\otimes\Lambda_{BB'})|\Psi\rangle\langle\Psi|$. As above, after discarding B' 1-qubit system the state would become symmetric extendible and we obtain $Q(\Lambda_{BB'}) \leq 2$.

The power of the above results appears especially in application of Theorem 7.3.2 to any channel reducible to anti-degradable channel which Choi-Jamiolkowski representation is symmetric extendible [123] or channels reducible to degradable channels which have known capacity [154].

7.4 Super-activation of quantum channel capacities

For completeness of the presentation, we consider in this section a matter of additivity of quantum capacities whether there exist quantum channels for which: $Q(\Lambda_1\otimes\Lambda_2) > Q(\Lambda_1) + Q(\Lambda_2)$. The existential proof of non-additivity of quantum channel capacities is based on finding such two channels which have zero quantum capacities but in pair can transfer faithfully quantum information with non-zero rate. The idea [153] is based on pairing two quantum channels, namely, a symmetric extendible channel and a private binding channel.

The following powerful theorem proved in [153] is a basis for offering a positive answer to this question and relates a quantum privacy concept with quantum channel capacity:

Theorem 7.4.1 *For any quantum channel Λ, there holds:*

$$Q_{ss}(\Lambda) = \sup_{\Lambda_{sym}} Q(\Lambda \otimes \Lambda_{sym}) \geq \frac{1}{2} P(\Lambda) \tag{7.35}$$

where Λ_{sym} is any symmetric extendible channel.

For capacity $Q_{ss}(\Lambda)$ of quantum channels Λ assisted with unlimited supply of symmetric extendible channels Λ_{sym}, there holds:

Theorem 7.4.2 *[154] For all channels $\Lambda : \mathscr{B}(\mathscr{H}_{A'}) \to \mathscr{B}(\mathscr{H}_B)$:*

$$Q_{ss}(\Lambda) = Q_{ss}^{(1)}(\Lambda) = \sup_{|\psi_{AA'CD}\rangle} I_c(A\rangle BC)_\omega \tag{7.36}$$

where $\omega = \mathbb{I}_{ACD} \otimes \Lambda(|\psi_{AA'CD}\rangle\langle\psi_{AA'CD}|)$ with optimization over all states $|\psi_{AA'CD}\rangle$ invariant under permutation of C and D.

It is worth mentioning that for any channel Λ: $Q_{ss}(\Lambda) \geq Q(\Lambda)$.

The quantum channel used in the proof of the non-additive inequality is an example of zero-capacity quantum channel with positive privacy (an example of a binding channel generating private bound entangled states), i.e. the four-dimensional private channel Λ_H [104] and is paired with a $1/2$-erasure channel $\Lambda_{erasure}$ which leaves the input state ρ unchanged with probability $\frac{1}{2}$ and generates a maximally mixed stated otherwise, i.e. $\Lambda_{erasure}(\rho) = \frac{1}{2}\rho + \frac{1}{2}\mathbb{I}$.

The channel Λ_H has as an input a tensor product of two qubits and has the following Kraus matrices M_k (in Kraus representation: $\Lambda_H(\rho) = \sum_k M_k \rho M_k^\dagger$ and $\sum_k M_k M_k^\dagger = \mathbb{I}$):

$$\{\sqrt{\frac{q}{2}}\mathbb{I} \otimes |0\rangle\langle 0|, \sqrt{\frac{q}{2}}\sigma_Z \otimes |1\rangle\langle 1|, \sqrt{\frac{q}{4}}\sigma_Z \otimes \sigma_Y, \sqrt{\frac{q}{4}}\mathbb{I} \otimes \sigma_X, \sqrt{1-q}\sigma_X \otimes X_0, \sqrt{1-q}\sigma_Y \otimes X_1\} \tag{7.37}$$

where $q = \frac{\sqrt{2}}{1+\sqrt{2}}$ and $\sigma_X, \sigma_Y, \sigma_Z$ stand for Pauli matrices and:

$$X_0 = \begin{pmatrix} \frac{1}{2}\sqrt{2+\sqrt{2}} & 0 \\ 0 & \frac{1}{2}\sqrt{2-\sqrt{2}} \end{pmatrix}, X_1 = \begin{pmatrix} \frac{1}{2}\sqrt{2-\sqrt{2}} & 0 \\ 0 & \frac{1}{2}\sqrt{2+\sqrt{2}} \end{pmatrix} \tag{7.38}$$

The private capacity $P(\Lambda_H)$ of this channel is lower bounded by 0.02 as follows [104]:

$$I(X;B) - I(X;E) \geq 1 - q\log q - (1-q)\log(1-q) > 0.02 \tag{7.39}$$

which in result gives also a bound on the quantum capacity of this private channel assisted with a symmetric extendible erasure channel: $Q(\Lambda_H \otimes \Lambda_{erasure}) > 0.01$. This clearly indicates non-additivity of quantum channel capacity and proves a great importance of a concept of symmetric extendibility for a theory of quantum channels.

Chapter 8

Quantum privacy

8.1 Quantum private states and secret key

The concepts of quantum privacy and quantum secret key have their roots in classical communication theory and classical cryptography which have a long tradition. Many classical quantities in this discipline, in similarity to classical channels theory, are redefined to a quantum version.

In a classical and quantum realm, *a secret key* shared between two parties Alice and Bob allows them to perform private communication over a public channel. A public channel denotes possibility of accessing the communication by other parties, e.g. an adversary Eve who tries to attack cryptographically their communication and overhear their messages. Thus, whenever Alice and Bob start with a state ρ_{AB}, one can always consider its extension to the third adversary party Eve ρ_{ABE} who can try to influence the state by operations on her side.

Thus, in the ideal scenario, the secret key shared between Alice and Bob is decoupled from Eve's system in a state ρ_E and is used by Alice and Bob to encode a message in cryptographically secure way. Then the extended state representing a classical key has a form:

$$\rho_{ABE}^{(d)} = (\sum_{i=1}^{d} \frac{1}{d} |ii\rangle_{AB}\langle ii|) \otimes \rho_E \tag{8.1}$$

It is so-called ccq-state, i.e. a classical-classical-quantum state.

Quantum states, from which one can extract secret key, are called private states or p-dits [96, 103, 48–51]. As we can observe in the following definition, the private states have a characteristic singlet-like key part and the shield part:

Definition 8.1.1 *[103] A private state or a p-dit is a state* $\gamma_{ABA'B'} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_{A'} \otimes \mathscr{H}_{B'})$ *(for dimensions* $d_A = d_B = d$*):*

$$\gamma_{ABA'B'} = \frac{1}{d} \sum_{i,j=0}^{d-1} |ii\rangle_{AB}\langle jj| \otimes U_i \rho_{A'B'} U_j^{\dagger} \tag{8.2}$$

where the arbitrary state of a subsystem A'B' (a shield) is $\rho_{A'B'}$ *and* U_i *are unitary operators. For* $d = 2$*, the state is called a p-bit.*

In this case, Alice and Bob can achieve a secret key from the key part (AB part) of the state. The shield protects in some sense the secure correlations between Alice and Bob from unwanted influence of the adversary party Eve. In a trivial scenario, the shield can vanish and the private state shared between Alice and Bob is just a maximally entangled state $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$.

In analogy to distillation of quantum entanglement, one can formulate distillation of a private state [96, 103] from a given state ρ_{AB} which could be finally a resource for extraction of a classical secret key [Fig. 8.1].

In the following we find a formal definition of the process of p-dit distillation from any quantum state:

Definition 8.1.2 *[103] For a bipartite state* $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ *consider a sequence* P_n *of LOCC operations such that* $P_n(\rho_{AB}^{\otimes n}) = \rho_n$ *where* $\rho_n \in \mathscr{B}(\mathscr{H}_A^{(n)} \otimes \mathscr{H}_B^{(n)})$*. Then the set* $\mathscr{P} = \bigcup_{n=1}^{\infty} \{P_n\}$ *is called a p-dit distillation protocol of the state* ρ_{AB} *if:*

$$\lim_{n\to\infty} \|\rho_n - \gamma_{d_n}\| = 0. \tag{8.3}$$

with a p-dit γ_{d_n} *which key part is of dimension* $d_n \times d_n$*. For a chosen distillation protocol* $\mathscr{P}$*, its rate is defined as:*

$$R(\mathscr{P}) = \lim_{n\to\infty} \sup \frac{\log d_n}{n} \tag{8.4}$$

Then the distillable key of the state ρ_{AB} *is defined as:*

$$K_D(\rho_{AB}) = \sup_{\mathscr{P}} R(\mathscr{P}), \tag{8.5}$$

where supremum is over all possible distillation protocols $\mathscr{P}$*.*

We take supremum over all accessible protocols to Alice and Bob to find the most optimal one which extracts a maximal possible number of private states (if any). We can also define a rate at which a protocol is able to distill a classical secret key:

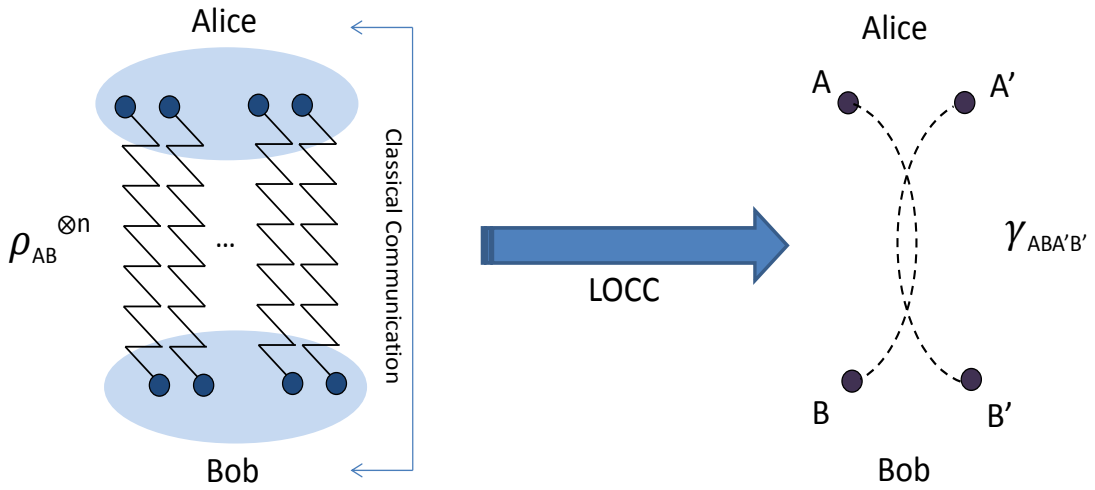

Fig. 8.1 Spatially separated Alice and Bob share n pairs of quantum states ρ_{AB}. They operate on the pairs with local quantum operations and engage also a public channel of communication, e.g. a mobile, to communicate classically. After action of this key distillation protocol, they achieve a private states $\gamma_{ABA'B'}$.

Definition 8.1.3 *[96, 103] For a tripartite state $\rho_{ABE} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_E)$ consider a sequence P_n of LOPC operations such that $P_n(\rho_{ABE}^{\otimes n}) = \rho_n$ where $\rho_n \in \mathscr{B}(\mathscr{H}_A^{(n)} \otimes \mathscr{H}_B^{(n)} \otimes \mathscr{H}_E^{(n)})$ is a ccq-state (classical-classical-quantum state) with $\dim \mathscr{H}_A^{(n)} = \dim \mathscr{H}_B^{(n)} = d_n$:*

$$\rho_n = \sum_{i,j=0}^{d_n-1} p_{ij} |ij\rangle\langle ij|_{AB} \otimes \rho_{ij}^E \tag{8.6}$$

Then the set $\mathscr{P} = \bigcup_{n=1}^{\infty} \{P_n\}$ is called a classical key distillation protocol of the state ρ_{ABE} if:

$$\lim_{n\to\infty} \|\rho_n - \rho'_{d_n}\| = 0, \tag{8.7}$$

where

$$\rho'_{d_n} = \frac{1}{d_n} \Big(\sum_{i=0}^{d_n-1} |ii\rangle_{AB}\langle ii| \Big) \otimes \rho_n^E \tag{8.8}$$

and ρ_n^E are arbitrary states in $\mathscr{B}(\mathscr{H}_E^{(n)})$.

For a chosen distillation protocol $\mathscr{P}$, its rate is defined as:

$$R(\mathscr{P}) = \lim_{n\to\infty} \sup \frac{\log d_n}{n} \tag{8.9}$$

Then the distillable classical key of the state ρ_{AB} is defined as:

$$C_D(\rho_{ABE}) = \sup_{\mathscr{P}} R(\mathscr{P}), \tag{8.10}$$

where supremum is over all possible distillation protocols $\mathscr{P}$.

There holds a fundamental equivalence between the rates of the two aforementioned protocols, namely, the distillable key of a state ρ_{AB} is equal to classical secret key of a state ρ_{AB}, which is a subject of the following theorem [96, 103]:

Theorem 8.1.4 *For any bipartite state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$, there holds:*

$$K_D(\rho_{AB}) = C_D(\rho_{AB}) \tag{8.11}$$

Since we can distill a secret key from any state which is distillable (i.e. the output state of the protocol is a singlet state), it is a trivial observation that any entanglement distillable states are key distillable states. Yet, it was not obvious for many years whether one can distill a secret key from bound entangled states (as mentioned previously, entangled PPT states from which no pure maximal entanglement can be distilled by any 2-LOCC quantum

protocol). The answer to this issue is positive and proved in [103, 97], following by the example:

Example 8.1.5 *(PPT private states) We present a bound entangled state $\gamma_{ABA'B'}$ from which one can distill a key, i.e.: $K_{\rightarrow}(\gamma_{ABA'B'}) > 0$:*

$$\gamma_{ABA'B'} = \begin{pmatrix} \frac{p}{2}(\tau_0+\tau_1) & 0 & 0 & \frac{p}{2}(\tau_1-\tau_0) \\ 0 & (\frac{1}{2}-p)\tau_0 & 0 & 0 \\ 0 & 0 & (\frac{1}{2}-p)\tau_0 & 0 \\ \frac{p}{2}(\tau_1-\tau_0) & 0 & 0 & \frac{p}{2}(\tau_0+\tau_1) \end{pmatrix} \tag{8.12}$$

The state is PPT for $p \leq \frac{1}{3}$ and $\sqrt[l]{\frac{1-p}{p}}(d-1) \geq d$, $\tau_0 = \rho_s^{\otimes l}$ and $\tau_1 = [(\rho_a+\rho_s)/2]^{\otimes l}$ are extreme Werner states, so-called hiding states, where $\rho_s = \frac{2}{d^2+d}P_{Sym}$ and $\rho_a = \frac{2}{d^2-d}P_{Asym}$. P_{Sym} and P_{Asym} denote projectors on symmetric and antisymmetric subspace respectively. It is crucial to note that to achieve security, one needs to engage large l and n to approximate a perfect key.

One-way secret key distillation

In analogy to one-way distillable entanglement $D_{\rightarrow}$, we can consider one-way distillable key $K_{\rightarrow}$ where Alice and Bob can use quantum local operations and only one-way classical communication from Alice to Bob. This is an alternative representation of $K_{\rightarrow}$ to the definition 8.1.2 with LOCC constrained only to one-way LOCC. As proved in [48–50], the one-way distillable key $K_{\rightarrow}$ for a state ρ_{AB} can be formulated as a regularization of one-copy formula $K_{\rightarrow}^{(1)}$ in terms of quantum conditional mutual information.

A one-way secret key distillation protocol is defined for cqq-states ρ_{ABE} (which is actually a broader class than a set of ccq-states) and reflects the fact that Alice starts with some POVM operations on her side and then sends the result to Bob. Thus, the state is [48]:

$$\rho_{ABE} = \sum_{x \in \mathscr{X}} P(x)|x\rangle_A\langle x| \otimes \rho_{BE}^x \tag{8.13}$$

and the protocol operates on n copies naturally:

$$\rho_{ABE}^{\otimes n} = \sum_{x^n} P^n(x^n)|x^n\rangle_A\langle x^n| \otimes \rho_{BE}^{x^n} \tag{8.14}$$

where $x^n = x_1x_2\ldots x_n$ and

$$|x^n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \ldots |x_n\rangle \tag{8.15}$$

$$\rho_{BE}^{x^n} = \rho_{BE}^{x_1} \otimes \rho_{BE}^{x_2} \otimes \ldots \rho_{BE}^{x_n} \tag{8.16}$$

The one-way secret key distillation protocol consists of (in similarity to entanglement distillation)[48]:
1. Alice acts with a quantum operation $\mathbf{T} : x^n \longrightarrow (l,m)$ on her subsystem $\rho_A^{(n)}$:

$$\mathbf{T}(\rho_A^{(n)}) = \sum_{x^n} P(C = l, K = m | A_n = x_n) |l\rangle\langle l| \otimes |m\rangle\langle m| \tag{8.17}$$

She uses the state of the system $K = m$ as a key and sends information about $C = l$ to Bob. 2. For each $C = l$ (communicated by Alice to Bob via a classical channel), there exists a quantum POVM operation D_l performed by Bob on his part: $D_l = \{D_m^{(l)}\}_{m=1}^M$. In a consequence, he achieves his version of the key K' with a probability:

$$P(K' = m | C = l, A_n = x_n) = Tr[D_m^{(l)} \rho_B^{x_n}]. \tag{8.18}$$

We call it an (n,ε)-protocol [48, 49] if it acts on n copies of the state shared between Alice and Bob and meets the following conditions (the number of possible messages sent by Alice is bounded $L \leq 2^{nF}$ for some constant F):
1.

$$P(K \neq K') \leq \varepsilon \tag{8.19}$$

2.

$$\| \sum_{m=0}^{K-1} P(K = m) |m\rangle\langle m| - \sum_{m=0}^{K-1} \frac{1}{K} |m\rangle\langle m| \|_1 \leq \varepsilon \tag{8.20}$$

3. And there exists a state ρ_0 such that for all m:

$$\| \sum_{x_n, l} P(A_n = x_n, C = l | K = m) |l\rangle\langle l| \otimes \rho_E^{x_n} - \rho_0 \|_1 \leq \varepsilon \tag{8.21}$$

The achievable rate R is possible if for all n there exist (n,ε)-protocols such that for $n \to \infty$ one gets: $\varepsilon \to 0$ an $\frac{1}{n} \log M \to R$. The one-way distillable key is then defined as [48, 49]:

$$K_{\rightarrow}(\rho) = sup\{R : R \, achievable\}. \tag{8.22}$$

These results lead I. Devetak and A. Winter to a lower bound on the one-way distillable key and more general formula for one-way key distillation in terms of quantum conditional mutual information:

Theorem 8.1.6 *[48] For any ccq-state ρ_{ABE}, there holds:*

$$K_{\rightarrow}(\rho_{ABE}) \geq I(X:B) - I(X:E) \tag{8.23}$$

As stated above, one can use [48, 49] a general tripartite state ρ_{ABE} to generate a secret key between Alice and Bob. Alice engages a particular strategy to perform a quantum measurement (POVM) described by $Q = (Q_x)_{x\in\mathscr{X}}$ which leads to: $\widetilde{\rho}_{ABE} = \sum_x |x\rangle\langle x|_A \otimes Tr_A(\rho_{ABE}(Q_x)\otimes I_{BE})$. Therefore, starting from many copies of ρ_{ABE} we obtain many copies of cqq-states $\widetilde{\rho}_{ABE}$ and we can restate the theorem defining one-way secret key $K_{\rightarrow}$:

Theorem 8.1.7 *[48] For every state ρ_{ABE}:*

$$K_{\rightarrow}(\rho) = \lim_{n\to\infty} \frac{K_{\rightarrow}^{(1)}(\rho^{\otimes n})}{n} \tag{8.24}$$

with

$$K_{\rightarrow}^{(1)}(\rho) = \max_{Q,T|X} I(X:B|T) - I(X:E|T) \tag{8.25}$$

where the maximization is over all POVMs $Q = (Q_x)_{x\in\mathscr{X}}$ and channels R such that $T = R(X)$ and the information quantities refer to the state:

$$\omega_{TABE} = \sum_{t,x} R(t|x)P(x)|t\rangle\langle t|_T \otimes |x\rangle\langle x|_A \otimes Tr_A(\rho_{ABE}(Q_x)\otimes I_{BE}). \tag{8.26}$$

The range of the measurement Q and the random variable T may be assumed to be bounded as follows: $|T| \leq d_A^2$ and $|\mathscr{X}| \leq d_A^2$ where T can be taken a (deterministic) function of $\mathscr{X}$.

8.2 Shareability of quantum correlations *vs.* quantum privacy

As already mentioned and in analogy to the case of entanglement distillation, no one-way secret key can be distilled from symmetric extendible states:

Observation 8.2.1 *If a bipartite state ρ_{AB} has a symmetric extension $\rho_{ABB'}$, so that $\rho_{ABB'} = \rho_{AB'B}$ and $\rho_{AB} = Tr_{B'}\rho_{ABB'}$, then for the one-way distillable key there holds:*

$$K_{\rightarrow}(\rho_{AB}) = 0. \tag{8.27}$$

Proof of the above theorem is immediate and follows again from quantum entanglement monogamy (cf. [26, 30]), and could be conducted in a similar way as in case of one-way

distillable entanglement. If Alice sends classical information to Bob and they distill key in the protocol, then the state can not have symmetric extension since Bob's colleague, say Brigitte (corresponding to index B') could also receive the same message from Alice and finally could share the same key with Alice too.

As all symmetric extendible state do not posses any private key, we can expect that in close neighborhood to the set of such states all other states can have only a small amount of distillable private key. That would have to be true assuming at least local continuity of private key $K_{\rightarrow}(\cdot)$ in such a neighborhood. To anylyze this subject, we start reminding an important theorem about entropic inequalities for conditional entropies of sufficiently close states in terms of a trace norm:

Theorem 8.2.2 *[4] For any two states ρ_{AB} and $\widetilde{\rho}_{AB}$ on $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$, let $\varepsilon \equiv \| \rho_{AB} - \widetilde{\rho}_{AB} \|_1$ and let d_A be the dimension of $\mathscr{H}_{\mathscr{A}}$, then the following estimate holds:*

$$|S(A|B) - S(\widetilde{A}|\widetilde{B})| \leq 4\varepsilon \log d_A + 2\eta(1-\varepsilon) + 2\eta(\varepsilon) \tag{8.28}$$

*In particular, the right hand side of (*8.28*) does not explicitly depend on the dimension of $\mathscr{H}_{\mathscr{B}}$.*

Basing one the above results and the definition of $K_{\rightarrow}$, we prove continuity of the quantity $K_{\rightarrow}^{(1)}(\rho)$ for one copy of a state ρ and further, consider behavior of the measure in the asymptotic regime:

Lemma 8.2.3 *[128] For any two states ρ and $\widetilde{\rho}$ on $\mathscr{H}_{\mathscr{A}\mathscr{B}} = \mathscr{H}_{\mathscr{A}} \otimes \mathscr{H}_{\mathscr{B}}$, let $\varepsilon \equiv \| \rho - \widetilde{\rho} \|_1$ and let d_A be the dimension of $\mathscr{H}_{\mathscr{A}}$, then the following estimate holds:*

$$|K_{\rightarrow}^{(1)}(\rho) - K_{\rightarrow}^{(1)}(\widetilde{\rho})| \leq 8\varepsilon \log d_A + 4\eta(1-\varepsilon) + 4\eta(\varepsilon) \tag{8.29}$$

Proof. One can put for the quantity $K_{\rightarrow}^{(1)}(\rho) = S(BC) - S(ABC) - S(EC) + S(AEC) = -S(A|BC) + S(A|EC)$ and respectively for $\widetilde{\rho}$ there holds $K_{\rightarrow}^{(1)}(\widetilde{\rho}) = -S(\widetilde{A}|\widetilde{BC}) + S(\widetilde{A}|\widetilde{EC})$. Further, engaging the results of (8.28) it is easy to conduct the following implications for a chain of inequalities:

$$\begin{aligned}
& |K_{\rightarrow}^{(1)}(\rho) - K_{\rightarrow}^{(1)}(\widetilde{\rho})| = \\
= \;& |[S(\widetilde{A}|\widetilde{BC}) - S(A|BC)] + [S(A|EC) - S(\widetilde{A}|\widetilde{EC})]| \\
\leq \;& |S(\widetilde{A}|\widetilde{BC}) - S(A|BC)| + |S(A|EC) - S(\widetilde{A}|\widetilde{EC})| \\
\leq \;& 2[4\varepsilon \log d_A + 2\eta(1-\varepsilon) + 2\eta(\varepsilon)]
\end{aligned}$$

□

Since it is not possible to distill any secret key by means of one-way communication and local operations from all symmetric extendible states, one can easily derive the following:

Corollary 8.2.4 *[128] For any state ρ on $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$ being in distance ε to the nearest symmetric extendible state $\widetilde{\sigma}$ in sense of a trace norm: $\varepsilon = \inf_{\sigma\in\Omega} \| \rho - \widetilde{\sigma} \|_1$ where Ω denotes a convex set of symmetric extendible states on $\mathscr{H}_{\mathscr{A}\mathscr{B}}$, there holds:*

$$K_{\rightarrow}^{(1)}(\rho) \leq 8\varepsilon \log d_A + 4\eta(1-\varepsilon) + 4\eta(\varepsilon) \tag{8.30}$$

Example 8.2.5 *As an example of application of the above corollary we will consider two states very close to one another in sense of a trace norm $\| \cdot \|_1$ from which one is symmetric extendible and the another is non-symmetric extendible. This shows that for one-copy applications the theorem can be used operationally to estimate one-way secret key rate of quantum states. Following results of [126], let us consider two arbitrary instances of a state on $\mathscr{H}_{AB} \cong \mathbb{C}^d \otimes \mathbb{C}^d$:*

$$\Upsilon(\varepsilon) = [\frac{d}{2d-1} + \varepsilon/2]P_+ + [\frac{1}{2d-1} - \frac{\varepsilon}{2(d-1)}] \sum_{i=1}^{d-1} |i\,0\rangle\langle i\,0| \tag{8.31}$$

which is non-symmetric extendible for $\varepsilon > 0$. Namely, one can put into the inequality (8.29) two states $\Upsilon(\varepsilon = 0)$ and $\Upsilon(\varepsilon > 0)$. Since for all symmetric extendible states ρ there holds: $K_{\rightarrow}^{(1)}(\rho) = 0$, then:

$$K_{\rightarrow}^{(1)}(\Upsilon(\varepsilon > 0)) \leq 8\varepsilon \log d_A + 4\eta(1-\varepsilon) + 4\eta(\varepsilon).$$

where $\varepsilon \leq \frac{2(d_A-1)}{2d_A-1}$.

It is proved [165] that in any open set of distillable states, all asymptotic entanglement measures $E(\rho)$ are continuous as a function of a single copy of ρ, even though they quantify the entanglement properties of $\rho^{\otimes N}$ in the large N limit.
However, the aforementioned theorem does not cast any light on the behavior of function $K_{\rightarrow}(\cdot)$ on the boundary of a set of all one-way distillable states adjacent to symmetric extendible states just due to the open conjecture 6.1.13. Motivated by this insight we put an open question in the following form for ε-neighborhood of symmetric extendible states having zero one-way secret key rate:

Conjecture 8.2.6 *[128] For any state ρ on $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$ being in distance ε to the nearest symmetric extendible state $\widetilde{\sigma}$ in sense of a trace norm: $\varepsilon = \inf_{\sigma\in\Omega} \| \rho - \widetilde{\sigma} \|_1$ where*

Ω *denotes a convex set of symmetric extendible states on* $\mathscr{H}_{\mathscr{A}\mathscr{B}}$*, there holds:*

$$K_{\rightarrow}(\rho) \leq 8\varepsilon \log d_A + 4\eta(1-\varepsilon) + 4\eta(\varepsilon) \tag{8.32}$$

8.3 Reduced secret key

In this section we propose a new reduced measure [127] of the one-way secret key that simplify in many cases an analysis of one-way security of quantum states.

In the following we define a modified version of the one-way secret key rate $K_{\rightarrow}$ basing on the results of [145, 96] for reduced intrinsic information and reduced entanglement measure.

Definition 8.3.1 *For the one-way secret key rate* $K_{\rightarrow}^{(1)}(\rho_{ABB'})$ *of a bipartite state* $\rho_{ABB'} \in B(\mathscr{H}_A \otimes \mathscr{H}_{BB'})$ *shared between Alice and Bob the reduced one-way secret key rate* $K_{\rightarrow}^{(1)} \downarrow (\rho_{ABB'})$ *is defined as:*

$$K_{\rightarrow}^{(1)} \downarrow (\rho_{ABB'}) = \inf_{\mathscr{U}} [K_{\rightarrow}^{(1)}(\mathscr{U}(\rho_{AB})) + \Delta_{K_{\rightarrow}}] \tag{8.33}$$

where $\mathscr{U}$ *denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve, i.e.* $\mathscr{U}(\rho_{AB}) = Tr_{B'}(I \otimes U_{BB'})\rho_{ABB'}$ *for some unitary* $U_{BB'}$*.* $\Delta_{K_{\rightarrow}} = 4S(\widetilde{\rho}_{B'})$ *denotes the defect parameter related to the increase of entropy produced by the transfer of B'-subsystem from Bob's side to Eve and* $\widetilde{\rho}_{B'} = Tr_{AB}(I \otimes U_{BB'})\rho_{ABB'}$*.*

The reduced one-way secret key rate is an upper bound on $K_{\rightarrow}$ which we prove now for every cqq-state ρ:

Theorem 8.3.2 *[127] For every cqq-state* ρ_{ABE} *there holds:*

$$K_{\rightarrow}(\rho) = \lim_{n\to\infty} \frac{K_{\rightarrow}^{(1)}(\rho^{\otimes n})}{n} \leq K_{\rightarrow} \downarrow (\rho) \tag{8.34}$$

where $K_{\rightarrow} \downarrow (\rho) = \lim_{n\to\infty} \frac{K_{\rightarrow}^{(1)} \downarrow (\rho^{\otimes n})}{N}$*.Particularly, for the identity operation* $\mathscr{U} = id$ *on Bob's side one obtains:* $K_{\rightarrow}(\rho_{ABB'}) \leq K_{\rightarrow}(\rho_{AB}) + 4S(\rho_{B'})$*.*

To prove this theorem one can start showing how the formula behaves for one-copy secret key:

Lemma 8.3.3 *For every cqq-state* ρ_{ABE} *there holds:*

$$K_{\rightarrow}^{(1)}(\rho) \leq K_{\rightarrow}^{(1)} \downarrow (\rho) \tag{8.35}$$

Proof.
Since

$$\begin{cases} I(A:B|C) = S(AC) + S(BC) - S(ABC) - S(C) \\ I(A:E|C) = S(AC) + S(EC) - S(AEC) - S(C) \end{cases}$$

then:

$$K_{\rightarrow}^{(1)}(\rho) = \max_{Q,C|A}[S(BC) - S(ABC) - S(EC) + S(AEC)]$$

To prove the thesis of this lemma it suffices to show that:

$$K_{\rightarrow}^{(1)}(\rho_{A(BB')E}) \leq K_{\rightarrow}^{(1)}(\rho_{AB(B'E)}) + 4S(B') \tag{8.36}$$

due to the fact that in case of application of $\mathscr{U}$ without discarding subsystem B' one obtains an equality. We denote by $\rho_{AB(B'E)}$ transition of B'-subsystem to the environment. Both parts (Alice and Bob) use the maximizing 1-LOCC protocol to find the secret key rate, thus, we omit further the maximization symbol for $K_{\rightarrow}^{(1)}$ which reflects a choice of the maximizing protocol by Alice and Bob, and can rewrite the inequality 8.36 as:

$$\begin{aligned} &S(BB'C) - S(ABB'C) - S(EC) + S(AEC) \leq \\ &S(BC) - S(ABC) - S(B'EC) + S(AB'EC) + 4S(B') \end{aligned}$$

It is easy to note that application of unitary operations on Bob's side do not change the inequality mainly due to the property of unitary invariancy of the von Neumann entropy. To simplify the proof one can decompose this inequality into following two inequalities:

$$\begin{cases} S(BB'C) - S(ABB'C) \leq S(BC) - S(ABC) + 2S(B') \\ S(B'EC) - S(AB'EC) \leq S(EC) - S(AEC) + 2S(B') \end{cases} \tag{8.37}$$

or equivalently considering the assumption that the initial state is of cqq-type and 'A' represents classical distribution $\{p_i\}$ we can rewrite the first inequality into the form:

$$\begin{aligned} &S(\sum_i p_i \rho_i^{BB'C}) - H(p_i) - \sum_i p_i S(\rho_i^{BB'C}) - S(\sum_i p_i \rho_i^{BC}) \\ &+H(p_i) + \sum_i p_i S(\rho_i^{BC}) \leq 2S(B') \end{aligned}$$

and similarly for the second inequality which gives in result a more compact structure:

$$\begin{cases} \chi(\sum_i p_i \rho_i^{BB'C}) - \chi(\sum_i p_i \rho_i^{BC}) \leq 2S(B') \\ \chi(\sum_i p_i \rho_i^{B'EC}) - \chi(\sum_i p_i \rho_i^{EC}) \leq 2S(B') \end{cases}$$

However, the above was proved in Observation 2.7.1 about the Holevo function [127] that completes the proof. □

Finally, we will extend this result in the asymptotic regime proving Theorem 8.3.2:

Proof. To prove Theorem 8.3.2 it suffices to notice that (8.35) holds under 1-LOCC and an arbitrary chosen $\mathscr{U}$ for any $\rho_n = \rho^{\otimes n}$. Moreover, existence of the defect parameter $\Delta_{K_\rightarrow}$ enables regularization of the reduced one-way secret rate since in the asymptotic regime after application of unitary operations on Bob side one can apply subadditivity of entropy to estimate entropy of the transferred B' part which implies $K_\rightarrow(\rho_{ABB'}) \leq K_\rightarrow(\rho_{AB}) + 4S(\rho_{B'})$. □

It is interesting that our results reflect E-nonlockability of the secret key rate [34] which means that the rate cannot be locked with information on Eve's side.

Monogamy of entanglement has been used to prove that for some region the quantum depolarizing channel has zero capacity even if does not destroy entanglement [26] which is a particular application of symmetric extendibility of states to evaluation of the quantum channel capacity. The following examples will show application of the concept:

Example 8.3.4 *As an example of application of Theorem 8.3.2 we present a state which after discarding a small B' part on Bob's side becomes a symmetric extendible state [126]. This example is especially important since the presented state does not possess [127] any symmetric extendible component in its decomposition for symmetric and non-symmetric parts, thus, one cannot use the method [122] to find an upper bound on $K_\rightarrow$ by means of linear optimization. Let us consider a bipartite quantum state shared between Alice and Bob on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B \cong \mathbb{C}^{d+2} \otimes \mathbb{C}^{d+2}$:*

$$\rho_{AB} = \frac{1}{2}\begin{bmatrix} \Upsilon_{AB} & 0 & 0 & \mathscr{A} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathscr{A}^\dagger & 0 & 0 & \Upsilon_{AB} \end{bmatrix} \tag{8.38}$$

where $\mathscr{A}$ is an arbitrary chosen operator so that ρ_{AB} represents a correct quantum state. This matrix is represented in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ held by Alice and Bob and possess a canonical maximally-entangled state structure. Whenever one party (Alice or Bob) measures the state, the state decoheres and off-diagonal elements vanish which leads to a symmetric extendible state [126]:

$$\Upsilon_{AB} = \frac{d}{2d-1} P_+ + \frac{1}{2d-1} \sum_{i=1}^{d-1} |i\,0\rangle\langle i\,0| \tag{8.39}$$

from which no entanglement nor secret key can be distilled by means of 1-LOCC [55, 56, 122, 126]. Therefore, applying Theorem 8.3.2 one derives $K_{\rightarrow}(\Upsilon_{AB}) = 0$ *and* $K_{\rightarrow}(\rho_{AB}) \leq K_{\rightarrow}\downarrow(\rho_{AB}) = 4$.

Example 8.3.5 *Let us consider again the graph state [88]* $|\mathscr{G}\rangle = \bigotimes_{i,j\in\mathscr{E}} CZ_{ij}|\mathscr{G}_0\rangle$ *of a* $3n+1$*-qubit system associated with a mathematical graph* $\mathscr{G} = \{\mathscr{V},\mathscr{E}\}$*, composed of a set* $\mathscr{V}$ *of* $3n+1$ *vertices and a set* $\mathscr{E}$ *of edges* $\{i,j\}$ *connecting each vertex i with some other j: where* $3n+1$ *qubits are initialized in the product state* $|\mathscr{G}_0\rangle = \bigotimes_{i\in\mathscr{V}} |\psi_i\rangle$ *with* $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|0_i\rangle + |1_i\rangle)$.

If Alice takes no more than n qubits from the graph system that will use to establish communication with Bob who uses other n qubits in this graph state, then they will be not able by any means to set secure one-way communication. This results from the fact that the state ρ_{2n}^{AB} *(with n qubits on Alice side and n qubits on Bob's side) is symmetric extendible to a state* ρ_{3n}^{AB} *which means that* $K_{\rightarrow}(\rho_{2n}^{AB}) = 0$*. A natural symmetric extension of* ρ_{2n}^{AB} *is a state* $\rho_{3n}^{AB} = Tr_{B'}|\mathscr{G}\rangle\langle\mathscr{G}|$ *resulting from tracing out an arbitrary chosen qubit B' from graph* $\mathscr{G}$*. However, if Alice takes n qubits and Bob takes* $n+1$ *qubits from the graph system, the resulting state* ρ_{2n+1}^{AB} *is not symmetric extendible anymore. Exemplary, for* $n = 2$ *this state has spectral representation:*

$$\rho_{2n+1}^{AB} = \frac{1}{2}(|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|) \tag{8.40}$$

where $|\phi_0\rangle = |0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle$, $|\phi_1\rangle = |0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle$ *and* $\{|0\rangle_A = |00-01-10-11\rangle_A, |1\rangle_A = |00+01+10-11\rangle_A, |0\rangle_B = |001+010+100-111\rangle_B, |1\rangle_B = |000-011-101-110\rangle_B\}$*. This state is isomorphic to a qubit bipartite state and meets the condition [123, 124] for* $\mathbb{C}^2\otimes\mathbb{C}^2$ *Bell-diagonal states to be symmetric extendible:* $4\sqrt{det(\rho_{AB})} \geq Tr(\rho_{AB}^2) - \frac{1}{2}$*. One can easily show the isomorphism of* ρ_{2n+1}^{AB} *for any n with a qubit bipartite state structure (8.40). Thus, for one-way secret key of the state there holds:* $K_{\rightarrow}(\rho_{2n+1}^{AB}) \leq K_{\rightarrow}\downarrow(\rho_{2n+1}^{AB}) = 4$*, since after discarding one qubit B' on Bob's side his system would become symmetric extendible.*

Dual picture for one-way distillable entanglement and private information.

Our results for one-way secret key and quantum channel capacity lead immediately to similar reduced formula for private information and one-way entanglement distillation quantities.

The private capacity [50, 51] $P(\Lambda)$ of a quantum channel is equal to regularization of private information:

$$P(\Lambda) = \lim_{n\to\infty} \frac{P^{(1)}(\Lambda^{\otimes n})}{n} \tag{8.41}$$

where a single-letter formula is:

$$P^{(1)}(\Lambda) = \max_{X,\rho_x^A}(I(X,B) - I(X,E)) \tag{8.42}$$

with maximization over classical random variables X and input quantum states ρ_x^A depending on the value of X.

Absorbing T into X variable in Theorem 8.1.7[1] leads to definitions for private information and private capacity [51], thus, following Lemma 7.3.3, we can derive an upper bound on private information and private capacity via their reduced counterparts:

Definition 8.3.6 *[127] For a one-way quantum channel $\Lambda_{BB'} : B(\mathscr{H}_{BB'}) \to B(\mathscr{H}_{\widetilde{B}\widetilde{B'}})$ the reduced private information is defined as:*

$$P^{(1)} \downarrow (\Lambda_{BB'}) = \inf_{\mathscr{U}}[P^{(1)}(\mathscr{U}(\Lambda_{BB'})) + \Delta_P] \tag{8.43}$$

where $\mathscr{U}$ denotes unitary operations on Bob's system with a possible transfer of subsystems from Bob to Eve, i.e. $\mathscr{U}(\Lambda_{BB'}(\rho_{BB'})) = Tr_{B'}U_{BB'}\Lambda_{BB'}(\rho_{BB'})$. $\Delta_P = 4\sup_{\rho_{BB'}} S(Tr_B U_{BB'}\Lambda_{BB'}(\rho_{BB'}))$ denotes the defect parameter related to increase of entropy produced by the transfer of B'-subsystem from Bob's side to Eve.

Theorem 8.3.7 *[127] For a one-way quantum channel $\Lambda_{BB'} : B(\mathscr{H}_{BB'}) \to B(\mathscr{H}_{\widetilde{B}\widetilde{B'}})$ there holds:*

$$P(\Lambda_{BB'}) \leq P \downarrow (\Lambda_{BB'}) \tag{8.44}$$

where $P \downarrow (\Lambda_{BB'}) = \lim_n P \downarrow^{(1)} (\Lambda_{BB'}^{\otimes n})/n$ denotes the reduced private capacity.

The proof can be conducted in analogy to Theorem 7.3.2 and Lemma 7.3.3, however, for regularization of reduced private information it is crucial to derive the below lemma for a one-copy case:

Lemma 8.3.8 *[127] For every one-way quantum channel $\Lambda_{BB'} : B(\mathscr{H}_{BB'}) \to B(\mathscr{H}_{\widetilde{B}\widetilde{B'}})$ there holds:*

$$P^{(1)}(\Lambda_{BB'}) \leq P^{(1)} \downarrow (\Lambda_{BB'}) \tag{8.45}$$

Proof. To prove this lemma it suffices to absorb variable T into X in Theorem 8.1.7. for the definition of private information and conduct the proof in analogy to the proof of Lemma 7.3.3 for a channel $\Lambda_{BB'}$ and a chosen state ρ sent through it. □

[1] Vide chap. Quantum Privacy.

Finally, we can state an observation about the private capacity of a quantum channel Λ being Choi-Jamiolkowski isomorphic with a symmetric extendible state ρ_{AB}, i.e. $\rho_{AB} = [\mathbb{I} \otimes \Lambda]|\Psi^+\rangle\langle\Psi^+|$, basing on the results for the secret key:

Observation 8.3.9 *If a one-way quantum channel Λ is Choi-Jamiolkowski isomorphic with a bipartite state ρ_{AB} having a symmetric extension $\rho_{ABB'}$, so that $\rho_{ABB'} = \rho_{AB'B}$ and $\rho_{AB} = Tr_{B'}\rho_{ABB'}$, then for the private capacity of this channel, there holds:*

$$P(\Lambda) = 0. \tag{8.46}$$

Proof of the above theorem is immediate and follows from the definition of the secret key. As already observed, absorbing T into X variable in Theorem 8.1.7[2] leads to definitions for private information and private capacity [51], thus, a zero secret key for a symmetric extendible state ρ_{AB} implies a zero private capacity for a channel isomorphic with this state (we have indeed a dual picture between the secret key and the private capacity be means of the Choi-Jamiolkowski isomorphism).

Alternatively, one can justify that due to the extendibility of the channel Λ isomorphic with ρ_{AB}, extendible to three parties ρ_{ABE} shared between Alice, Bob and Eve, after action of a local filter on Alice side F_A: $\widetilde{\rho}_{ABE} = [F_A \otimes \mathbb{I}_{BE}]\rho_{ABE}[F_A \otimes \mathbb{I}_{BE}]$, we get the same ensembles of states ($\mathfrak{A}_{AB}$ and $\mathfrak{A}_{AE}$) shared between the pairs: Alice and Bob, and the pair: Alice and Eve respectively. Due to additivity of the property of symmetric extendibility and the closeness of the set of symmetric extendible states under 1-LOCC, we can extend this result to the asymptotic regime for any symmetric extendible states ρ_{AB}^n. This implies the zero private capacity.

[2] Vide chap. Quantum Privacy.

Chapter 9

Quantum entanglement in time

Recent years have proved a great interest of quantum entanglement monogamy concept showing its usability in quantum communication theory, especially in domain of one-way communication and its applications to quantum secure key generation [123, 124, 122, 112, 48, 119, 126, 127]. While spatial quantum correlations and especially their non-locality became a central subject of quantum information theory and their applications to quantum computation, potentiality of application of temporal non-local correlations is poorly analyzed. The crucial issue relates to the very nature of time and temporal correlations phenomenon with their understanding within the framework of modern quantum and relativistic theories.

Non-local nature of quantum correlations in space has been accepted as a consequence of violation of local realism, expressed in Bell's theorem [12] and analyzed in many experiments [5, 70]. As an analogy for a temporal domain, violation of macro-realism [118] and Legett-Garg inequalities [117] seem to indicate non-local effects in time and are a subject of many experimental considerations [146, 6, 114, 155]. However, the open problem relates to the mathematical structures that could represent quantum states correlated in time in similarity to multipartite quantum states in space. In this chapter we analyze a variation of the consistent histories approach [77–80] with a concept of entangled histories [109, 110] built on a tensor product of projective Hilbert spaces that can be considered as a potential candidate of mathematical structures representing quantum states correlated in time. In particular, we focus on showing that entangled histories demonstrate monogamous properties reflecting the phenomenon in case of spatial quantum entanglement. It is worth mentioning that the two-state-vector formalism (TSVF) [2] brings another perspective on representation of quantum correlations in time broadly discussed in the literature.

However, it is crucial to note that in this context many 'obvious' facts about structure and behavior of spatial correlations and tensor algebra of spatial quantum states cannot be easily transferred into the temporal domain as the tensor structure of temporal correlations is richer

due to the binding evolution between instances of 'time' and the observation-measurement phenomenon that is also a subject of this chapter.

The outline of this chapter is as follows: in first section, we present the well known concepts of consistent histories approach [79] and present new concepts of entangled histories [40, 41] which are substantial for further considerations on monogamies and entanglement in time as such [130]. In the following sections, we introduce partial trace on quantum histories and show that quantum entanglement in time is monogamous for a particular history [129]. Monogamy of quantum entanglement in time for a particular history seems to be an inherent feature of quantum correlations in time and as such is the opposite to symmetric extendibility of a history in time, in similarity to monogamy of quantum entanglement in space. In the final section, the Tsirelson bound on quantum correlations in time is derived from the entangled histories [129, 130].

We believe that further research on temporal correlations and time evolution will be substantial for development of quantum information theory including applications to quantum cryptography or quantum computation but also to quantum gravity theory.

9.1 Entangled consistent histories theory

The decoherent histories theory (or consistent histories theory) has a long tradition [85–87, 77–82, 109, 110] and is built on the ground of well known and broadly applied Feynman's path integrals theory [69] for calculation of probability amplitudes of quantum processes, especially in quantum field theory or quantum electrodynamics. It is presented also as a generalization of quantum mechanics applied to closed systems such as the universe as a whole and discussed as a necessary element of future quantum gravity theory [85].

For readers interested in deepening this matter, it might be useful to refer to the literature [79, 85–87, 74]. In this section we focus on introduction to the concept of a consistent history and its recent modification, an entangled history [40, 41]. We present also a proposal of a temporal partial trace operator [130] acting on $\mathscr{C}^*$-Algebra of history operators as a tool necessary to achieve reduced histories, in similarity to a partial trace operator acting on a multipartite quantum state.

For the sake of the concept of a consistent history, it is substantial to note that for an evolving system (e.g. a non-relativistic particle being in an initial state $|\psi_0\rangle$ which evolution is governed by the Hamiltonian H), we can ask questions about the states of the system at different times $t_1 < t_2 < ... < t_n$. It could be performed during the repeating measuring process where a question at time t_x could be represented naturally by a projector P_x. The

alternatives at a given time t_x form an exhaustive orthogonal set of projectors $\{P_x^{\alpha_x}\}$ where:

$$\sum_{\alpha_x} P_x^{\alpha_x} = \mathbb{I} \tag{9.1}$$

$$P_x^{\alpha_x} P_x^{\tilde{\alpha}_x} = \delta_{\alpha_x \tilde{\alpha}_x} P_x^{\alpha_x} \tag{9.2}$$

and $\mathbb{I}$ stands for the identity operator.
Therefore, the alternative histories could be represented by the sets of alternative operators $\{P_1^{\alpha_1}\}$, $\{P_2^{\alpha_2}\}$,..., $\{P_n^{\alpha_n}\}$ at different times $t_1 < t_2 < ... < t_n$. A particular history is then represented as a tensor product $Proj(\mathscr{H}) \ni |H) = P_n^{\alpha_n} \odot P_{n-1}^{\alpha_{n-1}} \odot \ldots \odot P_1^{\alpha_1}$ ($\odot$ operation behaves here just like the tensor operation $\otimes$). This could be perceived that the system had a property $P_i^{\alpha_i}$ at time t_i [79].

We could interpret that during this process we project the global state of the system onto the n-fold tensor product $\bigodot_{i=1}^{n} P_i^{\alpha_i}$ achieving a consistent wave function which can be used to deduce probabilities of the events [130] in accordance with the Born rule.

The fundamental tool introduced in the consistent history framework which connects different times is the bridging operator [77] $\mathscr{B}(t_2,t_1)$. It is a counterpart of an unitary evolution operation having the following properties:

$$\mathscr{B}(t_2,t_1)^{\dagger} = \mathscr{B}(t_1,t_2) \tag{9.3}$$

$$\mathscr{B}(t_3,t_2)\mathscr{B}(t_2,t_1) = \mathscr{B}(t_3,t_1) \tag{9.4}$$

and can be represented for a unitary quantum evolution as $\mathscr{B}(t_2,t_1) = \exp(-iH(t_2-t_1))$ (with the evolution governed be a Hamiltonian H).

Since we assumed for a given time that $\sum_{\alpha_x} P_x^{\alpha_x} = \mathbb{I}$, for the sample space of consistent histories $|H^{\overline{\alpha}}) = P_n^{\alpha_n} \odot P_{n-1}^{\alpha_{n-1}} \odot \ldots \odot P_1^{\alpha_1} \odot P_0^{\alpha_0}$ ($\overline{\alpha} = (\alpha_n, \alpha_{n-1}, \ldots, \alpha_0)$) there holds $\sum_{\overline{\alpha}} |H^{\overline{\alpha}}) = \mathbb{I}$.

Further, the consistent histories formalism introduces the chain operator $K(|H^{\overline{\alpha}}))$ which can be directly associated with a time propagator of a given quantum process:

$$K(|H^{\overline{\alpha}})) = P_n^{\alpha_n} \mathscr{B}(t_n,t_{n-1}) P_{n-1}^{\alpha_{n-1}} \ldots \mathscr{B}(t_2,t_1) P_1^{\alpha_1} \mathscr{B}(t_1,t_0) P_0^{\alpha_0} \tag{9.5}$$

The operator $K : Proj(\mathscr{H}_{t_n} \otimes \mathscr{H}_{t_{n-1}} \otimes \ldots \otimes \mathscr{H}_{t_0}) \longrightarrow Proj(\mathscr{H}_{t_0} \to \mathscr{H}_{t_n})$ performs mapping of a history from $Proj(\mathscr{H}_{t_n} \otimes \mathscr{H}_{t_{n-1}} \otimes \ldots \otimes \mathscr{H}_{t_0})$ onto an operator performing the map $\mathscr{H}_{t_0} \to \mathscr{H}_{t_n}$ (e.g. $P = |\phi_{t_n}\rangle\langle\phi_{t_0}|$).
Equipped with this operator, one can associate a history $|H^{\alpha})$ with its weight:

$$W(|H^{\alpha})) = TrK(|H^{\alpha}))^{\dagger} K(|H^{\alpha})) \tag{9.6}$$

being by Born rule a counterpart of relative probability and can be interpreted as a probability of a history realization.

As an example, suppose that the system is in a state $|\psi_0\rangle \in \mathscr{H}$ at time t_0 and evolves to time t_2 under the bridging operator $\mathscr{B}(t_1,t_0)$, then applying the Born rule one can determine the probability that the system at time t_1 has a property P_{t_1}:

$$\begin{aligned} Pr(P_{t_1},t_1) &= \|P_{t_1}\mathscr{B}(t_1,t_0)|\psi_0\rangle\|^2 && (9.7)\\ &= \langle\psi_0|\mathscr{B}^\dagger(t_1,t_0)P_{t_1}\mathscr{B}(t_1,t_0)|\psi_0\rangle && (9.8)\\ &= Tr(\mathscr{B}^\dagger(t_1,t_0)P_{t_1}\mathscr{B}(t_1,t_0)[\psi_0]) && (9.9)\\ & && (9.10)\end{aligned}$$

where $[\psi_0] = |\psi_0\rangle\langle\psi_0|$ as discussed further.

The set of histories is coarse-grained as the alternatives are defined for chosen times, yet not for every possible time [85, 86]. It means that the set of potential histories is partitioned into the set of mutually exclusive classes called coarse-grained histories, those which are observable during the process of measurements. Coarse graining of measurements is a natural feature of "standard" quantum mechanics. The consistent histories theory describes also fine-grained histories and relations between the sets of coarse-grained and fine-grained histories, however, this is not a subject of this presentation and it does not change generality of the following conclusions.

Recent years show also an extensive discussion about a subject of so-called consistency or decoherence of allowed histories [85–87] which is directly related to the degree of interference between pairs of histories in the set of histories. The consistent histories framework assumes that the family [1] of histories is consistent, i.e. one can associate with a union of histories a weight equal to the sum of weights associated with particular histories included in the union [40, 41]. This implies the following *consistency condition* (α and β are indexes of the histories from the same history family):

$$\begin{cases} (H^\alpha|H^\beta) \equiv TrK(|H^\alpha))^\dagger K(|H^\beta)) = 0 \; for \; \alpha \neq \beta \\ (H^\alpha|H^\beta) = 0 \; or \; 1 \\ \sum_\alpha c_\alpha|H^\alpha) = \mathbb{I} \; for \; c_\alpha \in \mathbb{C} \end{cases} \tag{9.11}$$

There are different conditions for the so-called decoherence functional $TrK(|H^\alpha))^\dagger K(|H^\beta))$ discussed, including the weaker condition that $TrK(|H^\alpha))^\dagger K(|H^\beta)) \approx \delta_{\alpha\beta}P(\alpha)$ (medium decoherence and $P(\alpha)$ standing for probability of a history $|H^\alpha)$) or the linear positivity

[1] The family of consistent histories is such a set of histories $\mathscr{F} = \{|H^{\overline{\alpha}})\}_{\overline{\alpha}=(\alpha_n,\alpha_{n-1},\ldots,\alpha_0)}$ that $\sum_{\overline{\alpha}}|H^{\overline{\alpha}}) = \mathbb{I}$ and any pair of histories from the set meets the consistency condition.

condition by Goldstein and Page [75] but as observed by F. Wilczek [40, 41], it is unclear at this moment if the variants are significant.

It is helpful to assume normalization of histories with non-zero weight which enables normalization of probability distributions for history events, i.e.: $|\widetilde{H}) = \frac{|H)}{\sqrt{(H|H)}}$ [40, 41, 130].

If the observed system starts its potential history in a pure state $P_{t_0} = |\Psi_0\rangle\langle\Psi_0|$, then a consistent set of its histories create a tree-like structure (Fig. 9.1). Further, the consistency condition implies that the tree branches are mutually orthogonal.

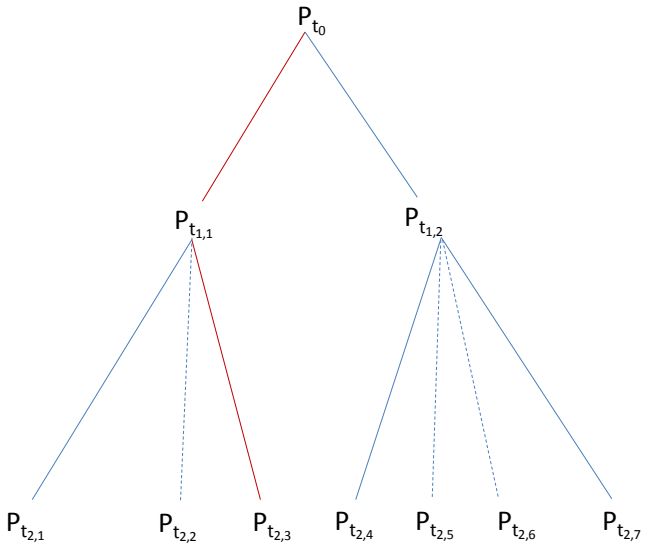

Fig. 9.1 If the observed evolution is initiated in a state $[P_{t_0}] = |\Psi_0\rangle\langle\Psi_0|$, then the history family can be represented as a tree-like structure where each branch represents a potential history. The branches are mutually orthogonal due to the consistency condition. The exemplary red branch represents history $|H) = P_{t_{2,3}} \odot P_{t_{1,1}} \odot P_{t_0}$.

The consistent history framework does not consider non-locality in space or time as such [83], however, since the space of histories spans the complex vector space, we can consider complex combinations of history vectors, i.e. any history can be represented as [40]:

$$|\Psi) = \sum_i \alpha_i |H^i) \tag{9.12}$$

where $\alpha_i \in \mathbb{C}$ and $\mathscr{F} \ni |H^i)$ represents a consistent family of histories which is actually a complex extension of the consistent histories framework and α_i parameters are normalized to give a normalized history as mentioned above.

Having defined above, the histories space can be also equipped with an inner semi-definite product [77] between any two histories $|\Psi)$ and $|\Phi)$:

$$(\Psi|\Phi) = Tr[K(|\Psi))^{\dagger}K(|\Phi))]. \tag{9.13}$$

It is fundamental to note that a history $|H^{\alpha})$ can be consistent or inconsistent (physically not realizable) basing on the associated evolution $\mathscr{B}$ of the system [79] as its consistency is verified by means of the aforementioned inner product engaging bridging operators. Thus, a temporal history is always associated with evolution and for completeness, there should be considered a pair consisting of a family of histories and the bridging operators $\{\mathscr{F},T\}$. Whenever we analyze features of a spatial pure quantum state, it is assumed that all necessary knowledge is hidden in the vector $|\psi\rangle$ so actually we analyze only one-element history objects $[\psi] = |\psi\rangle\langle\psi|$ from a perspective of a temporal local frame.

Example 9.1.1 *Let us consider now a family of inconsistent histories on three times for an evolution of a $\frac{1}{2}$-spin particle assuming that the bridging operator is trivial, i.e. $\mathscr{B} = \mathbb{I}$:*

$$\begin{aligned}
|H^0) &= [z^-]\odot\mathbb{I}\odot\mathbb{I}\\
|H^1) &= [z^+]\odot[x^+]\odot[z^+]\\
|H^2) &= [z^+]\odot[x^+]\odot[z^-]\\
|H^3) &= [z^+]\odot[x^-]\odot[z^+]\\
|H^4) &= [z^+]\odot[x^-]\odot[z^-]
\end{aligned} \tag{9.14}$$

with the operators projecting e.g. on the spin up in z-direction: $[z^+] = (1+\sigma_3)/2$ etc. Then clearly the consistency condition is not kept as:

$$\begin{aligned}
(H^1|H^3) &= Tr(K(|H^1))^{\dagger}K(|H^3))) \\
&= Tr\frac{1+\sigma_1}{2}\frac{1+\sigma_3}{2}\frac{1-\sigma_1}{2}\frac{1+\sigma_3}{2}\frac{1+\sigma_3}{2}\\
&= \frac{1}{16}Tr(1+\sigma_1+i\sigma_2+\sigma_3)(1-\sigma_1-i\sigma_2+\sigma_3)\\
&= \frac{1}{4}\neq 0
\end{aligned} \tag{9.15}$$

Example 9.1.2 *We consider also, as an example, histories of a decaying particle [41]. For this example, we assume that the particle decays emitting a photon either at time t_1 with a probability amplitude α or at time t_2 with a probability amplitude β.*

In case of emitting the photon at time t_1, an auxiliary system associated with the particle will change its state from $|0\rangle$ to $|1\rangle$. If the particle decays at t_2 time, then the auxiliary system changes its state from $|0\rangle$ to $|2\rangle$.

We additionally assume a trivial ($\mathscr{B} = \mathbb{I}$) evolution for both systems otherwise. Thus the history state for such a bipartite system consisting of the particle P and the auxiliary system A can be represented as:

$$|H_{PA}) = \alpha|D_{t_1}) \otimes |1) + \beta|D_{t_2}) \otimes |2) \tag{9.16}$$

with the local histories for the auxiliary system A:

$$\begin{aligned} |1) &= [1] \odot [1] \odot \ldots \odot [1] \odot \underbrace{[1]}_{t_1} \odot [0] \ldots \odot [0] \\ |2) &= [2] \odot [2] \odot \ldots \odot \underbrace{[2]}_{t_2} \odot [0] \odot [0] \ldots \odot [0] \end{aligned} \tag{9.17}$$

We will measure then at some time $t > t_2$ the auxiliary system A in a basis $\{|\phi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, post-selecting on $\mathbb{P} = |\phi_1\rangle\langle\phi_1|$ and tracing out the auxiliary system afterwards. Then the remaining particle would be in a history state:

$$|H_P) = \alpha|D_{t_1}) + \beta|D_{t_2}) \tag{9.18}$$

9.2 Towards monogamy of quantum entanglement in time

We consider in this section a concept of entanglement in time basing on the entangled consistent histories framework. In particular, we discuss monogamous character of quantum entanglement in time for a particular history in similarity to monogamy of quantum entanglement in case of a spatial singlet, leaving a general discussion for all classes of histories and allowable evolutions as a subject of further research.

Since the algebra of histories with $\odot$ operation is a form of tensor algebra, it inherits the properties of a standard tensor algebra with $\otimes$ operation and all mathematical questions valid for vectors representing spatial correlations are mathematically valid for temporal correlations although not necessarily having similar physical interpretation [130].

Quantum entanglement for spatial correlations shared between two parties A and B, say Alice and Bob, denotes that the state $\rho_{AB} \in \mathscr{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ of their bipartite system cannot be represented as a convex combination $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$ (which represents a separable state). The maximally entangled state of a bipartite system shared between Alice and Bob in

space, so-called singlet, is represented as $|\Psi_{AB}\rangle = \frac{1}{\sqrt{d}}\sum_i |ii\rangle$. For the sake of spatial quantum entanglement, it is crucial to define the reductions of multipartite states and their extensions. To find a reduced state ρ_A of a local state possessed e.g. by Alice, it is necessary to trace out Bob's system from the bipartite state ρ_{AB} which is performed by the partial trace operation:

$$\rho_A = Tr_B \rho_{AB} = \sum_i \langle i_B|\rho_{AB}|i_B\rangle \tag{9.19}$$

where the operation can be performed in a computational basis $|i_B\rangle$ of B-subsystem.

We will conduct further a similar reasoning for reductions of entangled histories, defining an operation of a partial trace over chosen times of a particular history state.

Now, it is substantial to note that any history $|Y) = F_n \odot \ldots \odot F_0$ can be extended to $I \odot Y$ as identity I represents a property that is always true and does not introduce additional knowledge about the system. Conversely, if one considers reduction of a history to smaller number of time frames, then information about the past and future of the reduced history is lost. Let us consider the potential history of the physical system $|Y_{t_n \ldots t_0}) = F_n \odot F_{n-1} \odot \ldots \odot F_2 \odot F_1 \odot F_0$ on times $\{t_n \ldots t_0\}$, then at time t_1 the reduced history is $|Y_{t_1}) = F_1$. That was the trivial case of factorizable history, in analogy to factorizable quantum states in space, e.g. for $|\phi_{ABE}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle \otimes |\phi_E\rangle$, the reduction over E results in $|\phi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$. To find reductions over complex superpositions of histories, it is necessary to define a partial trace operator over a history.

In analogy to partial trace for spatial quantum states, we introduced in [130] a partial trace operation on a history state in accordance with general rules of calculating partial traces on tensor algebras:

Definition 9.2.1 *For a history $|Y_{t_n \ldots t_0})$ acting on a space $\mathscr{H} = \mathscr{H}_{t_n} \otimes \cdots \otimes \mathscr{H}_{t_0}$, a partial trace over times $\{t_j \ldots t_{i+1} t_i\}$ $(j \geq i)$ is:*

$$Tr_{t_j \ldots t_{i+1} t_i} |Y_{t_n \ldots t_0})(Y_{t_n \ldots t_0}| = \sum_{k=1}^{\dim \mathscr{F}} (e_k|Y_{t_n \ldots t_0})(Y_{t_n \ldots t_0}|e_k) \tag{9.20}$$

where $\mathscr{F} = \{|e_k)\}$ creates an orthonormal consistent family of histories on times $\{t_j \ldots t_{i+1} t_i\}$ and the strong consistency condition for partial histories holds for base histories, i.e. $(e_i|e_j) = Tr[K(|e_i))^\dagger K(|e_j))] = \delta_{ij}$.

We proposed further a general form of maximally entangled history in similarity to a singlet state of a bipartite system $|\Psi_+\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N} |i\rangle \otimes |i\rangle$, $2 \leq N < \infty$:

Proposition 9.2.2 *[130] A history state 'maximally entangled' in time is represented by:*

$$|\Psi) = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |e_i) \odot |e_i), \; 2 \leq N < \infty \tag{9.21}$$

with a trivial bridging operator I and $\{|e_i)\}$ *creating an orthonormal consistent histories family.*

It is important to note that one can always employ such a bridging operator that $|\Psi)$ could become intrinsically inconsistent which means it would be dynamically impossible [79], thus, an identity bridging operator is associated with the above state.

Further, one could also introduce τGHZ and τW states substantial for studies of multipartite correlations and their applications (e.g. for secret key generation, quantum algorithms or spin networks) in analogy to spatial $|GHZ\rangle$ and $|W\rangle$ states with trivial bridging operators:

$$\begin{cases} |\tau GHZ) = \frac{1}{\sqrt{2}}(|e_0)^{\odot N} + |e_1)^{\odot N}) \\ |\tau W) = \frac{1}{\sqrt{N}}(|e_1) \odot |e_0) \odot \cdots \odot |e_0) + \\ |e_0) \odot |e_1) \odot \cdots \odot |e_0) + \cdots + |e_0) \odot |e_0) \odot \cdots \odot |e_1)) \end{cases} \tag{9.22}$$

Example 9.2.3 *Let us consider as an example potential entangled histories of a spin-*$\frac{1}{2}$ *particle at three times* $\{t_3, t_2, t_1\}$ *evolving trivially by* $\mathscr{B} = \mathbb{I}$*. In the following, we present an exemplary family of entangled history states which span a space of potential histories:*

$$\begin{aligned} |H^1) &= \sqrt{2}([z^+] \odot [x^+] \odot [z^+] + [z^-] \odot [x^-] \odot [z^+]) \\ |H^2) &= \sqrt{2}([z^-] \odot [x^+] \odot [z^+] + [z^+] \odot [x^-] \odot [z^+]) \\ |H^3) &= \sqrt{2}([z^+] \odot [x^+] \odot [z^-] + [z^-] \odot [x^-] \odot [z^-]) \\ |H^4) &= \sqrt{2}([z^-] \odot [x^+] \odot [z^-] + [z^+] \odot [x^-] \odot [z^-]) \end{aligned} \tag{9.23}$$

If we consider a state $|\Phi) = \frac{1}{\sqrt{2}}|H^1) + \frac{1}{\sqrt{2}}|H^2)$*, then a particle, measured at time* t_1 *and having a spin up in a direction* z^+*, can evolve within the history* $|H^1)$ *with probability* $P(|H^1)) = \frac{1}{2}$ *and be in the history* $|H^2)$ *with probability* $P(|H^2)) = \frac{1}{2}$*.*
Noteworthily, one can also find in the space of histories $\mathscr{S} = span\{|H^1), |H^2), |H^3), |H^4)\}$

the following GHZ-like vector [40] (normalized for $|\alpha|^2+|\beta|^2=1$):

$$\begin{aligned}|\Psi) &= \frac{\alpha}{\sqrt{2}}|H^1)+\frac{\alpha}{\sqrt{2}}|H^2)+\frac{\beta}{\sqrt{2}}|H^3)+\frac{\beta}{\sqrt{2}}|H^4)\\ &= \alpha[z^+]\odot[z^+]\odot[z^+]+\beta[z^-]\odot[z^-]\odot[z^-]\end{aligned} \tag{9.24}$$

It is worth mentioning that recently [40, 41] the concept of Bell-like tests have been proposed for experimental analysis of entangled histories. We further consider the Mach-Zehnder interferometer (Fig. 9.2 where $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$) to discuss the matter of monogamy of quantum entanglement in time [130].
In the following let us consider an intrinsically consistent history on times $\{t_3,t_2,t_1,t_0\}$:

$$|\Lambda) = \alpha([\varphi_{3,1}]\odot I_{t_2}\odot[\varphi_{1,1}]+[\varphi_{3,2}]\odot I_{t_2}\odot[\varphi_{1,2}])\odot[\varphi_0] \tag{9.25}$$

where α stands for the normalization factor, $[\varphi_{i,j}]=|\varphi_{i,j}\rangle\langle\varphi_{i,j}|$ and potentiality of the history means that one can construct a history observable $\widehat{\Lambda}=|\Lambda)(\Lambda|$. Now, after tracing out the time t_2, one gets the reduced history on times t_1 and t_3:

$$|\Lambda_1) = \tilde{\alpha}([\varphi_{3,1}]\odot[\varphi_{1,1}]+[\varphi_{3,2}]\odot[\varphi_{1,2}]) \tag{9.26}$$

which displays entanglement in time apparently. Noticeably, we have to show that to be in agreement with the partial trace definition and Feynman propagators' formalism [69], the history $|\Lambda_1)$ cannot be extracted from the following $|\tau GHZ)$-like state $|\Psi)$, i.e. $|\Lambda_1)(\Lambda_1|\neq Tr_{t_2}|\Psi)(\Psi|$ [130].

We stress that the history state $|\Psi)$ is also allowed in the setup of the aforementioned interferometer (Fig. 2) as a potential history:

$$|\Psi) = \gamma([\varphi_{3,1}]\odot[\varphi_{2,1}]\odot[\varphi_{1,1}]+[\varphi_{3,2}]\odot[\varphi_{2,2}]\odot[\varphi_{1,2}]) \tag{9.27}$$

We observe that the reduced history $[\varphi_{3,1}]\odot[\varphi_{1,1}]$ is correlated with $[\varphi_{2,1}]$ and not with $[\varphi_{2,2}]$. Thus, we cannot simply add the histories: $[\varphi_{3,1}]\odot[\varphi_{1,1}]+[\varphi_{3,2}]\odot[\varphi_{1,2}]$ as a reduction of $|\Psi)$ over time t_2. It would imply decorrelation with the next instance of the history in such a case, i.e. it could be always expanded to a history e.g. $[\varphi_{t_x}]\odot([\varphi_{3,1}]\odot[\varphi_{1,1}]+[\varphi_{3,2}]\odot[\varphi_{1,2}])$. This result is in agreement with the Feynman's addition rule for probability amplitudes since this scenario would mean e.g. existence of detectors in the consecutive step performing measurements of the light states.

Moreover, we can apply a similar reasoning for presenting a monogamous feature of quantum entanglement in time to the argument in sec. (3.2) *Quantum entanglement is monogamous*, where we showed that a singlet $\rho_{AB} = |\Psi^+\rangle\langle\Psi^+|$ can have only factorizable extensions of a form $\rho_{ABE} = \rho_{AB} \otimes \rho$. Imagine that for a maximally entangled history (9.2.2) $\rho_{t_1t_2} = |\Psi)(\Psi|$ on times $\{t_1, t_2\}$ there exists a purification to a history state $|H_{t_1t_2t_3t_4})$ then in accordance with the partial trace definition (9.2.1), the maximally entangled history would have to be a reduction of $|H_{t_1t_2t_3t_4})(H_{t_1t_2t_3t_4}|$, i.e. $|\Psi)(\Psi| = \sum_i (e_i| \odot I_{t_1t_2}|H_{t_1t_2t_3t_4})(H_{t_1t_2t_3t_4}|I_{t_1t_2} \odot |e_i)$ for some consistent history family $\mathscr{F} = \{|e_i)\}$ on times $\{t_3, t_4\}$ but due to the consistency condition, one gets $|\Psi)$ only if $|H_{t_1t_2t_3t_4}) = |H_{t_3t_4}) \odot |\Psi)$ (for some history $|H_{t_3t_4}) = \sum_i \gamma_i |e_i)$, where γ_i are complex numbers), otherwise the reduction would be a mixture of some consistent histories from the family. One can also observe immediately that $|\Psi)(\Psi| = \sum_i (e_i| \odot I_{t_1t_2}|H_{t_1t_2t_3t_4})(H_{t_1t_2t_3t_4}|I_{t_1t_2} \odot |e_i)$ implies that for any family base vector $|e_i)$, $|\Psi) = \gamma_i (e_i| \odot I_{t_1t_2}|H_{t_1t_2t_3t_4})$ (for some complex amplitude γ_i) and $(e_i| \odot (\Psi|\Psi') \odot |e_i) = 0$ for any orthogonal $|\Psi)$ and $|\Psi')$. Thus, $|H_{t_1t_2t_3t_4}) = \sum_i \gamma_i |e_i) \odot |\Psi)$.

In general, any extension of such a maximally entangled history is of a form $\rho_{t_1t_2t_X} = \rho_{t_X} \odot \rho_{t_1t_2}$ where $\rho_{t_X} = \sum_i \alpha_i |e_i)(e_i|$ for some consistent history family $\mathscr{F} = \{|e_i)\}$ on times t_X.

It is important to note that these considerations are related to $|\Psi)(\Psi|$ - observable and the particular history $|\Psi)$. Yet, other histories in the Mach-Zehnder interferometer are also accessible. It shows clearly a physical sense of quantum entanglement in time and further a concept of its monogamy for a particular entangled history.

Therefore, basing on the above observations, we find temporal monogamy phenomenon for a particular entangled history of similar nature to the spatial monogamy of quantum states [43]. On the ground of consistent histories approach, it implies that we cannot build a tripartite (i.e. defined on three different times) history state $\rho_{t_3t_2t_1}$ where $\rho_{t_3t_2} = \rho_{t_2t_1} = |\Psi)(\Psi|$ and $Tr_{t_1}\rho_{t_3t_2t_1} = \rho_{t_3t_2}$.

Besides the aforementioned reasoning derived from Feynman's quantum paths, one can refer to a broadly used explanation [43] for spatial monogamy of entanglement between parties ABC (or further $\{t_3, t_2, t_1\}$ for temporal correlations). As mentioned in previous section, it states that A cannot be simultaneously fully entangled with B and C since then AB would be entangled with C having a mixed density matrix that contradicts purity of the singlet state shared between A and B.

For the history spaces one can build naturally $\mathscr{C}^*$-Algebra of history operators equipped with a partial trace operation (9.20) and follow the same reasoning for entangled histories. We can summary these considerations with the following corollary about monogamy of

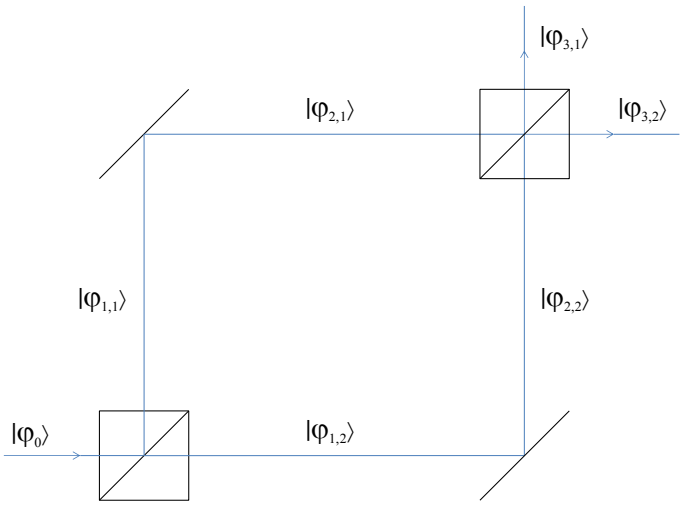

Fig. 9.2 The Mach-Zehnder interferometer with an input state $|\varphi_0\rangle$ - a vacuum state is omitted which does not change further considerations. The beam-splitters can be represented by Hadamard operation acting on the spatial modes. One can analyze the interferometer via four-times histories on times $t_0 < t_1 < t_2 < t_3$ for the interferometer process: $|\varphi_0\rangle \rightarrow \frac{1}{\sqrt{2}}(|\varphi_{1,1}\rangle + |\varphi_{1,2}\rangle) \rightarrow \frac{1}{\sqrt{2}}(|\varphi_{2,1}\rangle + |\varphi_{2,2}\rangle) \rightarrow \frac{1}{\sqrt{2}}(|\varphi_{3,1}\rangle + |\varphi_{3,2}\rangle)$.

temporal entangled histories [130]:

Corollary 9.2.4 *There does not exist any such a history* $|H) \in Proj(\mathscr{H}^{\otimes n})$ *so that for three chosen times* $\{t_3,t_2,t_1\}$ *one can find reduced histories* $|\Psi_{t_3t_2}) = \frac{1}{\sqrt{2}}(|e_0) \odot |e_0) + |e_1) \odot |e_1))$ *and* $|\Psi_{t_2t_1}) = \frac{1}{\sqrt{2}}(|e_0) \odot |e_0) + |e_1) \odot |e_1))$.

This corollary holds for any finite dimension n and also for general entangled states of the form 9.21.

As a consequence, there does not exist such a temporal observable $\widehat{\Lambda}_{A_1A_2A_3}$ so that A_1A_2 parties are maximally entangled and A_2A_3 are maximally entangled simultaneously on times $\{t_3,t_2,t_1\}$. However, in principle there exist observables of different histories that do not commute and cannot be observed at the same reference frame by an observer that are maximally entangled between A_1A_2 and A_2A_3 [131].

Further, we discuss as an example a simplified scheme for experimental generation of $|GZH)$-like state in time. Recently F. Wilczek et al. [42] have proposed an experimental test for entangled histories in laboratory using a modified Mach-Zehnder interferometer which proves a physical sense of these considerations.

Example 9.2.5 *We present below a protocol for generation of $|\tau GHZ)$ state that can be implemented in laboratory on the Mach-Zehnder interferometer with a set of detectors [42]:*

$$|\tau GHZ) = \frac{1}{\sqrt{2}}([z^+] \odot [z^+] \odot [z^+] - [z^-] \odot [z^-] \odot [z^-]) \tag{9.28}$$

We start with a bipartite system at time t_0 consisting of a spin-$\frac{1}{2}$ particle P being in a state $|\phi_0\rangle = \frac{1}{\sqrt{2}}(|z^+\rangle + |z^-\rangle)$ ($|\phi_0\rangle = |x^+\rangle$) and a reference system R, consisting of three qubits in a state $|000\rangle$ which actually can be even perceived as a clock for the process. Thus, at time t_0 the system PR is in a state (for states at each particular time, we write down the spatial state of the system in $|\cdot\rangle$ notation):

$$t_0 : \ |\Psi_{t_0}\rangle_{PR} = \frac{1}{\sqrt{2}}[(|z^+\rangle + |z^-\rangle)]|000\rangle \tag{9.29}$$

Then, at a later time t_1 we act on the system with the CNOT unitary operation where the control system is the particle and negation is performed on the first qubit of the reference system R (the CNOT operation changes the reference qubit if the controlled state is $|z^-\rangle$), basing on the state of the particle (we will repeat this action on times t_2 on the second qubit, and at t_3 on the third qubit):

$$t_1 : \ |\Psi_{t_1}\rangle_{PR} = CNOT_{PR_1} \otimes \mathbb{I}_{R_2R_3}|\Psi_{t_0}\rangle_{PR} = \frac{1}{\sqrt{2}}|z^+\rangle|000\rangle + \frac{1}{\sqrt{2}}|z^-\rangle|100\rangle \tag{9.30}$$

where $CNOT_{PR_1}$ acts on the particle and the first qubit of the reference system.
At time t_2 we act on the particle and the second qubit of the reference system achieving:

$$t_2 : \ |\Psi_{t_2}\rangle_{PR} = CNOT_{PR_2} \otimes \mathbb{I}_{R_1R_3}|\Psi_{t_1}\rangle_{PR} = \frac{1}{\sqrt{2}}|z^+\rangle|000\rangle + \frac{1}{\sqrt{2}}|z^-\rangle|110\rangle \tag{9.31}$$

Finally, at time t_3 we repeat this operation but on the particle and the third qubit of the reference system:

$$t_3 : \ |\Psi_{t_3}\rangle_{PR} = CNOT_{PR_3} \otimes \mathbb{I}_{R_1R_2}|\Psi_{t_2}\rangle_{PR} = \frac{1}{\sqrt{2}}|z^+\rangle|000\rangle + \frac{1}{\sqrt{2}}|z^-\rangle|111\rangle \tag{9.32}$$

After this step, we can measure the reference system in the computational basis $\{|000\rangle, |001\rangle, \ldots, |111\rangle\}$. If we measure the reference system projecting on $|000\rangle$ then particle has been in the history $[z^+] \odot [z^+] \odot [z^+]$. If we project it on $|111\rangle$, then the history of the particle (with which we correlate) has been in $[z^-] \odot [z^-] \odot [z^-]$.

Finally, if we measure the reference system on $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$*, the particle has been in the history state* $|\tau GHZ) = \frac{1}{\sqrt{2}}([z^+] \odot [z^+] \odot [z^+] - [z^-] \odot [z^-] \odot [z^-])$.

9.3 Tsirelson bound on Leggett-Garg Inequalities from entangled histories

For many years have been studied the violation of local realism (LR) [12] and macrorealism (MR) [118] in relation to quantum theories in experimental setups where measurement outputs are tested against violation of Bell inequalities for LR and Leggett-Garg inequalities (LGI) [117] for MR. For quantum theories, the former raises as a consequence of non-classical correlations in space while the latter as a consequence of non-classicality of dynamic evolution. Macrorealism consists of the following assumptions about the reality:

Macrorealism. A physical object is at any 'given' time at a definite quantum state.

Noninvasive measurability. It is possible to determine the state of the object without any effect on the state and the subsequent evolution.

Induction. The properties of an ensemble of quantum states are determined by the initial conditions exclusively (and not by the final conditions.)

In this section we recall the result [130] that entangled histories approach gives the same well-known Tsirelson bound [38] on quantum correlations for LGI as quantum entangled states in case of bi-partite spatial correlations for CHSH-inequalities which saturates the inequalities by quantum mechanical probability distributions.

We take a temporal version of CHSH inequality which is a modification of Legett-Garg inequalities. Then Alice performs a measurement at time t_1, choosing between two dichotomic observables $\{A_1^{(1)}, A_2^{(1)}\}$. Bob performs a measurement at time t_2 choosing between $\{B_1^{(2)}, B_2^{(2)}\}$.

Then, for such a scenario the Leggett-Garg inequality can be represented in the following form [25]:

$$S_{LGI} \equiv c_{12} + c_{21} + c_{11} - c_{22} \leq 2 \tag{9.33}$$

where $c_{ij} = \langle A_i^{(1)}, B_j^{(2)} \rangle$ stands for the expectation value of consecutive measurements performed at time t_1 and t_2.

Since history operators build a $\mathscr{C}^*$-Algebra for normalized histories from projective Hilbert spaces equipped with a well-defined inner product, one can provide reasoning about bounding the LGI purely on the space of entangled histories, and achieve the quantum bound $2\sqrt{2}$ of CHSH-inequality specific for spatial correlations.

The importance of this analytical result is due to the fact that previously it was derived basing on convex optimization methods by means of semi-definite programming [27] and by means of correlator spaces [71] (related to probability conditional distributions of consecutive events).

We will now recall the theory by B.S. Cirel'son about bounds on Bell's inequalities that is broadly used for finding quantum bounds on spatial Bell-inequalities:

Theorem 9.3.1 *[38] The following conditions are equivalent for real numbers c_{kl}, $k = 1,\ldots,m$, $l = 1,\ldots,n$:*

1. *There exists $\mathscr{C}^*$-Algebra $\mathscr{A}$ with identity, Hermitian operators $A_1,\ldots,A_m,B_1,\ldots,B_n \in \mathscr{A}$ and a state f on $\mathscr{A}$ so that for every k,l:*

$$A_kB_l = B_lA_k;\ \mathbb{I} \leq A_k \leq \mathbb{I};\ \mathbb{I} \leq B_l \leq \mathbb{I};\ f(A_kB_l) = c_{kl}. \tag{9.34}$$

2. *There exists a density matrix W such that for every k,l:*

$$Tr(A_kB_lW) = c_{kl} \text{ and } A_k^2 = \mathbb{I};\ B_l^2 = \mathbb{I}. \tag{9.35}$$

3. *There are unit vectors $x_1,\ldots,x_m,y_1,\ldots,y_n$ in a $(m+n)$-dimensional Euclidean space such that:*

$$\langle x_k, y_l\rangle = c_{kl}. \tag{9.36}$$

For a temporal setup one considers measurements $\mathbb{A} = I \odot \mathbb{A}^{(1)}$ (measurement $\mathbb{A}$ occurring at time t_1) and $\mathbb{B} = \mathbb{B}^{(2)} \odot I$, which will in an exact analogy to the proof of the above theorem for a spatial setup [130].

The history with 'injected' measurements could be represented as $|\widetilde{H}) = \alpha\mathbb{A}\mathbb{B}|H)\mathbb{A}^\dagger\mathbb{B}^\dagger$ where α stands for a normalization factor. The history observables are history state operators which are Hermitian and their eigenvectors can generate a consistent history family[40].

For an exemplary observable $A = \sum_i a_i|H_i)(H_i|$, its measurement on a history $|H)$ generates an expectation value $\langle A\rangle = Tr(A|H)(H|)$ (i.e. the result a_i is achieved with probability $|(H|H_i)|^2$) in analogy to the spatial case.

Thus, one achieves a history $|\widetilde{H})$ as a realized history with measurements and the expectation value of the history observable $\langle A\rangle$.

It is noticeable that $|\widetilde{H})$ and $|H)$ are both compatible histories, i.e. related by a linear transformation. Thus basing on these results, we can state the following lemma:

Lemma 9.3.2 *[129] For any history density matrix W and Hermitian history dichotomic observables $A_i = I \odot A_i^{(1)}$ and $B_j = B_j^{(2)} \odot I$ where $i, j \in \{1,2\}$ the following bound holds:*

$$\begin{aligned} S_{LGI} &= c_{11} + c_{12} + c_{21} - c_{22} \\ &= Tr((A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2)W) \\ &\leq 2\sqrt{2} \end{aligned} \tag{9.37}$$

Proof. The proof of this observation can be performed in similar to the spatial version of CHSH-Bell inequality under assumption that the states are represented by entangled history states and for two possible measurements $\{A_1^{(1)}, A_2^{(1)}\}$ at time t_1 and two measurements $\{B_1^{(1)}, B_2^{(1)}\}$ at time t_2. These operators can be of dimension 2×2 meeting the condition $A_i^2 = B_j^2 = I$. Therefore, they can be interpreted as spin components along two different directions. In consequence, it is well-known that the above inequality is saturated for $2\sqrt{2}$ for a linear combination of tensor spin correlation that holds also for temporal correlations. Additionally, one could also apply for this temporal inequality reasoning based on the following obvious finding [38] that holds also for the temporal scenario due to the structure of $\mathscr{C}^*$-Algebra of history operators with $\odot$-tensor operation:

$$\begin{aligned} A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2 &\leq \\ \frac{1}{\sqrt{2}}(A_1^2 + A_2^2 + B_1^2 + B_2^2) &\leq 2\sqrt{2}I \end{aligned} \tag{9.38}$$

□

Despite its long tradition, the field of entangled consistent histories becomes now a new promising arena for discussion of the entanglement phenomenon in time. It is possible mainly due to extension of the paradigm of the consistent (decoherent) histories into the realm of complex superpositions of decoherent histories allowing occurrence of the quantum entanglement between two 'potential' histories of an evolving object.

We have to recall at this point that the consistent histories framework is a 'local' theory as already emphasized by R. Griffiths [79, 80, 83] and as such is in some opposition to the modifications proposed by F. Wilczek, J. Cotler et al. and the author of this thesis. However, as already proved these modifications have a well-established physical sense [42]. This slight but of a great importance enhancement of the theory of consistent histories opens brand a new exciting research field in quantum entanglement in time. It will be of utmost meaning for further development of quantum information processing, quantum field theory and quantum gravity theory.

Chapter 10

Conclusions

Recent years have seen enormous advances in quantum information theory proving it has been well established as a basis for a concept of quantum computation and communication. They have proved also a great interest of symmetric extendibility concept showing its usability in quantum communication theory, especially in domain of one-way communication which was a subject of this PhD thesis. A natural relation between monogamy of entanglement and symmetric extendibility concept was established [55, 56, 161] with an important application to analysis of Bell inequalities for multipartite settings where some of the parties possess the same sets of measurement settings.

Much work [1, 15, 17, 16, 10, 48–50] has been performed to understand how to operate on quantum states and distill entanglement enabling quantum data processing or establish quantum secure communication between two or more parties. One of the central problems of the quantum communication field is to estimate efficiency of communication protocols establishing secure communication between involved parties or distilling quantum entanglement [145, 96, 97, 48–50, 153]. Most simple communication scenarios are those that do not use classical side channel or use it only in one-way setup. The challenge for the present theory is to determine good bounds on such quantities like the secret key rate or quantum channel capacity and distillable entanglement of a quantum state, that allow to estimate the communication capabilities. We engaged the concept of symmetric extendibility of quantum states to simplify this discussion by introduction of new upper bounds on these quantum quantities [126, 123, 124, 122, 112, 127] and new entanglement monotones, and parameters.

It seems also that symmetric extendibility is fundamental for studies on recovery and entanglement breaking channels including its neighborhood [119] as well as for such measures like squashed entanglement and quantum discord [136] or analysis of directed communication in 1D/2D spin chains [89]. Recently a great attention has been paid to the so-called k-extendible maps [136, 35, 23] and recovery maps [68, 24] where it is proved that small

value of squashed entanglement implies closeness to highly extendible states. These results and the results presented in this dissertation show importance of symmetric extendibility notion for analysis of one-way quantum communication rates and sufficiently prove importance of the notion for quantum communication theory.

In particular, the key results presented in the PhD thesis include:

- It has been proved that due to the Choi-Jamiolkowski isomorphism between quantum states and quantum channels, the convex optimization methods can be used as a quick test of non-zero quantum channel capacity. This result can be achieved in particular for quantum channels having hight entanglement transmission and having zero-way quantum capacity. We discussed symmetric extendibility in a context of quantum channel capacities and their super-activation.

- We analyzed the geometry of the convex set of symmetric extendible states having symmetric extensions of k-rank. We proved that the set is closed under action of 1-LOCC operations, and even if the parties engaged into a quantum protocol apply 1-LOCC to multiple copies of the symmetric extendible state, then they cannot go beyond the set.

- We discussed the entanglement measures and introduced new one-way entanglement monotone based on the best symmetric extendible approximation. We introduced new entanglement parameter based on relative entropy proving that it is a new upper bound on one-way distillable entanglement.

- In this thesis we provided efficient upper bounds avoiding a massive overestimation of communication rates. We considered two pairs of quantities: private capacity P, quantum one-way secret key $K_{\rightarrow}$ and one-way quantum channel capacity $Q_{\rightarrow}$, one-way distillable entanglement $D_{\rightarrow}$ providing new efficient upper bounds. We proved that in some cases the bounds explicitly show that the corresponding quantity is relatively small if compared to sender and receiver systems. The main method is again the fact that all the above quantities vanish on some classes of systems. Moreover, we introduced 'defect' parameters Δ for the reduced quantities resulting from possible transfer of sub-systems on receivers' side which are (sub)additive and hence, can be exploited in case of composite systems and regularization.

- We analyzed symmetric extendibility of composite systems introducing the extendible number notion for a quantum state as the characteristic number assessing extendibility of a quantum state.

- We analyzed the relations between symmetric extendibility and monogamy of quantum entanglement and the Bell theorem, discussing also separability of quantum states in a context of their symmetric extendibility.

- The challenge for the present quantum information theory in domain of one-way communication is to better understand behavior of all quantum states in the region of non-

symmetric extendibility and in particular in a region of non-positive coherent information [48] where no known one-way protocol for distillation of entanglement and private key exists. Inspired by these findings, we proposed further an important conjecture about distillability of all non-symmetric extendible states and analyzed behavior of a secret key rate in a neighborhood of symmetric extendible states. This would substantially simplify the full characterization of two-qubit states in terms of their privacy and distillability. In relation to this question, we analyzed Werner states in the domain of non-positive coherent information, which would indicate one-way NPT bound entangled features in the case that the conjecture was not true.

- We also studied the behavior of the private key in the neighborhood of symmetric extendible states, showing that for one copy a quantum state close to the symmetric extendible state can possess only a small number of private keys.

- We showed that the concept of monogamy of quantum entanglement can be transferred to the domain of temporal correlations and as such opens a new research area for applications of the tools presented in this thesis.

- We proved that in the paradigm of the entangled consistent histories, a particular history is monogamous in similarity to a quantum state entangled in space. Further, we derived the Tsirelson bound on the temporal Leggett-Garg inequalities basing on the entangled histories which is the first such a derivation in the literature.

The symmetric extendibility concept built on symmetry of quantum states finds out to be one of the central concept for the quantum information theory, especially in domain of one-way communication. Due to its natural relation to monogamy of quantum entanglement which is a key resource in quantum information processing, the symmetric extendibility of quantum entangled states has a chance to be one of the building blocks of further research in this area. In a context of symmetric extendibility of quantum states, future research can be focused on complete characterization of non-symmetric extendible two-qubit states and their distillability, but also on development of new entanglement measures based on the concept and analysis of symmetric extendibility of two-qudit states. As aforementioned, the symmetric extendibility is also fundamental for the theory of k-extendible channels which is now a new stream in the theory of quantum channels. For quantum privacy, it would be fundamental to develop better methods of detection of symmetric extendibility of given correlations shared between Alice and Bob. Finally, monogamy of quantum entanglement in time opens a new research field for development of the symmetric extendible concepts in domain of quantum correlations in time which now is a brand new research field.

References

[1] H.-K. Lo, S. Popescu and T. Spiller, (eds.) *Introduction in quantum information and computation*, World Scientific, (1998); J. Gruska, *Quantum Computing*, McGraw-Hill, London 1999; D. Bouwmeester, A. K. Ekert, A. Zeilinger (eds.), *The physics of quantum information : quantum cryptography, quantum teleportation, quantum computation*; Springer, New York 2000; M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge 2000; G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Röttler, H. Weinfurter, R. F. Werner, and A. Zeilinger, *Quantum information: an introduction to basic theoretical concepts and experiments.*, volume 173 of *Springer Tracts in Modern Physics*, Springer, Berlin 2001.

[2] Y. Aharonov, L. Vaidman, The two-state vector formalism of quantum mechanics, in Time in Quantum Mechanics, Springer, 369 (2002).

[3] G. Alber, R. Werner et al., Quantum Information, Springer, (2001).

[4] R. Alicki, M. Fannes, J. Phys. A **37**, L55 (2004).

[5] A. Aspect, J. Dalibard, G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).

[6] A. Asadin, C. Brukner and P. Rabl, Phys. Rev. Lett. **112**, 190402 (2014).

[7] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[8] J. Barrett, Information processing in generalized probabilistic theories, Preprint quant-ph/0508211 (2005).

[9] H. Barnum, E. Knill and M. A. Nielsen, IEEE Trans.Info.Theor. **46** 1317 (2000).

[10] H. Barnum, J. A. Smolin and B. M. Terhal, Phys. Rev. A **58**, 3496 (1998).

[11] H. Barnum, E. Knill and M. Nielsen, Preprint quant-ph/9809010 (1998).

[12] J. S. Bell, Physics **1**, 195 (1964).

[13] I. Bengtsson, K. Zyczkowski, Geometry of Quantum States, Cambridge, (2006).

[14] G. Brassard, P. Horodecki and T. Mor, IBM J. Res. Dev. **84**, 87 (2004).

[15] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters Phys. Rev. A **5**, 3824 (1996)

[16] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).

[17] C. H. Bennett et al., Phys. Rev. Lett. **76**, 722 (1996).

[18] C. H. Bennett, D. P. Di Vincenzo, J. Smolin and W. K. Wootters, Phys. Rev. A **54**, 3814 (1997).

[19] A. Berman, R. Plemmons, Nonnegative Matrices in the Mathematical Sciences, SIAM, (1994).

[20] R. Bhatia, Partial traces and entropy inequalities, Lin. Alg. and Its Appl. **370**, 125-132 (2003).

[21] R. Bhatia, Matrix Analysis, Springer, (1997).

[22] S. Boyd, L. Vanderberghe, Convex Opitmization, Cambridge (2004).

[23] F. Brandao, M. Christandl, Phys. Rev. Lett. **109**, 160502 (2012)

[24] F. G. Brandao, A. W. Harrow, J. Oppenheim and S. Strelchuk, Preprint quant-ph/1411.4921 (2014).

[25] C. Brukner, S. Taylor, S. Cheung, V. Vedral, Quantum Entanglement in Time, Preprint quant-ph/0402127, (2004).

[26] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello and J. A. Smolin, Phys. Rev. A, **57**, 2368 (1998).

[27] C. Budroni, T. Moroder, M. Kleinmann, O. Guhne, Phys. Rev. Lett. 111, 020403 (2013).

[28] P. Bush, M. Grabowski, P. J. Lathi, Operational Quantum Physics, Springer, (1995).

[29] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. 43, 4537 (2002).

[30] N. Cerf et al., Phys. Rev. A. **60**, 898 (1999).

[31] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).

[32] M. Christandl, A. Winter, IEEE Trans Inf Theory **51**, no 9, pp 3159-3165 (2005).

[33] M. Christandl and A. Winter, J. Math. Phys., 45(3), 29 (2004).

[34] M. Christland, A. Ekert et al., Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Science **4392**, 456 (2007).

[35] G. Chiribella, Theory of Quantum Computation, Communication and Cryptography 9, Springer, (2011).

[36] M. D. Choi, Can. J. Math. **24**, 520 (1972).

[37] M. D. Choi, Linear Algebra and Its Applications **10**, 285 (1975).

[38] B. S. Cirel'son, Lett. Math. Phys. **4**, 93-100 (1980).

[39] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[40] J. Cotler, F. Wilczek, Entangled Histories, Preprint quant-ph/1502.02480 (2015).

[41] J. Cotler, F. Wilczek, Bell Tests for Histories, Preprint quant-ph/1503.06458 (2015).

[42] J. Cotler, F. Wilczek et al., Experimental Test of Entangled Histories, Preprint quant-ph/1601.02943 (2016).

[43] Valerie Coffman, Joydip Kundu, William K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[44] M. Curty, M. Lewenstein, N. Lütkenhaus, Phys. Rev. Lett.**92**, 217903 (2004).

[45] B. de Finetti, Ann. Inst. H. Poincare **7**, 1 (1937).

[46] W. Dür, J. I. Cirac, Phys. Rev. A **62**, 022302 (2000).

[47] I. Devetak I, The private classical information capacity and quantum information capacity of a quantum channel, Preprint quant-ph/0304127 (2003).

[48] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).

[49] I. Devetak, A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).

[50] I. Devetak, IEEE Trans. Inform. Theory **51**, 44 (2005).

[51] I. Devetak, The private classical capacity and quantum capacity of a quantum channel, Preprint quant-ph/9809023 (1998).

[52] I. Devetak, P. Shor, Commun. Math. Phys. **256**, 287 (2005).

[53] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal and A. V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).

[54] D. P. DiVincenzo et al., Phys. Rev. Lett. **92**, 067902 (2004).

[55] A. C. Doherty, P. A. Parillo and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002) .

[56] A. C. Doherty, P. A. Parillo and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).

[57] M. J. Donald and M. Horodecki, Phys. Lett. A **264**, 257 (1999).

[58] M. J. Donald, M. Horodecki and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).

[59] W. Dur, J. I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A. **61**, 062313 (2000).

[60] W. Dür, J. I. Cirac and P. Horodecki, Phys. Rev. Lett. **93**, 020503 (2004).

[61] W. Dur, G. Vidal, J.I. Cirac, Phys. Rev. A **62**, 062314 (2000) .

[62] T. Eggeling, R. F. Werner, Phys. Rev. A **63**, 042111 (2001).

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

[64] J. Eisert, private communication.

[65] J. Eisert, P. Hyllus, O. Guehne and M. Curty, Phys. Rev. A **70**, 062317 (2004).

[66] U. Fano, Rev. Mod. Phys. **55**, 855 (1983).

[67] M. Fannes, J.T. Lewis, and A. Verbeure, Lett. Math. Phys., **15**, 255 (1988).

[68] O. Fawzi and R. Renner, Preprint quant-ph/1410.0664 (2014).

[69] R. P. Feynman, Space-time approach to non-relativistic quantum mechanics, Rev. Mod. Phys. **20**, 367 (1948).

[70] S. J. Freedman, J. F. Clauser, Phys. Rev. Lett. **28**, 938 (1972).

[71] T. Fritz, New J. Phys. 12, 083055 (2010).

[72] C. A. Fuchs and R. Schack, Preprint quant-ph/0404156 (2004).

[73] C. A. Fuchs, R. Schack, and P. F. Scudo, Phys. Rev. A **69**, 062305 (2004).

[74] M. Gell-Mann, J. B. Hartle, Phys. Rev. A **89**, 052125 (2014).

[75] S. Goldstein, D. Page, Phys. Rev. Lett. **74**, 3715 (1995).

[76] J. Gruska, Quantum Computing, McGraw-Hill, (1999).

[77] R. Griffiths, Journal of Statistical Physics 36.1-2, 219-72 (1984).

[78] R. Griffiths, Phys. Rev. Lett **70**, 2201-204 (1993).

[79] R. Griffiths, Consistent Quantum Theory, Cambridge: Cambridge UP, (2002).

[80] R. Griffiths, Consistent Quantum Measurements, Preprint quant-ph/1501.04813 (2015).

[81] R. Griffiths, Phys. Rev. A 54, 2759 (1996).

[82] R. Griffiths, R. Omn‘es, Physics Today **52**, 26-31 (1999).

[83] R. Griffiths, Private communication.

[84] M. Hastings, Nature Physics **5**, 255 (2009).

[85] J. B. Hartle, Generalizing Quantum Mechanics for Quantum Spacetime, The Quantum Structure of Space and Time: ed. by D. Gross, M. Henneaux, and A. Sevrin, World Scientific, Singapore, (2007).

[86] J. B. Hartle, Phys. Rev. A, **70**, 02210 (2004).

[87] J. B. Hartle, Phys.Rev. A, **69**, 042111 (2004).

[88] M. Hein et al., Preprint quant-ph/0602096 (2006).

[89] S. Hengl, J. Aberg and R. Renner, New J. Phys. **15**, 033025 (2013).

[90] A. S. Holevo, Coding theorems for quantum channels, Preprint quant-ph/9809023 (1998).

[91] A. S. Holevo, Probl. Inf. Transm. USRR **9**, 31-42 (1973).

[92] A. S. Holevo, IEEE Trans.Info.Theor. **44**, 269 (1998).

[93] R. L. Hudson and G. R. Moody, Z. Wahrschein. verw. Geb. **33**, 343 (1976).

[94] M. Horodecki, P. Horodecki and R.Horodecki, Phys. Rev. Lett. **85**, 433 (2000).

[95] P. Horodecki, Centr. Eur. J. Phys. **4**, 695 (2003).

[96] K. Horodecki et al., Phys. Rev. Lett. **94**, 200501 (2005).

[97] K. Horodecki et al., IEEE Trans. Inf. Theory **55**, 1898 (2009).

[98] M. Horodecki. Entanglement measures. Quantum Inf. Comp. **1**, 3 (2001).

[99] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Let. A **223**, 1 (1996).

[100] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Let. **80**, 5239 (1998).

[101] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[102] M. Horodecki, P. Horodecki and R.Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).

[103] K. Horodecki et al., Phys. Rev. Lett. **94**, 160502 (2005).

[104] K. Horodecki, L. Pankowski, M. Horodecki, P. Horodecki, IEEE Trans. Info. Theory **54**, 2621 (2008).

[105] M. Horodecki, P. W. Shor, M. B. Ruskai, Rev. Math. Phys **15**, 629 (2003).

[106] P. Horodecki et al., J.Mod.Opt. **47**, 347 (2000).

[107] L. P. Hughston, R. Jozsa, W. K. Wootters, Phys. Lett. A **183**, 14-18 (1993).

[108] P. Hyllus et al., Phys. Rev. A **72**, 012321 (2005).

[109] C. J. Isham, Journal of Math. Phys. **35**, 2157 (1994).

[110] C. J. Isham and N. Linden, Journal of Math. Phys. **35**, 5452 (1994).

[111] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).

[112] Jianxin Chen et. al, Phys. Rev. A **90**, 032318 (2014).

[113] S. Karnas, M. Lewenstein, J. Phys. A: Math. Gen. **34**, 6919 (2001).

[114] H. Katiyar et al., Phys. Rev. A **87**, 052102 (2013).

[115] K. Kraus, States, Effects and Operations, Springer, (1983).

[116] D. Kretschmann and R. F. Werner, New J. Phys. **6** 26 (2004).

[117] A. J. Leggett and A. Garg, Phys. Rev. Lett. **54**, 857 (1985).

[118] A. J. Leggett, J. Phys.: Condens. Matter **14**, R415 (2002).

[119] K. Li, A. Winter, Squashed entanglement, *k*-extendibility, quantum Markov chains, and recovery maps, Preprint quant-ph/1410.4184 (2014).

[120] L. Masanes, Phys. Rev. Lett. **97**, 050503 (2006).

[121] A. Milne, D. Jennings, S. Jevtic et al., Phys. Rev. A **90**, 1050 (2014).

[122] T. Moroder, N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).

[123] G. O. Myhr, N. Lütkenhaus, Phys. Rev. A **79**, 062307 (2009).

[124] G. O. Myhr et. al., Symmetric extensions in two-way quantum key distribution, Preprint quant-ph/0812.3607v1 (2008).

[125] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge, (2002).

[126] M. L. Nowakowski, P. Horodecki, J. Phys. A: Math. Theor. **42**, 135306 (2009).

[127] M. L. Nowakowski, P. Horodecki, Phys. Rev. A **82**, 042342 (2010).

[128] M. L. Nowakowski, J. Phys. A: Math. Theor. **49**, 385301 (2016).

[129] M. Nowakowski, Monogamy of quantum entanglement in time, Preprint quant-ph/1604.03976 (2016).

[130] M. Nowakowski, Quantum entanglement in time, American Institute of Phys. Conf. Proc.: Quantum Retrocausation III (2016).

[131] M. L. Nowakowski, In preparation.

[132] A. Peres, Quantum Theory: Concepts and Methods, Kluwer Academic Publishers, (1993).

[133] D. Petz, Prob. Th. Rel. Fields. 85 (1990).

[134] S. Popescu, D. Rohrlich, Found. Phys. **24**, 379 (1994).

[135] S. Popescu, Phys. Rev. Lett. **72**, 797 (1994).

[136] M. Piani, Hierarchy of efficiently computable and faithful lower bounds to quantum discord, Preprint quant-ph/1501.06855 (2015).

[137] M. B. Plenio and S. Virmani, An introduction to entanglement measures. Quantum Inf. Comp. **7**,1 (2006).

[138] G.A. Raggio and R.F.Werner, Helvetica Physics Acts., **62**, 980 (1989).

[139] E. M. Rains, Phys. Rev. A **60**, 179 (1999).

[140] R. Renner and S. Wolf, Advances in Cryptology - EUROCRYPT '03, Lecture Notes in Computer Science (2003).

[141] R. Quesada, A. Sanpera, Phys. Rev. A **89**, 052319 (2015).

[142] M. Pawlowski, C. Brukner, Phys. Rev. Lett. 102, 030403 (2009).

[143] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[144] S. Pironio, J. Phys. A: Math. Theor. **47**, 424020 (2014).

[145] R. Renner and S. Wolf, Advances in Cryptology - EUROCRYPT '03, Lecture Notes in Computer Science **2656**, 562 (2003).

[146] C. Robens et al., Phys. Rev. A 5, 011003 (2015).

[147] R. T. Rockafellar, Convex Analysis, Princeton Univ. Press, (1970).

[148] D. Rosset, N. Brunner et. al, Phys. Rev. Lett. **116**, 010403 (2016).

[149] W. Rudin, Analiza funkcjonalna, PWN, (2002).

[150] B. Schumacher, M. D. Westmoreland, Phys. Rev. A 56, 131 (1997).

[151] C. E. Shannon, Bell System Tech. J. **27**, 379 (1948).

[152] C. E. Shannon and W. Weaver, The Mathematical Theory of Communication, University of Illinois Press, Urbana, (1949).

[153] G. Smith and J. Yard, Science **321**, 1812 (2008).

[154] G. Smith, J. A. Smolin, A. Winter, IEEE Trans. Info. Theory **54** , 4208 (2008).

[155] A. M. Souza, I. S. Oliveira and R. S. Sarthour, New J. Phys. 13, 053023 (2011).

[156] W. F. Stinespring, Proc. Amer. Math. Soc. **6**, 211 (1955).

[157] J. Sturm, SEDUMI VERSION 1.05.2001, http://fewcal.kub.nl/sturm/software/sedumi.html.

[158] P. W. Shor, Capacities of quantum channels and how to find them, Preprint quant-ph/0304102 (2003).

[159] M. D. Schwartz, Quantum Field Theory and the Standard Model, Cambridge, (2013).

[160] E. Stormer, J. Funct. Anal. 3, 48 (1969).

[161] B. M. Terhal, A. C. Doherty and D. Schwab, Phys. Rev. Lett. **90**, (2003).

[162] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[163] V. Vedral, M. B. Plenio, M. A. Rippin and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[164] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[165] G. Vidal, On the continuity of asymptotic measures of entanglement, Preprint quant-ph/0203107 (2002).

[166] G. Vidal, J. Mod. Opt. **47**, 355 (2000).

[167] R. Werner, Physical Review A **40**, 8 (1989).

[168] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[169] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989).

[170] W. K. Wooters, W. H. Zurek, Nature **299**, 802 (1982).

[171] For instance one can propose fidelity of state according to the nearest purified extension as follows $F_{\mathscr{E}}(\rho_{AB}) = \inf_{\sigma_{AB}\in\mathscr{E}} F(\rho_{AB},\sigma_{AB}) = \inf_{\sigma_{AB}\in\mathscr{E}} |\langle\Phi_{ABB'C}|\Psi_{ABB'C}\rangle|$ where the set $\mathscr{E}$ is defined as in the above definition and both $\Phi_{ABB'C}$ and $\Psi_{ABB'C}$ is a purification of a suitable state. It can be shown that such quantity is also restricted 1-LOCC monotone.