MASARYK UNIVERSITY
FACULTY OF INFORMATICS

Quantum Entanglement

MASTER'S THESIS

Boris Ranto

Brno, 2013

Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out by my own. All sources, references and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Boris Ranto

Advisor: Colin Wilmott, M.Sc., Ph.D., prof. RNDr. Jozef Gruska, DrSc.

Acknowledgement

I would like to thank Colin Wilmott and Jozef Gruska for all the support and advice with which they provided me throughout the thesis.

Abstract

The core element of all the phenomena presented in this thesis is quantum entanglement. In order to present and outline the phenomena related to the quantum entanglement, the mathematical framework of quantum mechanics is presented at the beginning of this thesis. Afterwards, the idea of quantum entanglement along with the uniqueness of this resource and brief application of this resource are outlined. The study of entanglement of two, three and n parties with respect to the tasks of entanglement classification, entanglement detection and entanglement distillation follows in order to explore the structure of entanglement.

Keywords

Quantum mechanics, multipartite entanglement, entanglement theory, classification of entangled states, detection of entanglement, distillation of entanglement

Contents

1 Introduction & Preliminaries

This first chapter of thesis covers the very basic principles of quantum mechanics and will serve as an introduction to the topics that will be covered in this thesis. The aim of this chapter is to motivate the study of quantum mechanics for use in quantum information processing and provide reasonable background for understanding of the phenomena that is covered by this thesis.

The second chapter of this thesis will serve as an introduction to quantum entanglement that is one of the most important and interesting phenomena of quantum mechanics. The chapter also provides a discussion that suggests that thanks to quantum entanglement, the theory of quantum mechanics may not be superseded by a more standard and intuitive physical theory. At the end of the chapter a very basic entanglement manipulation protocols will be presented in order to demonstrate the power as well as a deficiency of quantum entanglement.

Afterwards, in three consecutive chapters, three very important tasks concerning the entanglement will be discussed for quantum systems of consecutively increasing complexity. These three tasks include the classification of entanglement, detection of entanglement and distillation of entanglement. Each of these tasks provides a different level of insight to the theory of quantum mechanics and in particular quantum entanglement. The task of entanglement classification provides an insight to the very basic structure of quantum entanglement. The remaining two tasks further refine the understanding of the structure of entanglement with concern to the applications of quantum entanglement that are more practical in their nature. Furthermore, the task of entanglement detection focuses on locally prepared quantum systems while the task of entanglement distillation is of a greater importance for preparation of quantum systems amongst remote parties.

However, before any quantum formalism will be presented in this thesis, a brief history of the field of quantum mechanics will be discussed in order to provide important insights to the theory of quantum mechanics and further motivate the study of this intriguing theory.

1.1 History

The field of quantum mechanics started as early as the middle of the nineteenth century when physicist Gustav Kirchhoff showed that the emitted energy of a blackbody depends solely on the temperature and the frequency of the emitted energy. The blackbody is a concept in physics and is known as both a perfect absorber and a perfect emitter in the sense that it absorbs or emits all the energy. Kirchhoff demonstrated that the emitted energy is dependent on these two quantities however, he was not successful in correctly formulating the blackbody energy emission rate. Hence, he set a challenge to all physicists to find the correct formulae for the emitted blackbody energy.

Over the coming years there were several attempts to tackle the blackbody problem, many of which turned out to be incomplete, until the problem was finally solved by Max Planck in 1900. Amazingly, as soon as Planck discovered the problem it was only a matter of hours before he derived the correct formulae for blackbody emission. While his deduction was triggered by an ingenious conjecture, he remained unsatisfied with his work and sought out an exact reason that would justify in theoretical terms the reason for his conjecture. In his workings, Planck made important assumption that energy is not continuous but rather discrete quantity. In particular, Planck stated that energy consists of quanta of energy.

Initially, Planck's explanation was not taken very seriously within physics. However, there was a physicist that became interested in the Planck's theory about the discreteness of energy and he went by name Albert Einstein. Einstein used Planck's idea to derive his seminal work on discrete properties of light, and in 1905, Einstein made very important realisation – if the light behaves as if it was made out of a quanta then perhaps it is also emitted and absorbed in that way. Einstein used this realisation to describe the photoelectric effect. This quanta of the light – the light particle – is now known as photon. The main problem with his theory was that the theory of classical electrodynamics postulated that the light is a wave. It was counterintuitive to think that something can be both a particle and a wave. This led to the phenomenon that is now known as the wave-particle duality of light.

While Einstein's explanation of the photoelectric effect provided for testable predictions, it took ten years to design an experiment that could show that his predictions were correct and hence, in the meantime his quantisation did not receive widespread support. However, Einstein found another application for quantisation within the theory of specific heats[1]. This use of the quantisation was soon supported by experiments and brought a broader audience to the quantisation debate. This eventually resulted in the Solvay Congress in 1911 where similar ideas were mooted. Here, as the second youngest physicist at the conference, Einstein gave a talk on the specific heats and offered his insights on electromagnetic radiation.

The next stop for quantisation was the model of atom. Niels Bohr, in his doctoral studies, noticed inconsistencies in one of the theories trying to describe the model of atom – Rutherford's model. In Rutherford's model, the electrons circle around a dense core. Bohr's intuition led him to the idea of quantisation of the model. Bohr suggested that electrons circle the dense core in orbits and that for an electron to switch the orbits it must overcome a quanta of energy. Following the Bohr's result, Einstein successfully connected the Bohr's model with blackbody radiation. In the same paper, Einstein also postulated that the transition between the orbits can not be determined precisely. In particular, he stated that the transition can only be determined probabilistically.

Bohr's model of atom allowed for a much more general quantum theory. Unfortunately, this task was not as simple as one might wish. While some parts of the model could be described classically, some could not be described that way. Continuous work on the theories with conjunction with Bohr's model resulted in the concepts known as the old quantum theory. The old quantum theory was simply a collection of results built around the Bohr's model of atom. The collection of the results was quite successful in explaining many experiments but suffered from inconsistencies and incompleteness. There was not a single failure as such rather a collection of little missing doubts. Moreover, the number of these doubts was overwhelming.

To overcome these obstacles and help better explain the assump-

1. The specific heat describes the relation between the change in the heat – energy – per change in the temperature.

tions that were used in the model of atom, Niels Bohr formulated the correspondence principle. Simply put, the principle states that for large systems the results of quantum theories must match the classical results. This simple principle based on the previous experience happened to be a very important building block of what is now known as the quantum mechanics.

The correspondence principle on itself was a positive start but it was not sufficient to help build a more consistent and more complete quantum theory. A group of theorists suspected that the assumption that electrons circle around a dense core in orbits might not be consistent with the rest of theory and hence, they tried to abstract from the orbits. The group eventually focused on the probabilistic transitions of the electrons in the atom core.

Two seemingly distinct quantum theories eventually made their appearance in 1925-1926. The first was offered by Heisenberg and took the approach of following the Bohr's correspondence principle to the uttermost detail. The result was a theory that was counter-intuitive on many levels. However, the theory managed to acquire several followers and hence, it was accepted by some.

While Heisenberg's theory was built around the revised Bohr's model and the absolute discreteness of the particles, the second theory was based on the wave-particle duality. Louis de Broglie proposed that if light may act as both a particle and a wave, then maybe electrons can act as both particles and waves. This idea, amongst others, led Erwin Schrödinger to formulate his own quantum theory.

Schrödinger thought about the discreteness of particles simply as if they were merely stable forms of continuous matter waves and built his theory around this intuition. The result was that there were two fundamentally different theories. Although the theories soon turned out to be mathematically equivalent, they still offered two fundamentally different explanations for their mathematics. To address this confusion, several modifications to the interpretations of both theories had to be made. Max Born changed the waves in the Schrödinger's theory to abstract probabilities of discrete particles occurring while Heisenberg postulated his uncertainty principle reducing the possibilities of even the things as fundamental as measurements. Finally, Bohr's principle of complementarity that stated that the result of the experiment must be described in classical, not quan-

tum terms made the interpretation into its more conventional form by Copenhagen interpretation of quantum mechanics.

Approximately a quarter of a century after the first Planck's realisation into the quantisation, the theory as well as the interpretation for the quantum mechanics was ready. Many, including one of the pioneers of the quantum theory – Albert Einstein, found the resulting theory and the explanations for the theory insufficient and unsatisfactory. The fact remains that the theory allowed for an explanation of many phenomenons that simply couldn't be explained without it. Further, unlikely phenomena could now be shown to be present in the theory. The phenomena that contrary to a natural intuition eventually turned out to be physically realisable. Hence, amazingly, if such quantum mechanics is to be ever superseded by a new theory, its explanations and predictions will certainly remain a very good approximation of the physics of the universe that we all live in.

1.2 Hilbert spaces

We review the mathematical properties of vector space, fundamental to the construction of the quantum mechanical framework. In particular, we will establish the concept of Hilbert space. A vector space V is a set that is closed under vector addition and scalar multiplication. The simplest example is the n-dimensional Euclidean space $\mathbb{R}^n$ where every element is represented by a list of real numbers, scalars are real numbers, addition is component-wise and scalar multiplication is multiplication on each term separately [54].

For a more general vector space, the scalars are elements of a field $\mathbb{F}$ in which case V is called a vector space over $\mathbb{F}$. Thus, the Euclidean n-dimensional space $\mathbb{R}^n$ is known as real vector space. However, we will focus on the complex vector space that is defined as a vector space over the field of complex numbers. In particular, we will focus on the complex vector spaces $\mathbb{C}^n$. A general definition of vector space follows.

Definition 1. Let $\mathbb{F}$ be a field, then set V endowed with the operation of addition $(+)$ that maps each pair (u, v) of elements of set V to an element in the set and the operation of scalar multiplication $(\cdot)$ that maps a pair of an element of field $\mathbb{F}$ and an element of set V to an

element of set V is a *vector space* if for all vectors $u, v, w \in V$ and scalars $\alpha, \beta \in \mathbb{F}$

$u + v = v + u$	Addition is commutative.
$(u + v) + w = u + (v + w)$	Addition is associative.
$0 + u = u + 0 = u$	There is an additive identity.
$u + (-u) = 0$	There is an additive inverse.
$\alpha(\beta u) = (\alpha\beta) u$	Multiplication is associative.
$(\alpha + \beta) u = \alpha u + \beta u$	Scalar sums are distributive.
$\alpha(u + v) = \alpha u + \alpha v$	Vector sums are distributive.
$1u = u$	There is a multiplicative identity.

A complex vector space $\mathbb{C}^n$ contains infinitely many vectors but as a consequence of the axiom of choice [52], $\mathbb{C}^n$ can be spanned by a finite set of vectors. In particular, $\mathbb{C}^2$ can be spanned by set of vectors $\{(1, 0), (0, 1)\}$. To limit the number of elements in such a spanning set we can impose the condition of linear independence on subsets of a vector space.

Definition 2. Let V be a vector space over field $\mathbb{F}$, a subset $S \subseteq V$ of vectors $S = \{v_1, \ldots, v_n\}$ is *linearly independent* if and only if there are no scalars $\alpha_i \in \mathbb{F}$ with at least one non-zero scalar $\alpha_i \neq 0$ such that

$$\sum_i \alpha_i v_i = 0 \tag{1.1}$$

A *basis* of the vector space V is a set $\{v_1, \ldots, v_n\} \subseteq V$ of linearly independent vectors such that it spans the vector space V

$$\{c_1 \cdot v_1 + \cdots + c_n \cdot v_n \mid c_1, \ldots c_n \in \mathbb{C}\} = V \tag{1.2}$$

It can be shown that the number of basis elements of a vector space is invariant for all the bases of the vector space. Hence, the number of basis elements defines the *dimension* of a vector space. Furthermore, the number of elements of the basis is equal to the number of elements of the basis of dual vector space – vector space of linear functionals on vectors from V.

Definition 3. Let V be a vector space over $\mathbb{F}$, a *linear functional* η on vector space V is a function from the vector space to its field $\eta : V \to \mathbb{F}$ such that for all vectors $u, v \in V$ and scalars $\alpha, \beta \in \mathbb{F}$ it holds that

$$\eta(\alpha \cdot u + \beta \cdot v) = \alpha \cdot \eta(u) + \beta \cdot \eta(v)$$

Dual space $V^\perp$ of a vector space V is defined as the set of all linear functionals on the vector space V.

Let $\{u_i \mid i \leq n\}$ be a basis of an n-dimensional vector space V, then there is a uniquely determined basis $\{u_j{}^\dagger \mid j \leq n\}$ in $V^\perp$ such that the linear functional $u_j(u_i)$ is identically $u_j{}^\dagger(u_i) = \delta_{ij}$ where δ_{ij} denotes Kronecker delta function[2]. Hence, for all vectors $u = \sum_i \alpha_i u_i$ and $v = \sum_j \beta_j u_j$, the value of $v(u)$ is determined by

$$v(u) = v^\dagger(u) = \sum_{i,j} \beta_j{}^* \alpha_i u_j{}^\dagger(u_i) = \sum_i \beta_i{}^* \alpha_i \tag{1.3}$$

where the unary operator $(*)$ in β^* denotes *complex conjugation*[3]. Consequently, we want to induce geometry on the vector space. For Euclidean space $\mathbb{R}^n$, the geometry is induced by vector dot product operator $(\cdot)$. The length of a vector v can be computed as its norm $\|v\| = \sqrt{v \cdot v}$ and the angle between two vectors can be derived from $\cos\theta = \frac{u \cdot v}{\|u\|\|v\|}$. A generalization of this concept leads to the definition of inner product.

Definition 4. Let V be a vector space over a field $\mathbb{F}$, a function from a pair of vectors to an element of the field $\langle u, v\rangle : V \times V \to \mathbb{F}$ is *inner product* if for all vectors $u, v, w \in V$ and a scalar $\alpha \in \mathbb{F}$

$\langle \alpha u + v, w\rangle = \alpha \langle u, w\rangle + \langle v, w\rangle$	Linearity
$\langle u, v\rangle = \langle v, u\rangle^*$	Conjugate symmetry
$\langle u, u\rangle \geq 0$ and $\langle u, u\rangle = 0$ if and only if $u = 0$	Positive definiteness

By the induced geometry, inner product allows to define *orthogonality* of vectors u, v as the perpendicularity of the vectors. Two vectors u, v are orthogonal if their inner product vanishes $\langle u, v\rangle = 0$. Furthermore, it holds that sets of orthogonal vectors are linearly independent.

Theorem 1. *Every set S of mutually orthogonal vectors such that $0 \notin S$ is set of linearly independent vectors.*

---

2. Kronecker delta function δ_{ij} is defined as 1 for $i = j$ and 0 otherwise, i.e. it is the function that vanishes if the arguments do not equal.

3. Complex conjugate of a complex number $\beta = a + bi$ is a complex number $\beta^* = a - bi$.

Proof. Let's assume that there is a set of mutually orthogonal vectors of a vector space $S = \{v_i\}_{i=1}^n \subseteq V$ such that the set is not linearly independent. Therefore there is a $j \leq n$ such that $v_j = \sum_{i \neq j} c_i v_i$. From the definition of inner product we get that $\langle v_j, v_j \rangle \geq 0$ and $\langle v_j, v_j \rangle = 0$ if and only if $v_j = 0$. Since $0 \notin S$, we get

$$0 < \langle v_j, v_j \rangle = \left\langle v_j, \sum_{i \neq j} c_i v_i \right\rangle = \sum_{i \neq j} c_i \langle v_j, v_i \rangle = 0$$

and that's a contradiction. Hence there is no such set S and therefore every set $S, 0 \notin S$ of mutually orthogonal vectors is also a set of linearly independent vectors. □

It follows from the theorem that to specify a basis, it is sufficient to find a set of mutually orthogonal vectors. Hence, vector space V can be spanned by a set of n orthogonal vectors. If we limit the length of the orthogonal vectors to be always one $\langle u_i, u_i \rangle = 1$, then the set of mutually orthogonal length one vectors forms *orthonormal basis*. Consequently, a vector space endowed with the operation of inner product defines *inner product vector space*. Finally, the definition of Hilbert space may be presented.

Definition 5. Let $\mathcal{H}$ be an inner product vector space over a field of complex numbers $\mathbb{C}$ of a finite dimension, then $\mathcal{H}$ is a *Hilbert space*.

For a Hilbert space $\mathbb{C}^n$ with a basis $\{u_i\}_{i=1}^n$, we define the inner product of vectors v, u as the application of linear functional of the vector v: $v^* \in (\mathbb{C}^n)^\perp$ to the vector u.

$$\langle v, u \rangle = v(u) = v^\dagger(u) = \sum_{i,j} {\beta_j}^* \alpha_i {u_j}^\dagger(u_i) = \sum_i {\beta_i}^* \alpha_i \tag{1.4}$$

Each Hilbert space $\mathbb{C}^n$ endowed with the inner product forms *n-dimensional Hilbert space*. For a fixed n, there is up to an isomorphism exactly one n-dimensional Hilbert space. Hence, we focus on the Hilbert spaces $\mathbb{C}^n$ endowed with the operation of inner product as defined above. As an example, if we consider 2-dimensional complex Hilbert space of tuples $\mathbb{C}^2$, a vector $v = \beta_1 u_1 + \beta_2 u_2$ and a vector $u = \alpha_1 u_1 + \alpha_2 u_2$, then the basis vectors vanish and the inner product

expands to the sum of component-wise multiplications of conjugates of scalars in v and scalars in u

$$\langle v, u \rangle = {\beta_1}^* \cdot \alpha_1 + {\beta_2}^* \cdot \alpha_2$$

1.3 Pure quantum states

The notion of inner product allows for classification of specific subsets of the endowed vector space. We specify the subset of the vector space by enforcing additional constraints on the elements of the vector space. The most elementary condition for the elements is the one of being a pure quantum state. In this case, the word quantum suggests a specific kind of notation for the pure states of a Hilbert space $\mathcal{H}$. The notation is known as Dirac notation and it is aimed at the notion of the inner product. For an inner product of two vectors $|\phi\rangle$, $|\psi\rangle$ denoted by $\langle\phi|\psi\rangle$, the notation introduces the notion of left part of the inner product as ket vector and right part of the product as bra vector.

Definition 6. Let $|\phi\rangle$, $|\psi\rangle$ be vectors in a Hilbert space $\mathcal{H}$ endowed with the inner product function denoted by $\langle\phi|\psi\rangle$ and let $\{|b_i\rangle\}_{i=1}^n$ be a basis in the Hilbert space, then the vector $|\psi\rangle = \sum_{i=1}^n \alpha_i |b_i\rangle$ is *ket* vector and it is represented by the column vector of the coefficients α_i. Consequently, the vector $\langle\phi|$ denotes a *bra* vector and for the vector $|\phi\rangle = \sum_{i=1}^n \beta_i |b_i\rangle$, it is defined as the linear functional corresponding to the vector $|\phi\rangle$. The bra vector is represented by row vector of the coefficients ${\beta_i}^*$.

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \qquad \langle\phi| = ({\beta_1}^*, \ldots, {\beta_n}^*) \tag{1.5}$$

A *pure quantum state* over a Hilbert space $\mathcal{H}$ is defined as unit one ket vector over the Hilbert space $\mathcal{H}$. A ket vector $|\psi\rangle \in \mathcal{H}$ is a unit one vector over the Hilbert space $\mathcal{H}$ if it is of length one

$$\langle\psi|\psi\rangle = 1$$

In particular, the set of all pure quantum states of Hilbert space $\mathbb{C}^n$ forms a set of all unit one vectors in $\mathbb{C}^n$. If a vector is not a unit one vector, then the process of normalisation can be applied in order to turn the vector to a pure quantum state. Every vector $|\psi\rangle \in \mathbb{C}^n$ can be turned into a state by normalisation function $\tau : \mathbb{C}^n \to \mathbb{C}^n$ defined by

$$\tau(|\psi\rangle) = \frac{1}{\sqrt{\langle\psi|\psi\rangle}} \cdot |\psi\rangle \tag{1.6}$$

In order to show that the function τ turns a vector $|\psi\rangle = (\alpha_i)_{i=1}^n$ to a pure quantum state $\tau(|\psi\rangle) \in \mathbb{C}^n$ we compute the inner product of the vector $|\phi\rangle = \tau(|\psi\rangle)$ after the application of τ function

$$\langle\phi|\phi\rangle = \sum_{i=1}^{n} \frac{1}{\langle\psi|\psi\rangle} \cdot {\alpha_i}^* \cdot \alpha_i = \frac{1}{\langle\psi|\psi\rangle} \cdot \sum_{i=1}^{n} {\alpha_i}^* \cdot \alpha_i = \frac{1}{\langle\psi|\psi\rangle} \cdot \langle\psi|\psi\rangle = 1$$

With the definition of pure quantum states in mind we can say that orthonormal basis is a set of orthogonal pure quantum states. In particular, for a two-dimensional Hilbert space $\mathbb{C}^2$, we can see that the set of two pure states $\{|0\rangle, |1\rangle\}$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

is orthogonal and hence it forms an orthonormal basis in $\mathbb{C}^2$. Since every state $|\phi\rangle \in \mathbb{C}^2$ is a linear combination of the basis vectors $|0\rangle, |1\rangle$ then for an arbitrary $|\phi\rangle$ there are scalars $\alpha, \beta \in \mathbb{C}$ such that it holds that

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

The state $|\phi\rangle$ over the Hilbert space $\mathbb{C}^2$ is known as *qubit*. The qubit is a quantum equivalent of classical bit. Hence, the basis states are usually $|0\rangle, |1\rangle$ and qubit is linear combination of the two states such that it satisfies the condition for being a pure quantum state. From the relation of qubits and classical bits, the basis that the vectors $|0\rangle$, $|1\rangle$ form goes by the name of *computational basis*. To provide an example of a different basis, the *dual basis* will be introduced. For the Hilbert space $\mathbb{C}^2$, dual basis consists of two mutually orthogonal states $|+\rangle$ and $|-\rangle$ given by

$$|+\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle, \quad |-\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle \tag{1.7}$$

Since $|+\rangle$ and $|-\rangle$ are mutually orthogonal states, the basis $\{|+\rangle, |-\rangle\}$ is orthonormal. Now, if we try to express the computational basis vectors in the dual basis we can notice the resemblance of the definition of $|+\rangle$ in computational basis and the definition of $|0\rangle$ in dual basis. The same resemblance can be found for $|-\rangle$ and $|1\rangle$.

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} + \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \tag{1.8}$$

$$|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\-1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \tag{1.9}$$

Consequently, it is necessary to remark that the computational basis can be further generalized to higher dimensions by means of the Kronecker delta function where the set of pure quantum states $\{|b_i\rangle\}_{i=1}^{n}$ in $\mathbb{C}^n$ defined by $|b_i\rangle = (\delta_{ij})_{j=1}^{n}$ is the generalization.

1.4 Products & Operators

The definition of the notion of inner product and the concept of inner product vector space were already presented. However, in the meantime, the Dirac notation was introduced. Hence, as a way to connect the two notations, the definition of the inner product in terms of Dirac notation will be provided. Originally, the inner product was defined by the application of linear functional of a vector to a vector. Hence, in terms of Dirac notation, the definition of the inner product for the states $|\psi\rangle = (\alpha_i)_{i=1}^{n}$, $|\phi\rangle = (\beta_i)_{i=1}^{n}$ over an n-dimensional Hilbert space $\mathcal{H}$ yields

$$\langle\phi|\psi\rangle = \phi^{\dagger}(|\psi\rangle) = \sum_{i=1}^{n} {\beta_i}^{*}\alpha_i \tag{1.10}$$

We will now turn to introduce a second form of product. In particular, the notion of outer product will be introduced. The definition of outer product that will be presented necessitates the introduction of the concept of operators that are linear with respect to their arguments.

Definition 7. For Hilbert spaces $\mathcal{H}^A$, $\mathcal{H}^B$, *linear operator* is a function $L : \mathcal{H}^A \to \mathcal{H}^B$ such that for all vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}^A$ it holds that

$$L(|\psi\rangle + |\phi\rangle) = L(|\psi\rangle) + L(|\phi\rangle) \tag{1.11}$$

For all vectors $|\psi\rangle$, $|\phi\rangle$, $|\xi\rangle$ over a Hilbert space $\mathcal{H}$, an *outer product* of vectors $|\psi\rangle$ and $|\phi\rangle$, denoted by $|\psi\rangle\langle\phi| : \mathcal{H} \to \mathcal{H}$, is a linear operator defined by

$$|\psi\rangle\langle\phi|\left(|\xi\rangle\right) = |\psi\rangle \cdot \langle\phi|\xi\rangle = \langle\phi|\xi\rangle \cdot |\psi\rangle \tag{1.12}$$

In particular, for vectors $|\psi\rangle = (\alpha_i)_{i=1}^n$ and $|\phi\rangle = (\beta_i)_{i=1}^n$, we represent the outer product of the states by a matrix in the following way

$$|\psi\rangle\langle\phi| = \begin{pmatrix} \alpha_1{\beta_1}^* & \dots & \alpha_1{\beta_n}^* \\ \vdots & \ddots & \vdots \\ \alpha_n{\beta_1}^* & \dots & \alpha_n{\beta_n}^* \end{pmatrix} \tag{1.13}$$

More generally, it holds that it is possible to assign a matrix representation M to an arbitrary linear operator L. Let $\mathcal{H}^A$, $\mathcal{H}^B$ be Hilbert spaces with bases $\{|v_1\rangle, \dots, |v_n\rangle\}$ and $\{|w_1\rangle, \dots, |w_m\rangle\}$ respectively and let $L : \mathcal{H}^A \to \mathcal{H}^B$ be a linear operator then there are scalars $\gamma_{ij} \in \mathbb{C}$, $i \leq n$, $j \leq m$ such that for each i it holds that

$$M(|v_i\rangle) = \sum_j \gamma_{ij} |w_j\rangle$$

The values γ_{ij} form the matrix representation of the linear operator L. As for every matrix M it is possible to define linear operator L by $L(v) = Mv$, the matrices and linear operators are equivalent. Therefore, we can switch between the two representations without any loss of consistency of the overall theory. No matter how the outer products are represented they map vectors to vectors. In particular, it can be shown that outer product $|\psi\rangle\langle\phi|$ maps a vector $|\phi\rangle$ to a vector $|\psi\rangle$

$$|\psi\rangle\langle\phi|\left(|\phi\rangle\right) = |\psi\rangle\,\langle\phi|\phi\rangle = \langle\phi|\phi\rangle\,|\psi\rangle = |\psi\rangle$$

As a consequence of Riesz representation theorem [40], for each linear operator L on a Hilbert space $\mathcal{H}$ there is a unique *adjoint linear operator* $L^\dagger : \mathcal{H} \to \mathcal{H}$ such that for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ it holds that

$$\left\langle L^\dagger\psi\middle|\phi\right\rangle = \langle\psi|L\phi\rangle \tag{1.14}$$

The theorem allows us to describe the adjoints of linear operators and in particular outer products. The adjoints can be specified with

help of the matrix representation of linear operators. Let $\mathcal{H}$ be a Hilbert space, $L : \mathcal{H} \to \mathcal{H}$ be a linear operator and $M = (\alpha_{ij})_{i,j=1}^{n}$ be its matrix representation then the adjoint linear operator $L^\dagger$ of L is represented by matrix $({\alpha_{ji}}^*)_{i,j=1}^{n}$. Consequently, the composition of a linear and adjoint linear operator is defined as multiplication of their matrix representations.

Linear operators are defined as operators that map vectors to vectors and in particular, they can map states to vectors that are not states. Consequently, we focus on operators that preserve the inner product of Hilbert space and hence, they map states to states.

Definition 8. An identity operator, denoted by $\mathbb{I}$, is a unique linear operator such that for all $|\psi\rangle \in \mathcal{H}$, $\mathbb{I}(|\psi\rangle) = |\psi\rangle$. A linear operator $U : \mathcal{H} \to \mathcal{H}$ on a Hilbert space $\mathcal{H}$ is a *unitary* operator on $\mathcal{H}$ if it holds that

$$UU^\dagger = U^\dagger U = \mathbb{I}$$

For a unitary operator U, directly from its definition there is a prescription for inverse operator. From the definition, for $|\psi\rangle \in \mathcal{H}$ it holds that $U^\dagger(U(|\psi\rangle)) = (U^\dagger U)(|\psi\rangle) = \mathbb{I}(|\psi\rangle) = |\psi\rangle$. Hence, U^* is an inverse operator of U. In order to demonstrate that unitary operators preserve inner product, it suffices to compute the inner product $\langle U\phi|U\psi\rangle$. From the definition of adjoint operator it follows that $\langle U\phi|U\phi\rangle = \langle U^\dagger U\phi|\psi\rangle$ and as it was previously demonstrated, $U^\dagger U(\phi) = |\phi\rangle$. Hence, it holds that

$$\langle U\phi|U\psi\rangle = \langle\phi|\psi\rangle \tag{1.15}$$

As an example of linear and, in particular, unitary operators, consider the following three operators given by their matrix representations

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.16}$$

The matrices σ_x, σ_y, σ_z are known as Pauli matrices. Their importance arises from the fact that they correspond to the very basic operations on qubits. In particular, the Pauli matrix σ_x maps a qubit $\alpha|0\rangle + \beta|1\rangle$ to qubit $\beta|0\rangle + \alpha|1\rangle$ and is often known as bit flip or bit error. The Pauli matrix σ_z maps a qubit $\alpha|0\rangle + \beta|1\rangle$ to qubit $\alpha|0\rangle - \beta|1\rangle$ and

is often known as sign flip or sign error. The Pauli matrix σ_y maps a qubit $\alpha|0\rangle + \beta|1\rangle$ to qubit $-i\beta|0\rangle + i\alpha|1\rangle$ and hence it represents both the sign and the bit flip. There are also different ways of specifying the unitary operators. The Dirac notation is a very powerful tool and the operators can in fact be defined even purely in terms of the notation. For instance, the representation of Pauli matrix σ_y in Dirac notation is provided by linear operator

$$\sigma_y = 0 \cdot |0\rangle\langle 0| - i \cdot |0\rangle\langle 1| + i \cdot |1\rangle\langle 0| + 0 \cdot |1\rangle\langle 1| \tag{1.17}$$

As was previously demonstrated, the outer product of two vectors is a linear operator that maps vectors of a Hilbert space $\mathcal{H}$ to vectors in Hilbert space $\mathcal{H}$. To map the vectors to higher dimensions, the notion of tensor product is important. For a given vector $|\phi\rangle$ in n-dimensional Hilbert space $\mathcal{H}^A$ and a vector $|\psi\rangle$ in m-dimensional Hilbert space $\mathcal{H}^B$, the tensor product ($\otimes$) of $|\phi\rangle$ and $|\psi\rangle$ is vector $|\phi\rangle \otimes |\psi\rangle$ in $(n \cdot m)$-dimensional tensor product Hilbert space $\mathcal{H}^A \otimes \mathcal{H}^B$ that is formed by linear combinations of tensors of vectors in $\mathcal{H}^A$ and $\mathcal{H}^B$. In column vector representation, the tensor product is given by

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \otimes \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} \alpha_1 |\psi\rangle \\ \vdots \\ \alpha_n |\psi\rangle \end{pmatrix} \tag{1.18}$$

Consequently, the tensor product space can de defined as the space spanned by tensor products of basis vectors of $\mathcal{H}^A$ and $\mathcal{H}^B$. Furthermore, given a linear operator L^A on $\mathcal{H}^A$ and linear operator L^B on $\mathcal{H}^B$, the constraint of linearity gives the direct prescription for the definition of linear operator $L^A \otimes L^B$ on $\mathcal{H}^A \otimes \mathcal{H}^B$ and it is defined by

$$L_n \otimes L_m(\sum_i \alpha_i |\phi_i\rangle \otimes |\psi_i\rangle) \equiv \sum_i \alpha_i L_n(|\phi_i\rangle) \otimes L_m(|\psi_i\rangle) \tag{1.19}$$

For instance, the simplest case of complex Hilbert spaces with $n = 2, m = 2$ yields two-dimensional complex Hilbert spaces $\mathcal{H}^A = \mathbb{C}^2$ and $\mathcal{H}^B = \mathbb{C}^2$. All the vectors of both spaces can be spanned by the set of vectors in computational basis

$$\left\{ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \tag{1.20}$$

Consequently, the tensor product space $\mathbb{C}^2 \otimes \mathbb{C}^2$ is a Hilbert space spanned by the set of vectors $\{|0\rangle \otimes |0\rangle, |1\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |1\rangle\}$ where

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

It can be seen that the basis is formed by a set of mutually orthogonal vectors and that it corresponds to the computational basis in $\mathbb{C}^4$. Hence, we write that $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$. Furthermore, it can be seen that the number of elements of the basis grows significantly with the number of tensored Hilbert spaces. In particular, for Hilbert space of qubits $\mathbb{C}^2$, the dimension grows exponentially with the number of qubits and hence, n-qubit states live in 2^n-dimensional complex Hilbert space $\mathbb{C}^{2^n}$.

It is necessary to remark that the $\otimes$ sign is often omitted and the two kets are often enclosed in a single ket. For instance, the tensor product of ket vectors $|0\rangle$ and $|1\rangle$ yields the equality $|0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle$. Furthermore, it is being noted that the indexation of the vectors of orthonormal basis can be further generalized to any n-dimensional Hilbert space $\mathcal{H}$ where vector $|i\rangle$ denotes the i-th vector of an orthonormal basis in $\mathcal{H}$.

1.5 Measurements

Quantum mechanics is a physical theory and as such it relies heavily on the outcomes of experiments. The process of getting the outcome by an experiment is known as measurement and in quantum mechanics it is governed by a set of measurement operators.

Definition 9. Let $M = \{M_i\}_{i=1}^n$ is a set of linear operators on a Hilbert space $\mathcal{H}$ then M is a *set of measurement operators* if

$$\sum_{i=1}^{n} M_i^\dagger M_i = \mathbb{I} \tag{1.21}$$

where $\mathbb{I}$ is an identity operator and $\{i\}_{i=1}^{n}$ is the set of the classical measurement outcomes. The probability to measure the outcome i for a state $|\phi\rangle \in \mathcal{H}$ is given by

$$p(i) = \langle\phi| M_i{}^{\dagger} M_i |\phi\rangle$$

and the state $|\phi\rangle$ collapses into the state

$$|\phi\rangle \rightarrow \frac{M_i |\phi\rangle}{\sqrt{\langle\phi| M_i{}^{\dagger} M_i |\phi\rangle}}$$

It is often said that a measurement is performed in an orthonormal basis. In order to demonstrate such a process, at first, it will be shown that the inner product extracts scalars from the representation of a vector in an orthonormal basis. For orthonormal set $\{|b_i\rangle\}_{i=1}^{n}$ in $\mathbb{C}^n$ and vector $|\phi\rangle \in \mathbb{C}^n$, we know that $|\phi\rangle$ is a linear combination of basis states $|\phi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle$. Hence, if we compute the inner product of $|\phi\rangle$ and any of the $|b_i\rangle$ knowing that $\langle b_i|b_j\rangle = \delta_{ij}$, we get

$$\langle b_i|\phi\rangle = \langle b_i| (\sum_{j=1}^{n} \alpha_j |b_j\rangle) = \sum_{j=1}^{n} \alpha_j \langle b_i|b_j\rangle = \alpha_i \langle b_i|b_i\rangle = \alpha_i$$

Consequently, we can show that any set M of outer products of the orthonormal basis such that $M = \{|b_i\rangle\langle b_i|\}_{i=1}^{n}$ is a set of measurement operators. Initially, since the outer products are by definition linear operators then for an arbitrary state $|\phi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle \in \mathbb{C}^n$ it holds that

$$(\sum_{i=1}^{n} |b_i\rangle\langle b_i|)(|\phi\rangle) = \sum_{i=1}^{n} |b_i\rangle \langle b_i|\phi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle = |\phi\rangle \tag{1.22}$$

Hence, $\sum_{i=1}^{n} |b_i\rangle\langle b_i| = \mathbb{I}$ and from the fact that $|\phi\rangle\langle\phi|^{\dagger} |\phi\rangle\langle\phi| = |\phi\rangle\langle\phi|$, the set M is a set of measurement operators. Hence if a measurement is performed with respect to an orthonormal basis, the set of outer products of the states in orthonormal basis forms the desired set of measurement operators. For instance, a set of measurement operators for the dual basis will be derived. The vectors $|+\rangle$, $|-\rangle$ form an orthonormal basis in $\mathbb{C}^2$. Hence, the set of measurement operators is given by linear operators $M_1 = |+\rangle\langle+|$ and $M_2 = |-\rangle\langle-|$ and

${M_1}^\dagger M_1 + {M_2}^\dagger M_2 = \mathbb{I}$. Consequently, the measurement of the state $|0\rangle$ in the dual basis yields

$$p(1) = \langle 0| {M_1}^\dagger M_1 |0\rangle = \langle 0| M_1 |0\rangle = \frac{1}{2} \tag{1.23}$$

$$p(2) = \langle 0| {M_2}^\dagger M_2 |0\rangle = \langle 0| M_2 |0\rangle = \frac{1}{2} \tag{1.24}$$

and the state $|0\rangle$ will collapse into one of the states $|\phi_1\rangle, |\phi_2\rangle$

$$|\phi_1\rangle = \frac{M_1 |0\rangle}{\sqrt{p(1)}} = \sqrt{2} \cdot \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle \tag{1.25}$$

$$|\phi_2\rangle = \frac{M_2 |0\rangle}{\sqrt{p(2)}} = \sqrt{2} \cdot \frac{1}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle \tag{1.26}$$

The concept of measurement as presented in Definition 9 currently provides the most general way to define the measurement process. Hence, it is sometimes referred to as the *general measurement*. There are also different common ways to define measurements. One of them is the projective measurement where the measurement is governed by Hermitian operators. A liner operator L is Hermitian if it is equal to its adjoint operator

$$M = M^\dagger$$

The Hermitian operators in projective measurement are called *observables*. It holds that for each observable there is a set of measurement operators such that it sums up to the identity matrix. In fact, if we add the condition for the measurement operators to be Hermitian and the condition that $M_i M_j = \delta_{i,j} M_i$ where δ_{ij} is the Kronecker delta function, we get exactly the projective measurement operators [39].

A different description of the measurement process is provided by Positive Operator-Valued Measurements (POVM). This description of measurement process is designed for the systems with at most one measurement of the states as the description generally does not provide a way to compute the resulting state after the measurement. If we denote P_i by

$$P_i = {M_i}^\dagger M_i$$

then the set $P = \{P_i\}$ is the set of POVM operators[4]. Since the P_i operators were used directly in the definition of POVM operators and there is a need for the M_i operator in order to tell what state to collapse to, the description does not provide a way compute the resulting pure state. Hence, it follows from the revised definition of the POVM measurements that they are also a less general version of the general measurements defined earlier.

1.6 Postulates of quantum mechanics

All the theory so far led to the mathematical description of quantum systems. At this point, it is finally possible to connect the theory with the real physical systems. This connection is governed by postulates of quantum mechanics. The postulates of quantum mechanics map a mathematical theory to physical systems. Hence, they are the result of years of discoveries made by experimenters as well as theoreticians in the field of quantum mechanics. However, this also means that the postulates may still undergo more or less minor changes over time. Currently, the postulates may be formulated in the following form.

- *State space.* For every physical quantum system there is a complex vector space with inner product known as Hilbert space. The physical system is completely described by its state vector that is a unit one vector in the complex Hilbert space.

- *Evolution.* Every evolution of a physical quantum system is fully described by unitary operators.

- *Measurements.* Measurements of a quantum system in Hilbert space $\mathcal{H}$ are governed by measurement operators from set $M = \{M_i\}$ such that
$$\sum_i M_i^\dagger M_i = \mathbb{I}$$

4. This definition of POVM measurement was derived from the general definition of measurements, but there is also a different way to define the POVM measurements [39].

- *Tensor systems.* Let $\mathcal{H}^A, \mathcal{H}^B$ be Hilbert spaces for a description of some quantum systems, then the Hilbert space $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ defined as the space spanned by all the combinations of tensors of the basis states of $\mathcal{H}^A$ and $\mathcal{H}^B$ describes the composite quantum system.

These four simple postulates shall be sufficient to describe any physical quantum system realisable and in fact these postulates seem to be exhaustive from the mathematical point of view. A theory shall certainly define its space and vectors that are allowed in the space. The notion of evolution only allows to transform any physically realisable system to another physically realisable system. Considering that the roots of quantum mechanics are in physics, the necessity for the measurements is also justified. This leaves the last postulate that only makes it possible to compose two quantum systems.

2 Introduction to Entanglement

The quantum information theory is to a great extent built on the concept of randomness and the consequences of the special way the randomness functions in the theory. The randomness does not seem to be just a theoretical concept in this area. There are reasonable arguments that the randomness comes directly from the underlying physical nature of the quantum computer - the universe itself. This randomness led to many problems and results that are hard to believe. It also originated the famous criticism of the quantum theory by Albert Einstein

> "Quantum mechanics is very impressive. But an inner voice tells me that it is not yet the real thing. The theory produces a good deal but hardly brings us closer to the secret of the Old One. I am at all events convinced that He does not play dice."

Einstein continued to express the similar ideas about the Copenhagen probabilistic interpretation of the quantum mechanics and at the fifth Solvay congress Niels Bohr, one of the fathers of the interpretation, formulated an answer to the Einsten's remarks about the interpretation of quantum mechanics

> "I am pointing at the great caution, already called for by ancient thinkers, in ascribing attributes to Providence in every-day language."

The views on the randomness tended to move towards the Bohr's view in the years that followed and nowadays, the probabilistic interpretation is still the standard interpretation of quantum mechanics.

It was the disbelief in the completeness of the quantum mechanics that lead Albert Einstein, Boris Podolsky and Nathan Rosen to publish their paper about the famous EPR thought experiment [17]. While the thought experiment was originally created to show the incompleteness of quantum mechanics, contrary to its original intention, the experiment lead to the study of an important property of quantum systems – entanglement.

2.1 Entanglement of pure states

In this section, the definition for pure entangled states will be introduced and afterwards it will be shown that there are pure states that satisfy this condition. Since entangled states are usually defined as the complement of separable states, the definition of separable pure states and product states will precede the definition of entangled pure states.

Definition 10. Let $\mathcal{H}^A, \mathcal{H}^B$ be Hilbert spaces and let $|\phi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$ be a pure state. The state $|\phi\rangle$ is a *product state* in $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ if there are pure states $|\phi\rangle^A \in \mathcal{H}^A$, $|\phi\rangle^B \in \mathcal{H}^B$ such that

$$|\phi\rangle = |\phi\rangle^A \otimes |\phi\rangle^B \tag{2.1}$$

A pure state $|\phi\rangle$ is *separable* if it is a product state in $\mathcal{H}$. Otherwise, the state $|\phi\rangle$ is *entangled*.

The mere existence of pure states that would fulfil the condition of being entangled is not immediately obvious. Let $\{|a_i\rangle\}$ be a basis for $\mathcal{H}^A$ and let $\{|b_i\rangle\}$ be a basis for $\mathcal{H}^B$. The set $\{|a_i b_j\rangle\}$ is a basis for $\mathcal{H}$ and every pure state $|\phi\rangle$ in $\mathcal{H}$ can be expressed as

$$|\phi\rangle = \sum_{i=1}^{d^A} \sum_{j=1}^{d^B} \alpha_{ij} |a_i b_j\rangle \tag{2.2}$$

with complex parameters α_{ij} such that $\sum_{i,j} |\alpha_{ij}|^2 = 1$. Therefore, it is necessary to find a state such that it can be written as linear combination of tensor products of the basis states of the partitions[1] but cannot be written as a tensor product of two states from the respective partitions directly. It was already shown that the Hilbert space $\mathbb{C}^4$ is a tensor product space of $\mathbb{C}^2$ and $\mathbb{C}^2$. Hence, by consideration of two arbitrary states $|\psi_1\rangle = \alpha_1 |0\rangle + \alpha_2 |1\rangle$ and $|\psi_2\rangle = \beta_1 |0\rangle + \beta_2 |1\rangle \in \mathbb{C}^2$, an arbitrary product state $|\psi\rangle$ in $\mathbb{C}^4$ can be composed as

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \alpha_1\beta_1 |00\rangle + \alpha_1\beta_2 |01\rangle + \alpha_2\beta_1 |10\rangle + \alpha_2\beta_2 |11\rangle$$

1. Let $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ be a tensor product Hilbert space, then Hilbert spaces $\mathcal{H}^A$, $\mathcal{H}^B$ are partitions of the Hilbert space $\mathcal{H}$.

Now, if the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathbb{C}^4$ were to be a product state, it follows that $\alpha_1\beta_2 = 0$ and thus either $\alpha_1 = 0$ or $\beta_2 = 0$. Hence, $\alpha_1\beta_1$ or $\alpha_2\beta_2$ vanish and that yields a contradiction with the assumption that $|\Phi^+\rangle$ is a product state. From the definition of entangled states, this means that $|\Phi^+\rangle$ is entangled and thus, it was shown that entangled states do exist.

The state $|\Phi^+\rangle$ is a Bell state. There are four Bell states and all of them serve as an example of entangled states. Furthermore, the states are mutually orthogonal. Hence, they form an orthonormal basis in Hilbert space $\mathbb{C}^4$. The description of all four Bell states follows

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2.3}$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2.4}$$

2.2 Schmidt decomposition

In this section, we gradually introduce the Schmidt decomposition and the various mathematical concepts that are crucial for the understanding of Schmidt decomposition. The Schmidt decomposition is very powerful tool with various applications. For instance, the task of detection of entanglement for pure states is made possible with help of the Schmidt decomposition as will be demonstrated in section 3.2.

Let L be a linear operator on Hilbert space $\mathcal{H}$, then it is possible to define an eigenvector and an eigenvalue of the operator. The *eigenvector* of $L : \mathcal{H} \to \mathcal{H}$ is a vector $|\psi\rangle \in \mathcal{H}$ such that there is a scalar $\lambda \in \mathbb{C}$ so that

$$L\,|\psi\rangle = \lambda\,|\psi\rangle \tag{2.5}$$

The number λ is an *eigenvalue* of the linear operator L. If $|\psi\rangle$, $|\phi\rangle$ are two vectors with the same eigenvalue λ then also their linear combination has the eigenvalue λ. Hence, let λ be an eigenvalue of a linear operator then the *eigenspace* of the eigenvalue λ is the set of vectors such that their eigenvalue is λ. For a linear operator L, its *orthonor-*

mal decomposition is the representation of the operator such that

$$L = \sum_i \lambda_i |i\rangle\langle i|$$

where $|i\rangle$ are eigenvectors that form an orthonormal set and λ_i are eigenvalues. The representation is also known as diagonal representation of the linear operator L and hence we say that linear operator is *diagonalisable* if it has an orthonormal decomposition. Not every linear operator is diagonalisable but there is a subset of the operators that is. In particular, it is the set of normal operators. A linear operator L is *normal* if $LL^\dagger = L^\dagger L$.

Theorem 2. *[39] L is a normal linear operator if and only if L is diagonalisable.*

The theorem is known as the spectral decomposition theorem and it can be proved by induction with respect to the number of eigenvalues of a linear operator. Hence, for every normal linear operator L there are orthogonal states $|i\rangle$ and eigenvalues λ_i such that $L = \sum_i \lambda_i |i\rangle\langle i|$. The representation of the operator L is known as *spectral decomposition* of the operator.

A linear operator $L : V \to V$ is *positive semidefinite* if for every vector $|\psi\rangle \in V$ the inner product of $|\psi\rangle$ and $L|\psi\rangle$ is non-negative, that is $\langle\psi|L\psi\rangle \geq 0$. In particular, the inner product must be real. Each linear operator can be decomposed to positive semidefinite and unitary operator. This decomposition is a consequence of the polar decomposition theorem.

Theorem 3. *[39] Let V be a vector space and let $L : V \to V$ be a linear operator then there are positive semidefinite operators J, K and unitary operator U such that*

$$L = UJ = KU$$

Consequently, the combination of the polar decomposition and the spectral decomposition to a single theorem yields singular value decomposition theorem.

Theorem 4. *Let L be a linear operator then there are unitary operators U_1, U_2 and a diagonal matrix D with non-negative entries such that*

$$L = U_1 D U_2 \tag{2.6}$$

Proof. From the polar decomposition theorem, for each operator L there is a unitary operator U_3 and a positive semidefinite operator J such that $L = U_3 J$. Since positive semidefinite operators are normal it follows from the spectral decomposition that there is a unitary operator U_4 and a diagonal matrix D such that $J = U_4 D {U_4}^\dagger$. Now, let $U_1 = U_3 U_4$ and $U_2 = {U_4}^\dagger$ then $L = U_1 D U_2$. □

The application of singular value decomposition is of importance to the Schmidt decomposition theorem. We now state and prove this theorem.

Theorem 5. *Let $|\psi\rangle$ be a pure state in Hilbert space $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$, then there are orthonormal bases $\left\{\left|j^A\right\rangle\right\}_{i=1}^{d^A}$, $\left\{\left|j^B\right\rangle\right\}_{i=1}^{d^B}$ for $\mathcal{H}^A$, $\mathcal{H}^B$ respectively and non-negative real coefficients α_j, $\sum_j \alpha_j^2 = 1$ such that*

$$|\psi\rangle = \sum_{j=1}^{\min\left\{d^A, d^B\right\}} \alpha_j \left|j^A\right\rangle \left|j^B\right\rangle \tag{2.7}$$

Proof. Let $\left\{b_i^A\right\}_{i=0}^{d^A}$ be an orthonormal basis in $\mathcal{H}^A$, let $\left\{b_k^B\right\}_{k=0}^{d^B}$ be an orthonormal basis in $\mathcal{H}^B$ and let d^A, d^B be the dimensions of $\mathcal{H}^A$ and $\mathcal{H}^B$ respectively, then there are coefficients β_{ik} such that

$$|\psi\rangle = \sum_{i=0}^{d^A} \sum_{k=0}^{d^B} \beta_{ik} \left|b_i^A\right\rangle \left|b_k^B\right\rangle$$

The β_{ij} coefficients form a matrix β. It implies from the singular value decomposition that there is a diagonal matrix δ and unitary matrices γ, ϵ such that $\beta = \gamma\delta\epsilon$. In particular, there are diagonal matrices δ for both dimensions, d^A as well as d^B. Hence,

$$|\psi\rangle = \sum_{i=0}^{d^A} \sum_{j=0}^{\min\left\{d^A, d^B\right\}} \sum_{k=0}^{d^B} \gamma_{ij} \delta_{jj} \epsilon_{jk} \left|b_i^A\right\rangle \left|b_k^B\right\rangle$$

Let $\left|j^A\right\rangle = \sum_i \gamma_{ij} \left|b_i^A\right\rangle$, $\left|j^B\right\rangle = \sum_k \epsilon_{jk} \left|b_k^B\right\rangle$ and $\left|m^A\right\rangle$, $\left|n^A\right\rangle$ be two arbitrary $\left|j^A\right\rangle$ vectors then the inner product of the states is

$$\left\langle n^A \middle| m^A \right\rangle = \left(\sum_i {\gamma_{in}}^* \left\langle b_i^A \right| \right) \left(\sum_k \gamma_{km} \left|b_k^A\right\rangle \right)$$

Since $\{b_i\}$ is an orthonormal set then $\langle b_i^A | b_k^B \rangle$ is 0 for $i \neq k$ and 1 otherwise. Hence, the two sums can be made into one and we get $\langle n^A | m^A \rangle = \sum_i {\gamma_{in}}^* \gamma_{im}$. Furthermore, the matrix γ is unitary, hence $\sum_i \gamma_{in} {\gamma_{im}}^* = 0$ for $m \neq n$ and 1 otherwise. Therefore, the vectors are states and they are mutually orthogonal, hence they form an orthonormal basis. Similarly for $|j^B\rangle$. Now, rewriting the state $|\psi\rangle$ with help of $|j^A\rangle$ and $|j^B\rangle$ states, the equality yields

$$|\psi\rangle = \sum_{j=1}^{\min\{d^A, d^B\}} \delta_{jj} |j^A\rangle |j^B\rangle$$

where $\alpha_j = \delta_{jj}$ are non-negative real numbers and $|j^A\rangle$, $|j^B\rangle$ are orthonormal states. □

It follows from the theorem that every bipartite state can be rewritten in terms of Schmidt decomposition. Hence, let $|\psi\rangle$ be a state in a Hilbert space $\mathcal{H}$, then the Schmidt rank of the state written in Schmidt decomposition $|\psi\rangle = \sum_j \alpha_j |j^A\rangle |j^B\rangle$ is the number of non-zero α_j parameters. Let $|\psi\rangle$ be a state, the Schmidt rank of the state is denoted by $rk(|\psi\rangle)$.

2.3 Entanglement of mixed states

It is not always known what exact pure state is occupied by a given quantum system. In this case, all that is known is the set of possible pure states and probabilities of the pure states occurring. Therefore, it is important to consider classically probabilistic distribution amongst the pure states. This distribution gives rise to the set of mixed states.

Definition 11. Let $\{\phi_i\}_{i=1}^k$ be a set of pure states in a Hilbert space $\mathcal{H}$, then any convex combination of the pure states yields a *mixed* state. The mixed states are represented by convex combinations of the outer products of pure states known as density matrices

$$\varrho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i| \text{ where } p_i \geq 0 \text{ and } \sum_{i=1}^{k} p_i = 1 \tag{2.8}$$

From the duality of matrices and linear operators, it follows that the mixed states are linear operators and hence, the term *density operator* is often used to refer to a mixed state. From the definition of mixed states, it immediately follows that all pure states are mixed. However, the converse does not hold. In fact, the statement can be further generalised to the following theorem showing the relation between the set of mixed states and the set of pure states.

Theorem 6. *A mixed state ϱ is a pure state if and only if there is a single pure state in the convex combination of the mixed state ϱ.*

Proof. For the purposes of the proof, the mixed states will be represented by vectors in a Hilbert space $\mathcal{H}$ with basis $\{|b_j\rangle\}_{j=1}^{n}$. From the definition of mixed states, each mixed state is a convex combination of pure states, hence

$$|\varrho\rangle = \sum_{i=1}^{k} p_i \, |\phi_i\rangle = \sum_{i=1}^{k} p_i \sum_{j=1}^{n} \alpha_{ij} \, |b_j\rangle \tag{2.9}$$

Following the definition of pure states, the inner product of the state is computed in order to decide whether the vector is of length one. Consequently, interchanging the order of the sums and taking the p_i^2 coefficients before the second sum, the inner product yields

$$\langle\varrho|\varrho\rangle = \sum_{j=1}^{n} \left(\sum_{i=1}^{k} p_i^2 {\alpha_{ij}}^* \alpha_{ij} \right) = \sum_{i=1}^{k} \left(\sum_{j=1}^{n} p_i^2 {\alpha_{ij}}^* \alpha_{ij} \right) \tag{2.10}$$

$$= \sum_{i=1}^{k} p_i^2 \left(\sum_{j=1}^{n} {\alpha_{ij}}^* \alpha_{ij} \right) = \sum_{i=1}^{k} p_i^2 \, \langle\phi_i|\phi_i\rangle = \sum_{i=1}^{k} p_i^2 \tag{2.11}$$

Since ϱ is a mixed state then also $\sum_{i=1}^{k} p_i = 1$ and each p_i is a positive real number. Consequently $\langle\varrho|\varrho\rangle = 1$ holds if and only if $k = 1$. □

This result also shows that no convex combination of pure states yields a pure state. Now, we can look more closely at the representation of the mixed states given to us by the set of density matrices. In order to describe some of the properties of the density matrices, it is vital to introduce the notion of a trace of a matrix.

Definition 12. A trace, denoted by Tr, of a square $n \times n$ matrix

$$M = (a_{ij})_{i,j=1,1}^{n,n} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \tag{2.12}$$

is given by $Tr(M) = \sum_{i=1}^{n} a_{ii}$.

The trace of a density matrix representation of a pure state is related to its inner product as it holds that $Tr(|\phi\rangle \langle\phi|) = \langle\phi|\phi\rangle = 1$. The trace can also help determine whether a given density matrix ϱ is a matrix for a pure state or a mixed state. It suffices to compute the trace of the square of density matrix as it holds for all density matrices that

$$Tr(\varrho^2) \leq 1$$

and the trace is equal to 1 if and only if the state is pure. The proof of this statement is very similar to the proof of Theorem 6.

The density matrix representation of states allows the description of reduced density matrices. These are the mixed states with respect to the partitions $\mathcal{H}^A$, $\mathcal{H}^B$ of composite Hilbert space $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$. In order to find the reduced form of a density matrix, the trace out operator is of a great importance.

Definition 13. Let $\mathcal{H}^A, \mathcal{H}^B$ be Hilbert spaces and let $\mathcal{L}(\mathcal{H}^A)$ denote the set of linear operators on a Hilbert space $\mathcal{H}^A$, then *trace* $\mathcal{H}^B$ *out* operator is a unique linear operator $Tr_{\mathcal{H}^B} : \mathcal{L}(\mathcal{H}^A \otimes \mathcal{H}^B) \to \mathcal{L}(\mathcal{H}^A)$ such that for each $L^A \in \mathcal{L}(\mathcal{H}^A)$ and each $L^B \in \mathcal{L}(\mathcal{H}^B)$ it holds that

$$Tr_{\mathcal{H}^B}(L^A \otimes L^B) = L^A Tr(L^B)$$

Consequently, the definition of entanglement for mixed states can be presented. Similarly to pure states, entangled mixed states are the complement of separable mixed states. However, the definition of separable states is more complex as it is necessary to differentiate the definitions of product states and separable states.

Definition 14. Let $\mathcal{H}^A$, $\mathcal{H}^B$ be Hilbert spaces and let ϱ be a mixed state over Hilbert space $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$, then the state ϱ is a *product* state in $\mathcal{H}$ if there are mixed states $\varrho^A \in \mathcal{L}(\mathcal{H}^A)$, $\varrho^B \in \mathcal{L}(\mathcal{H}^B)$ such that

$$\varrho = \varrho^A \otimes \varrho^B$$

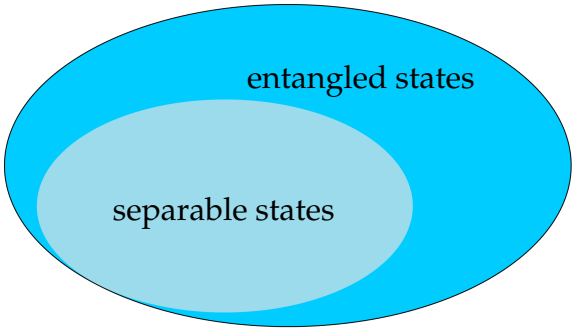

Figure 2.1: Geometrical representation of the sets of entangled and separable states.

Consequently, let $\varrho_1, \ldots, \varrho_n \in \mathcal{L}(\mathcal{H})$ be product states, then mixed state $\varrho \in \mathcal{L}(\mathcal{H})$ is *separable* if there are convex weights $p_i > 0$, $\sum_i p_i = 1$ such that

$$\varrho = \sum_{i=1}^{n} p_i \varrho_i$$

Finally, a mixed state ϱ is *entangled* if it is not separable.

It was already discussed that trace of a density matrix representation of a pure state is related to its inner product and hence, it is always 1. In fact, trace of all mixed states is always 1. Furthermore, every density matrix of trace 1 corresponds to a mixed state. Therefore, mixed states form a convex set. It follows from Theorem 6 that pure states are extremal[2] points of the convex set. Furthermore, from the definition of separable states, the set of separable states is a convex subset of the set of all mixed states. This all leads to the geometrical representation of set of all mixed states as depicted in Figure 2.1. The pure states lie on the edge of the whole set and the set of all separable states touches the edge of set of all states in infinitely many points as there is infinitely many separable pure states. The separable pure states cannot lie on the edge of subset of all separable states as depicted in Figure 2.1 since they are not convex combinations of any other states.

2. Extremal point of a convex set is a point in the set that is not a convex combination of two or more different points.

2.4 Bell inequalities

The EPR thought experiment introduced the conditions of locality, reality and completeness to the quantum mechanics. The condition of locality comes from the Einstein's theory of relativity and assumes that nothing can travel faster than the speed of light. The condition of reality postulates that if we can predict with certainty the outcome of a measurement of a physical quantity then the quantity is an element of the reality. The completeness suggests that a complete theory should describe every such an element of reality. The argument can be formulated with help of Bell state $|\Psi^-\rangle$ although any of the Bell states can be used to show the argument made in the EPR paper. First, to abstract from the condition of locality we assume that the measurements are performed instantaneously and hence, no local communication could be performed. Now, if we measure the first qubit of the state in computational basis and we get 0 then the outcome of the measurement of the second qubit will be 1 with certainty. Hence, we can conclude that there is an element of reality – a certain predetermination – for the second qubit. Quantum theory does not offer description of such an element of reality, it only offers description of its probabilities and hence the theory shall not be considered complete.

This argument spawned the study of local hidden variable interpretations of quantum mechanics and lead John S. Bell to show in his famous paper [5] that no such interpretation can exist[3]. This statement is known as *Bell theorem* and the proof of the theorem was originally shown in the Bell paper by what is now known as the original Bell inequality. The inequality postulated that any local hidden variable theory must satisfy the condition

$$1 + P(b, c) \geq |P(a, b) - P(a, c)|$$

where P is the expectation value function[4], a, b, c are variables with outcomes in $\{1, -1\}$ and we assume that each of the variables is dependent on a hidden variable λ. The value of $|P(a, b) - P(a, c)|$ is

3. There is a hidden variable interpretation [9] of quantum mechanics but the interpretation is not local.

4. The expectation value of a pure state $|\psi\rangle \in \mathcal{H}$ with respect to an observable O is equal to $\langle\psi|O\psi\rangle = \langle O\psi|\psi\rangle$ and is often denoted by $\langle\psi|O|\psi\rangle$.

generally non-zero and hence, the value $P(b, c)$ cannot be stationary at -1 in any local hidden variable interpretation of quantum mechanics. However it was shown in the Bell paper that for the following pure state

$$|\phi\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle |\uparrow\rangle - |\downarrow\rangle |\downarrow\rangle\right)$$

where 1 and -1 are the possible outcomes, there is an observable such that the expectation value $P(b, c)$ is always -1 and therefore it does not satisfy the inequality [5].

To provide a more detailed proof of the Bell theorem, a different inequality known as CHSH inequality will be presented. Nowadays, the CHSH inequality is likely the best known inequality that proves the Bell theorem. Let a_1, a_2, b_1, b_2 be classical observables with outcomes in $\{-1, 1\}$ and let P be the expectation value function, then it holds that

$$\begin{aligned} &P(a_1, b_1) - P(a_1, b_2) + P(a_2, b_1) + P(a_2, b_2) \\ &= P(a_1 b_1 - a_1 b_2 + a_2 b_1 + a_2 b_2) \\ &= P(a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

If $b_1 = b_2$, then $b_1 - b_2 = 0$ and the above equality reduces to $P(a_2(b_1 + b_2))$ and since b_1, b_2 and a_2 can all be just 1 or -1 then $P(a_2(b_1 + b_2)) \leq 2$. If $b_1 = -b_2$, then the above equality reduces to $P(a_1(b_1 - b_2))$ and since b_1, b_2 and a_1 can all be just 1 or -1 then also $P(a_1(b_1 - b_2)) \leq 2$. Hence, we can write

$$P(a_1, b_1) - P(a_1, b_2) + P(a_2, b_1) + P(a_2, b_2) \leq 2$$

Furthermore, if we assume that all the measurements are dependent on a local hidden variable λ then the expectation value still will not be higher than 2 that is the maximal value achievable by any of the possible cases and therefore the inequality still holds.

However, for the Bell state $|\Psi^-\rangle$, Alice acting on first qubit with observables a_1, a_2

$$\begin{aligned} a_1 = \quad \sigma_z \quad &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ a_2 = \quad \sigma_x \quad &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

and Bob acting on second qubit with observables b_1, b_2

$$\begin{aligned} b_1 = &\ \tfrac{1}{\sqrt{2}}(-\sigma_z - \sigma_x) = \tfrac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \\ b_2 = &\ \tfrac{1}{\sqrt{2}}(\sigma_z - \sigma_x) = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

the expectation values for all the cases can be computed with help of the observables. The computation of the expectation values yields

$$\begin{aligned} P(a_1, b_1) = &\ \langle \Psi^- | (a_1 \otimes b_1) \Psi^- \rangle &= \tfrac{1}{\sqrt{2}} \\ P(a_1, b_2) = &\ \langle \Psi^- | (a_1 \otimes b_2) \Psi^- \rangle &= -\tfrac{1}{\sqrt{2}} \\ P(a_2, b_1) = &\ \langle \Psi^- | (a_2 \otimes b_1) \Psi^- \rangle &= \tfrac{1}{\sqrt{2}} \\ P(a_2, b_2) = &\ \langle \Psi^- | (a_2 \otimes b_2) \Psi^- \rangle &= \tfrac{1}{\sqrt{2}} \end{aligned}$$

Hence, $P(a_1, b_1) - P(a_1, b_2) + P(a_2, b_1) + P(a_2, b_2) = 2\sqrt{2}$ and the pure state $|\Psi^-\rangle$ violates the CHSH inequality. Therefore no local hidden variable interpretation of quantum mechanics is possible.

2.5 Properties of entanglement

Following the Bell theorem, entanglement is considered to be a resource that is unique to quantum theory. They were entangled states that were used in the proof that quantum mechanics can violate the Bell inequality and the CHSH inequality. In this section, three topics in relation to the properties of entanglement will be presented. At first, a linear operator that can map separable states to entangled states will be presented. Consequently, a protocol that uses entanglement in order to manipulate with entanglement will be presented in order to demonstrate the power of entanglement. Finally, a theorem that shows the limitations of entanglement for application in quantum protocols will be presented.

2.5.1 Entanglement creation

The entangled states can be created by application of unitary operators on separable states. The unitary operators capable of transforming tensor product states to entangled states are called entangling

operators. An example of such a unitary operator is $CNOT$ operator

$$CNOT = \sum_{i,j=0,0}^{1,1} |i(i \oplus j)\rangle\langle ij| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.13}$$

where the operation $i \oplus j$ denotes the remainder after the division of $i + j$ by two. Consequently, let $|\psi\rangle = |+\rangle \otimes |0\rangle$, then the application of $CNOT$ operator to product state $|\psi\rangle$ yields the state

$$CNOT\,|\psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

and that is exactly the state $|\Phi^+\rangle$ which was already shown to be entangled. Hence, it was shown that $CNOT$ is entangling unitary operator. Since every unitary operator has its inverse and the inverse operator to $CNOT$ operator is again $CNOT$ operator, the operator can be used also to disentangle the state $|\Phi^+\rangle$ back to the state $|\psi\rangle$ directly by application of the operator to the state $|\Phi^+\rangle$.

2.5.2 Entanglement can be swapped

Let A, B, C are three parties represented by Alice, Bob and Charlie. Let Alice and Bob share entangled state $|\Phi^+\rangle^{AB}$ and let Alice and Charlie share entangled state $|\Phi^+\rangle^{AC}$. Hence the resulting state written with Alice's qubits at first two places is

$$\begin{aligned} |\psi\rangle^{AABC} = &\frac{1}{2}\left(|00\rangle^{AA} \otimes |00\rangle^{BC} + |01\rangle^{AA} \otimes |01\rangle^{BC}\right) \\ &+ \frac{1}{2}\left(|10\rangle^{AA} \otimes |10\rangle^{BC} + |11\rangle^{AA} \otimes |11\rangle^{BC}\right) \end{aligned}$$

Consequently, Alice wishes to perform a measurement on her two qubits. Hence she designs a set of measurement operators based on

Bell states M in the following way

$$\begin{aligned} M = \{ & \left|\Phi^+\right\rangle\left\langle\Phi^+\right|^{AA} \otimes \mathbb{I}^B \otimes \mathbb{I}^C, \\ & \left|\Phi^-\right\rangle\left\langle\Phi^-\right|^{AA} \otimes \mathbb{I}^B \otimes \mathbb{I}^C, \\ & \left|\Psi^+\right\rangle\left\langle\Psi^+\right|^{AA} \otimes \mathbb{I}^B \otimes \mathbb{I}^C, \\ & \left|\Psi^-\right\rangle\left\langle\Psi^-\right|^{AA} \otimes \mathbb{I}^B \otimes \mathbb{I}^C\} \end{aligned}$$

where $\mathbb{I}^B$, $\mathbb{I}^C$ are identity operators since neither Bob nor Charlie want to perform a measurement. Therefore there are four possible cases, one for each measurement operator. The probability of measuring each of the possibilities is always $\frac{1}{4}$. If Alice measures the outcome 00, then the first measurement operator was used and the state $|\psi\rangle^{AABC}$ collapsed into the state

$$\begin{aligned} |\psi\rangle^{AABC} \rightarrow & \frac{1}{2}\left(|0000\rangle^{AABC} + |0011\rangle^{AABC}\right) \\ & + \frac{1}{2}\left(|1100\rangle^{AABC} + |1111\rangle^{AABC}\right) \\ & = \frac{1}{\sqrt{2}}\left(|00\rangle^{AA} + |11\rangle^{AA}\right) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle^{BC} + |11\rangle^{BC}\right) \end{aligned}$$

Hence, Bob and Charlie do possess entangled pair $|\Phi^+\rangle$ and Alice has the outcome 00 as a witness of this situation. Now, if Alice gets 01, then the second measurement operator was used and the state collapsed into the state

$$\begin{aligned} |\psi\rangle^{AABC} \rightarrow & \frac{1}{2}\left(|0000\rangle^{AABC} - |0011\rangle^{AABC}\right) \\ & - \frac{1}{2}\left(|1100\rangle^{AABC} - |1111\rangle^{AABC}\right) \\ & = \frac{1}{\sqrt{2}}\left(|00\rangle^{AA} - |11\rangle^{AA}\right) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle^{BC} - |11\rangle^{BC}\right) \end{aligned}$$

Hence, Bob and Charlie do possess entangled pair $|\Phi^-\rangle$ and Alice has the outcome 01 as a witness for the pair. For the third measurement

operator, Alice gets the outcome 10 and the state collapses into

$$\begin{aligned}|\psi\rangle^{AABC} \rightarrow & \frac{1}{2}\left(|0101\rangle^{AABC} + |0110\rangle^{AABC}\right) \\ & + \frac{1}{2}\left(|1001\rangle^{AABC} + |1010\rangle^{AABC}\right) \\ & = \frac{1}{\sqrt{2}}\left(|01\rangle^{AA} + |10\rangle^{AA}\right) \otimes \frac{1}{\sqrt{2}}\left(|01\rangle^{BC} + |10\rangle^{BC}\right)\end{aligned}$$

Hence, in this case Bob and Charlie possess entangled pair $|\Psi^+\rangle$ and the witness for this is the Alice's outcome 10. The last measurement operator yields the outcome 11 and the state $|\psi\rangle^{AABC}$ collapses into the state

$$|\psi\rangle^{AABC} \rightarrow \frac{1}{\sqrt{2}}\left(|01\rangle^{AA} - |10\rangle^{AA}\right) \otimes \frac{1}{\sqrt{2}}\left(|01\rangle^{BC} - |10\rangle^{BC}\right)$$

Finally, in the last case Bob and Charlie possess an entangled pair $|\Psi^-\rangle$ and Alice's outcome 11 acts as a witness for this entangled pair. Bob and Charlie are in possession of one of the entangled pairs but neither of them know which entangled pair. For each entangled pair Alice possesses unique measurement outcome and hence, she can tell Bob and Charlie through classical communication which entangled pair they do possess. Therefore Bob and Charlie that might have never met before can now possess entangled pair with help of a man in the middle that is played out by Alice.

The described protocol swapped entanglement but both parties, Bob as well as Charlie, were aware of the swapping. However, the protocol can be refined with Alice in the last phase sending her outcome only to Bob. Consequently, based on the outcome that Alice sends to Bob, Bob can perform operation on his qubit by one of the unitary operators $\mathbb{I}$, σ_x, σ_z and $\sigma_z\sigma_x$ in order to obtain the entangled pair $|\Phi^+\rangle^{BC}$. In this way, Charlie is not aware of the fact that he is no longer in possession of entangled pair $|\Phi^+\rangle^{AC}$ with Alice but that he is in possession of entangled pair $|\Phi^+\rangle^{BC}$ with Bob.

2.5.3 No instant communication

The idea of entanglement as a "spooky action at a distance" may often lead to the idea of instant communication between two parties

that share an entangled pair. However, it can be shown that such a communication is not possible by the following no communication theorem.

Theorem 7. *Entanglement does not allow instant communication of two parties.*

Proof. Let ϱ be a mixed state over Hilbert space $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$. Every such a mixed state ϱ can be written as a sum of tensor products of linear operators A_i, B_i on the partitions $\mathcal{H}^A$, $\mathcal{H}^B$ respectively

$$\varrho = \sum_{i=1}^{n} A_i \otimes B_i \tag{2.14}$$

Let $M = \{M_j\}_{j=1}^{k}$ be a set of measurement operators in $\mathcal{H}^A$, then Alice can perform a measurement and she gets the mixed state

$$M(\varrho) = \sum_{i=1}^{n} \sum_{j=1}^{k} (M_j \otimes \mathbb{I})\, A_i \otimes B_i \left(M_j{}^{\dagger} \otimes \mathbb{I}\right) \tag{2.15}$$

where $M_j \varrho M_j{}^{\dagger}$ denotes the application of measurement operator to a mixed state ϱ. Consequently, the trace $\mathcal{H}^A$ out operation applied to mixed state $M(\varrho)$ yields

$$\begin{aligned}
tr_{\mathcal{H}^A}(M(\varrho)) =& tr_{\mathcal{H}^A}\left(\sum_i \sum_j (M_j \otimes \mathbb{I})^{\dagger} A_i \otimes B_i\, (M_j \otimes \mathbb{I})\right) \\
=& tr_{\mathcal{H}^A}\left(\sum_i \sum_j \left(M_j{}^{\dagger} A_i M_j\right) \otimes B_i\right) \\
=& \sum_i \sum_j tr\left(M_j{}^{\dagger} A_i M_j\right) B_i \\
=& \sum_i tr\left(A_i \sum_j M_j M_j{}^{\dagger}\right) B_i \\
=& \sum_i tr\left(A_i\right) B_i \\
=& tr_{\mathcal{H}^A}\left(\varrho\right)
\end{aligned}$$

Hence, the measurement did not change the traced out state. Furthermore, if Alice were to apply any unitary operator before the measurement she would map a mixed state into another mixed state and since this proof is for an arbitrary mixed state, it also covers this case. Therefore statistically Bob cannot gather any information about the system without the classical communication and that is not instant. □

3 Bipartite entanglement

The prefix *bi* in bipartite refers to the case where the number of partitions that are considered is two. Hence, for a Hilbert space $\mathcal{H}$, two Hilbert spaces $\mathcal{H}^A, \mathcal{H}^B$ such that $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$ are considered. Since $dim(\mathcal{H}) = dim(\mathcal{H}^A) \cdot dim(\mathcal{H}^B)$, Hilbert space $\mathcal{H}$ can have partitions only if its dimension is not a prime number[1]. Smallest dimension such that it is not a prime number is four with the corresponding complex Hilbert space $\mathbb{C}^4$. It was already discussed that $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ and that there are up to an isomorphism no other partitions of $\mathbb{C}^4$. However, for Hilbert space $\mathbb{C}^{12}$, several possible bipartitions[2] may be considered

$$\mathbb{C}^{12} = \mathbb{C}^2 \otimes \mathbb{C}^6 \qquad \mathbb{C}^{12} = \mathbb{C}^6 \otimes \mathbb{C}^2$$
$$\mathbb{C}^{12} = \mathbb{C}^3 \otimes \mathbb{C}^4 \qquad \mathbb{C}^{12} = \mathbb{C}^4 \otimes \mathbb{C}^3$$

The bipartitions $\{\mathbb{C}^2, \mathbb{C}^6\}$, $\{\mathbb{C}^6, \mathbb{C}^2\}$ as well as $\{\mathbb{C}^3, \mathbb{C}^4\}$, $\{\mathbb{C}^4, \mathbb{C}^3\}$ are symmetric with respect to the permutations of the partitions. Hence, globally, the two bipartitions represent the same case, respectively. Thus, the bipartitions are not usually considered separately. Consequently, the state $|\psi\rangle^A = |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle) \in \mathbb{C}^4$ and the state $|\psi\rangle^B = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \in \mathbb{C}^3$ may be considered so that one obtains

$$|\psi\rangle = |\psi\rangle^A \otimes |\psi\rangle^B = \frac{1}{\sqrt{6}}(|0\rangle + |1\rangle + |2\rangle + |9\rangle + |10\rangle + |11\rangle)$$

It immediately follows that the state $|\psi\rangle$ is separable with respect to partitions $\mathbb{C}^4$, $\mathbb{C}^3$ as there are states $|\psi\rangle^A \in \mathbb{C}^4$, $|\psi\rangle^B \in \mathbb{C}^3$ such that $|\psi\rangle = |\psi\rangle^A \otimes |\psi\rangle^B$. However, a general separable state with respect to partitions $\mathbb{C}^2 \otimes \mathbb{C}^6$ is given by

$$|\phi\rangle = \left(\sum_{i=0}^{1} \alpha_i |i\rangle\right) \otimes \left(\sum_{j=0}^{5} \beta_j |j\rangle\right) = \sum_{i=0}^{1}\sum_{j=0}^{5} \alpha_i\beta_j \left|i \cdot d^B + j\right\rangle$$

---

1. A number p is a prime number if it is not divisible by any number $j \in \mathbb{N}$ such that $j \neq 1$, $j \neq p$. By this definition, the number 1 is also a prime number.
2. Bipartition of a Hilbert space $\mathcal{H}$ is a set of partitions $\{\mathcal{H}^A, \mathcal{H}^B\}$ that generates the original Hilbert space, that is $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$.

where d^B is the dimension of the second partition that is in this case $d^B = 6$. Consequently, the assumption that $|\psi\rangle$ is a separable state yields $\alpha_0 \cdot \beta_0 = \alpha_1 \cdot \beta_5 = \frac{1}{\sqrt{6}}$. Hence, all four parameters have to be non-zero. Therefore also $\alpha_0 \cdot \beta_5$ is non-zero and that is a contradiction with the assumption that $|\psi\rangle$ is a separable state. Hence, the state is not separable with respect to the partitions $\mathbb{C}^2, \mathbb{C}^6$. This example shows that the choice of partitions is crucial to the separability decision problem. In order to abstract from the partitions, it is possible to define *genuinely entangled states* as the states that are entangled with respect to any bipartition. Examples of genuinely entangled states include Bell states as $\{\mathbb{C}^2, \mathbb{C}^2\}$ is the only bipartition of $\mathbb{C}^4$.

3.1 Classification

Let Alice and Bob share a pure state $|\psi\rangle^{AB}$ and assume that they know the density matrix of the state. One might ask himself what class of states can be obtained from the state without any direct exchange of quantum information. How to classify the state? In the case of bipartite entanglement, the answer to this question includes the notion of *local operation and classical communication* (LOCC) transformations.

Following from the name of the transformations, only unitary operations that are performed per partition[3], measurements that are performed per partition and unlimited classical two-way communication between the parties are permitted in the protocol transforming the states. As an example, let Alice and Bob share Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The state can be transformed into any other Bell state by application of local unitary Pauli matrices. In particular, the operations are

$$\left|\Phi^+\right\rangle = (\mathbb{I} \otimes \mathbb{I}) \left|\Phi^+\right\rangle \qquad \left|\Phi^-\right\rangle = (\sigma_z \otimes \mathbb{I}) \left|\Phi^+\right\rangle$$
$$\left|\Psi^+\right\rangle = (\sigma_x \otimes \mathbb{I}) \left|\Phi^+\right\rangle \qquad \left|\Psi^-\right\rangle = ((\sigma_z\sigma_x) \otimes \mathbb{I}) \left|\Phi^+\right\rangle$$

3. The fact that a unitary operator U is performed per partition A or B means that the operator $U \otimes \mathbb{I}^B$ or $\mathbb{I}^A \otimes U$ is performed, respectively. The per partition operators are also known as local operators.

Conversely, it holds that any other Bell state can be transformed to $|\Phi^+\rangle$ and hence, all Bell states are in the same class with respect to LOCC transformations. Similarly, let $|\psi\rangle^{AB} = |\psi\rangle^A \otimes |\psi\rangle^B$ be an arbitrary separable pure state. From the completeness of unitary transformations it follows that $|\psi\rangle^{AB}$ can be transformed to an arbitrary separable state by local operations $U^A \otimes \mathbb{I}^B$ and $\mathbb{I}^A \otimes U^B$ and hence, all the separable states are equivalent with respect to LOCC transformations. Consequently, for two pure states $|\psi\rangle$, $|\phi\rangle$ in a Hilbert space $\mathcal{H}$ with partitions $\mathcal{H}^A$, $\mathcal{H}^B$ of dimensions d^A, d^B respectively, there are Schmidt decompositions

$$|\psi\rangle = \sum_{i}^{\min\left\{d^A,d^B\right\}} \alpha_i \left|i^A\right\rangle \left|i^B\right\rangle \quad |\phi\rangle = \sum_{j}^{\min\left\{d^A,d^B\right\}} \beta_j \left|j^A\right\rangle \left|j^B\right\rangle \tag{3.1}$$

Let $\gamma = (\alpha_i^2)$ and $\eta = \left(\beta_j^2\right)$ be decreasingly ordered lists of parameters in Schmidt decompositions of states $|\psi\rangle$ and $|\phi\rangle$ respectively. It was shown in Ref. [37] that the state $|\psi\rangle$ may be transformed by LOCC to state $|\phi\rangle$ if and only if the ordered list γ is *majorized* by ordered list η, i.e. it holds for all $1 \leq k \leq \min\left\{d^A, d^B\right\}$ that

$$\sum_{i=1}^{k} \gamma_i \leq \sum_{j=1}^{k} \eta_j \tag{3.2}$$

Following the equation, one might ask whether there is a state that can be transformed to any other state. In particular, the question is equivalent to question whether there is a minimal list of coefficients in Schmidt decomposition. Let $d = \min\left\{d^A, d^B\right\}$, it can be shown that list $\left(\frac{1}{d}\right)_{i=1}^{d}$ is minimal. By contradiction, suppose that there is an ordered list of coefficients in Schmidt decomposition λ such that $\lambda_1 < \frac{1}{d}$. Hence, the average value of remaining coefficients is $\frac{1-\lambda_1}{d-1}$ and that is larger than the value of largest parameter λ_1 which is a contradiction. Hence, $\left(\frac{1}{d}\right)_{i=1}^{d}$ is a minimal list. Consequently, it is possible to provide a hierarchy of states that are most general with respect to a given bipartition. It can be seen that for states given by

$$|\chi_d\rangle = \sum_{i=1}^{d} \frac{1}{\sqrt{d}} \left|i^A\right\rangle \left|i^B\right\rangle \tag{3.3}$$

the ordered list of Schmidt parameters is exactly $\left(\frac{1}{d}\right)_{i=1}^{d}$ and hence, the list is minimal. Consequently, the state $|\chi_d\rangle$ can be transformed into any other state. In particular, in case of $d = 2$ and corresponding computational basis states $|0\rangle$, $|1\rangle$, the state $|\chi_d\rangle = |\Phi^+\rangle$ and hence, the state $|\Phi^+\rangle$ is the most general two-qubit state.

It follows from the Eq. 3.2 that two states can be mutually transformed to each other under LOCC if and only if there is a local unitary transformation $U^A \otimes U^B$ relating them. Hence, if we consider an arbitrary state in Schmidt decomposition and apply arbitrary local unitary transformation $U^A \otimes U^B$, then from the fact that unitary operators preserve inner product, the unitary operators will solely map orthonormal bases to possibly different orthonormal bases. Therefore, the Schmidt coefficients will not change under local unitary transformations. Consequently, if we consider entangled two-qubit states, then Schmidt rank of the states is necessarily higher than 1 as will be proved in subsection 3.2.1. Thus, the decomposition provides two Schmidt coefficients λ_1, λ_2. The only limitation for the Schmidt coefficients is to satisfy the condition $\lambda_1^2 + \lambda_2^2 = 1$. Hence, the classification yields infinitely many equivalence classes with respect to strict LOCC transformations. However, there is a state that can be transformed to any other bipartite state. Hence, the finiteness of the number of equivalence classes is not ultimately necessary.

3.2 Detection

The task of detection of entanglement can be defined as the task to decide whether a given general mixed state $\varrho \in \mathcal{H}$ with partitions $\mathcal{H}^A$, $\mathcal{H}^B$ is entangled with respect to the partitions or separable with respect to the partitions.

3.2.1 Pure states

The task of detection of entanglement in bipartite pure states was already fully solved for every bipartite pure state. The algorithm to decide this task uses the formalism of Schmidt decomposition and in particular Schmidt rank.

Theorem 8. *A state $|\psi\rangle \in \mathcal{H}$ is a product state if and only if its Schmidt*

rank is 1, that is $rk(|\psi\rangle) = 1$.

Proof. ($\Rightarrow$) Let $|\psi\rangle \in \mathcal{H}^{AB}$ be a product state with respect to the partitions $\mathcal{H}^A$, $\mathcal{H}^B$. By Schmidt decomposition

$$|\psi\rangle = \sum_j \alpha_j \left|j^A\right\rangle \left|j^B\right\rangle$$

The operation of tracing out the partition $\mathcal{H}^A$ or $\mathcal{H}^B$ yields reduced density matrices ϱ^B, ϱ^A of state $\varrho = |\psi\rangle\langle\psi|$

$$\begin{aligned} \varrho^B &= Tr_{\mathcal{H}^A}\left(\sum_{i,j} \alpha_i\alpha_j \left|i^A\right\rangle\left\langle j^A\right| \otimes \left|i^B\right\rangle\left\langle j^B\right|\right) = \sum_j \alpha_j^2 \left|j^B\right\rangle\left\langle j^B\right| \\ \varrho^A &= Tr_{\mathcal{H}^B}\left(\sum_{j,j} \alpha_i\alpha_j \left|i^A\right\rangle\left\langle j^A\right| \otimes \left|i^B\right\rangle\left\langle j^B\right|\right) = \sum_j \alpha_j^2 \left|j^A\right\rangle\left\langle j^A\right| \end{aligned}$$

and $\sum_j \alpha_j^2 = 1$. Furthermore the number of non-zero parameters of traced out states is equal to the number of non-zero parameters in Schmidt decomposition since $\alpha_j^2 = 0 \Leftrightarrow \alpha_j = 0$. From the assumption that $|\psi\rangle$ is a product state we get $|\psi\rangle = |\psi\rangle^A \otimes |\psi\rangle^B$ for some $|\psi\rangle^A \in \mathcal{H}^A$ and some $|\psi\rangle^B \in \mathcal{H}^B$. Hence $Tr_{\mathcal{H}^B}\left(|\psi\rangle\langle\psi|^A \otimes |\psi\rangle\langle\psi|^B\right) = |\psi\rangle\langle\psi|^A = \varrho^A$. Therefore ϱ^A must be pure and the trace of the square root of its density operator must be 1, i.e. $\sum_j \alpha_j^4 = 1$. Since $\sum_j \alpha_j^2 = 1$ this holds if and only if the number of non-zero parameters is 1 – the Schmidt rank is 1.

($\Leftarrow$) If Schmidt rank of the state $|\psi\rangle$ is 1 then the Schmidt decomposition of the state is

$$|\psi\rangle = \alpha_1 \left|1^A\right\rangle \otimes \left|1^B\right\rangle = \left|1^A\right\rangle \otimes \left|1^B\right\rangle$$

and $\left|1^A\right\rangle$, $\left|1^B\right\rangle$ are states in the corresponding partitions. Therefore $|\psi\rangle$ is a product state. □

It follows from the theorem that every bipartite entangled state has rank greater than one. Hence, it is possible to determine whether a given bipartite pure state is entangled directly by computation of its Schmidt rank.

3.2.2 Positive Partial Transpose criterion

There is an algorithm for detection of entanglement in pure states. Therefore, the task of entanglement detection focuses primarily on mixed states. The best-known criterion for this task is the positive partial transpose (PPT) criterion. Consequently, it is vital to notice that for a product basis, every density matrix ϱ can be decomposed to

$$\varrho = \sum_{i,j}^{N} \sum_{k,l}^{M} \varrho_{ijkl} \left|i\right\rangle\!\left\langle j\right| \otimes \left|k\right\rangle\!\left\langle l\right| \tag{3.4}$$

With this decomposition, one can define partial transposition with respect to each partition by

$$\varrho^{T^A} = \sum_{i,j}^{N} \sum_{k,l}^{M} \varrho_{ijkl} \left|j\right\rangle\!\left\langle i\right| \otimes \left|k\right\rangle\!\left\langle l\right| \tag{3.5}$$

$$\varrho^{T^B} = \sum_{i,j}^{N} \sum_{k,l}^{M} \varrho_{ijkl} \left|i\right\rangle\!\left\langle j\right| \otimes \left|l\right\rangle\!\left\langle k\right| \tag{3.6}$$

Given a density matrix ϱ, one can say that it is PPT if any of its partial transpositions ϱ^{T^A}, ϱ^{T^B} is positive semidefinite. Furthermore, it holds that ϱ^{T^A} is positive semidefinite if and only if ϱ^{T^B} is positive semidefinite. Now, it is possible to introduce PPT criterion.

Theorem 9 (PPT criterion)**.** *Every separable mixed state ϱ is PPT.*

Proof. Let ϱ be a separable mixed state, then $\varrho = \sum_i p_i \varrho_i^A \otimes \varrho_i^B$. Following the definition of partial transpose $\varrho^{T^A} = \sum_i p_i \left(\varrho_i^A\right)^T \otimes \varrho_i^B$ and that is again a mixed state. Since all mixed states are positive semidefinite, ϱ^{T^A} is positive semidefinite. Hence, ϱ is PPT. □

The PPT criterion provides a very powerful tool for detection of entanglement for mixed states while remaining simple. It can be shown that a matrix is positive semidefinite if and only if it has no negative eigenvalues. Therefore, if one finds a partial transpose of a density matrix that yields negative eigenvalues, one can say with certainty that the state is entangled. In fact, it was shown in Ref. [28] that for quantum systems of very low dimensions (2×2 and 2×3), the

criterion is complete. However, it was also shown that it is not complete already for quantum systems of dimensions 2×4. This result leads to the definition of bound entanglement that will be discussed in Section 3.3.

3.2.3 Positive, but not completely positive operator

A generalization of the PPT criterion leads to the notion of positive, but not completely positive operators. A linear operator Λ on set of all linear operators of a Hilbert space $\Lambda : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is *positive* if it maps hermitian operators to hermitian operators, preserves the adjoint operator $\Lambda(L^\dagger) = \Lambda(L)^\dagger$ and preserves positive semidefiniteness. A positive linear operator Λ is *completely positive* if it holds for all identity operators $\mathbb{I}_n^A$ that the operator given by $\mathbb{I}_n^A \otimes \Lambda$ is positive. Otherwise, Λ is positive but not completely positive operator.

As an example, consider the transposition operator. The operator is positive since it maps density matrices to density matrices but as was discussed in previous subsection, the partial transposition operator is not positive. Hence, the transposition operator is an instance of the set of positive, but not completely positive operators.

From the definition of tensor product linear operators, it can be seen that for a positive operator Λ and a separable mixed state $\varrho = \varrho^A \otimes \varrho^B$, the operators $\left(\mathbb{I}_n^A \otimes \Lambda\right)(\varrho)$ are positive

$$\left(\mathbb{I}_n^A \otimes \Lambda\right)(\varrho^A \otimes \varrho^B) = \mathbb{I}_n^A(\varrho^A) \otimes \Lambda(\varrho^B) = \varrho^A \otimes \Lambda(\varrho^B) \geq 0 \tag{3.7}$$

Therefore, the positive, but not completely positive operators can help tackle the task of entanglement detection. In particular, it was shown in Ref. [28] that a state ϱ is separable if and only if for each positive operator Λ, the operators $\left(\mathbb{I}_n^A \otimes \Lambda\right)(\varrho)$ are positive. Hence, the task of entanglement detection is in this sense equivalent to the task of classification of positive maps.

Apart from the transposition operator, there are many other examples of positive, but not completely positive operators. For instance, consider the following positive operator $\Lambda_r : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ called *reduction operator* defined by

$$\Lambda_r(\varrho) = Tr(\varrho) \cdot \mathbb{I}^A - \varrho \tag{3.8}$$

Since Λ_r is positive, then operator $\mathbb{I}_n \otimes \Lambda_R$ is positive for all separable states and hence, Λ_r can be utilised for entanglement detection. However, it was shown in Ref. [27] that reduction operator is decomposable to transposition operator and therefore, it can detect at most the same set of entangled states as PPT criterion[4]. To overcome this deficiency, for a unitary operator such that $U^T = -U$, the operator Λ_r can be extended to the following form

$$\Lambda'_r(\varrho) = Tr(\varrho) \cdot \mathbb{I}^A - \varrho - U\varrho^T U^\dagger \tag{3.9}$$

Operator Λ'_r is again positive, but not completely positive operator. Furthermore, the operator is not decomposable and can detect entangled states that are not detected by PPT operator although the unitary operators satisfying the given condition can only exist for Hilbert spaces of even dimensions.

3.2.4 Entanglement witnesses

All the criteria so far have assumed that density matrix of a mixed quantum state is known as it was required to modify the density matrix in order to detect the entanglement. To abstract from this assumption, one might want to define criterion that builds on the notion of measurement and in particular, observables.

Definition 15. Let $\mathcal{W}$ be an observable, $\mathcal{W}$ is *entanglement witness* if the following holds

$$Tr(\mathcal{W}\varrho_s) \geq 0 \qquad \text{for all separable states } \rho_s \tag{3.10}$$

$$Tr(\mathcal{W}\varrho_e) < 0 \qquad \text{for at least one entangled state } \rho_e \tag{3.11}$$

It follows from the definition that if $Tr(\mathcal{W}\varrho) < 0$, one can say with certainty that ϱ is entangled. Furthermore, entanglement witnesses have strong geometrical meaning. Since expectation value of a mixed state ϱ with respect to an observable $\mathcal{W}$ is defined by $Tr(\mathcal{W}\varrho)$ and the expectation value is linear with respect to mixed states, the set of states where $Tr(\mathcal{W}\varrho) = 0$ forms a hyperplane in the set of all mixed states, dividing the set of all states to entangled states and a

4. In fact, the reduction criterion is less powerful than the PPT criterion. However, it was shown that for the case of two qubits, it is still complete [27].

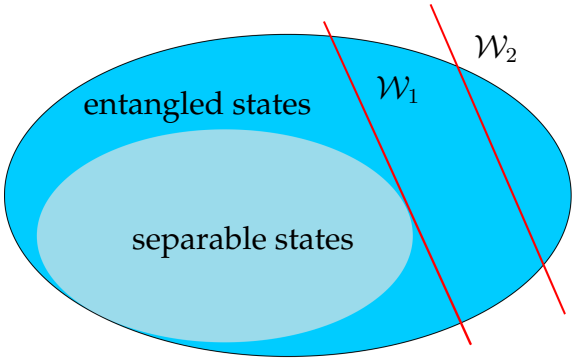

Figure 3.1: Geometrical representation of entanglement witnesses.

mixture of entangled and separable states as demonstrated in Figure 3.1. Consequently, it follows from the geometrical interpretation of witnesses as depicted in Figure 3.1 that it is possible to optimize an entanglement witness. A witness $\mathcal{W}_1$ is *finer* than witness $\mathcal{W}_2$ if $Tr(\mathcal{W}_2\varrho) < 0 \Rightarrow Tr(\mathcal{W}_1\varrho) < 0$ and there is an entangled state ϱ_e such that $Tr(\mathcal{W}_2\varrho_e) \geq 0$ and $Tr(\mathcal{W}_1\varrho_e) < 0$. In fact, this is the case if

$$\mathcal{W}_2 = \mathcal{W}_1 + P, \text{ where } P \text{ is a positive operator} \tag{3.12}$$

A witness $\mathcal{W}$ is *optimal* if there is no finer witness. Hence, it is optimal if there is no positive operator P such that observable $\mathcal{W} - P$ is a witness. It can be shown that a witness is optimal if and only if the set of product vectors $|\phi_i\rangle = |a_i b_i\rangle$ with expectation value equal to 0 spans the whole space. Geometrically, the optimal witnesses touch[5] the convex set of separable states. However, there are witnesses that touch the set of separable states and yet they are not optimal.

As was shown in Ref. [33] there is a procedure to obtain optimal witness from a given observable $\mathcal{W}$. However, it was shown in [45] that the procedure is in general equivalent to the separability problem. The existence of such a procedure still remains to be an important result and hence, the outline of the procedure will be presented, now.

5. Mathematically, the fact that a witness $\mathcal{W}$ touches the set of separable states means that there is a separable state ϱ_s such that $Tr(\mathcal{W}\varrho_s) = 0$.

1. Find a positive operator P such that $\langle a_i b_i|P|a_i b_i\rangle = 0$ for all product vectors where $\langle a_i b_i|\mathcal{W}|a_i b_i\rangle = 0$.

2. Find λ such that

$$\lambda \leq \lambda_0 = \inf_a \min_{eigenvalues} \left(\frac{1}{\sqrt{\langle a|P|a\rangle}} \langle a|W|a\rangle \frac{1}{\sqrt{\langle a|P|a\rangle}} \right) \quad (3.13)$$

3. $\mathcal{W}' = \mathcal{W} - \lambda P$ is a finer witness.

4. Repeat the procedure with $\mathcal{W}'$ if it is not already optimal.

The witnesses can also be constructed by violation of various separability criteria. Consider a state ϱ_e that violates the PPT criterion. Hence, there is a negative eigenvalue $\lambda < 0$ and a corresponding eigenvector $|\xi\rangle$ of $\varrho_e^{T^A}$. From the relation $Tr(XY^{T^A}) = Tr(X^{T^A}Y)$, it can be shown that $\mathcal{W} = |\xi\rangle\langle\xi|^{T^A}$ is an entanglement witness for ϱ_e as for all separable states ρ_s, the expectation value is positive

$$Tr\left(\mathcal{W}\varrho_e\right) = Tr(|\xi\rangle\langle\xi|^{T^A}\varrho_e) = Tr(|\xi\rangle\langle\xi|\,\varrho_e^{T^A}) = \lambda < 0$$
$$Tr\left(\mathcal{W}\varrho_s\right) = Tr(|\xi\rangle\langle\xi|\,\varrho_s^{T^A}) \geq 0$$

Furthermore, a generalization of this concept leads to the construction of an entanglement witness for an arbitrary positive, but not completely positive map. Let ϱ_e be an entangled state that is detected by a positive map Λ, then $\mathbb{I}\otimes\Lambda(\varrho_e)$ is not positive and hence, it has a negative eigenvalue λ and corresponding eigenvector $|\xi\rangle$. It can be shown that $\mathcal{W} = \mathbb{I}\otimes\Lambda^+(|\xi\rangle\langle\xi|)$[6] is entanglement witness for ϱ_e.

Therefore, witnesses are in general at least as powerful as any positive, but not completely positive operator and hence, in particular, PPT. In fact, witnesses are complete, i.e. for every entangled state ρ_e there is a witness $\mathcal{W}$ that detects the entangled state. This statement follows from completeness of positive but not completely positive maps and the fact that for each such an operator detecting an entangled state ϱ_e, there is a corresponding witness detecting the state ϱ_e.

6. Λ^+ is a unique linear operator such that for all X, Y, $Tr(\Lambda^+(X)Y) = Tr(X\Lambda(Y))$.

Furthermore, witnesses and positive operators are related by the notion of Choi-Jamiołkowski isomorphism – isomorphism between operators on $\mathcal{L}(\mathcal{H}^A)\otimes\mathcal{L}(\mathcal{H}^B)$ and operators from $\mathcal{L}(\mathcal{H}^A)$ to $\mathcal{L}(\mathcal{H}^B)$. For an operator $E : \mathcal{L}(\mathcal{H}^A) \otimes \mathcal{L}(\mathcal{H}^B) \to \mathcal{L}(\mathcal{H}^A) \otimes \mathcal{L}(\mathcal{H}^B)$ and an operator $\varepsilon : \mathcal{L}(\mathcal{H}^A) \to \mathcal{L}(\mathcal{H}^B)$, the isomorphism is given by the set of equations

$$\varepsilon(\varrho) = Tr^A(E\varrho^T \otimes \mathbb{I}^B) \tag{3.14}$$

$$E = \left(\mathbb{I}^{A'} \otimes \varepsilon\right)\left(\left|\phi^+\right\rangle\left\langle\phi^+\right|\right) \tag{3.15}$$

where Hilbert space $\mathcal{H}^A$ is isomorphic to $\mathcal{H}^{A'}$ and $|\phi^+\rangle = \sum_i |ii\rangle$ is a non-normalized maximally entangled state in $\mathcal{H}^{A'} \otimes \mathcal{H}^A$. Finally, the relation between witnesses and positive operators is given by properties of this isomorphism.

1. An operator ε is completely positive if and only if E is a positive semidefinite operator.

2. An operator ε is positive, but not completely positive operator if and only if E is an entanglement witness.

3. An operator ε is decomposable if and only if E is a decomposable[7] entanglement witness.

Furthermore, it can be shown that operator $\varepsilon(\mathcal{W})$ can detect more entangled states than witness $\mathcal{W}$ itself. The examples of these operators and states can de found in Ref. [8, 22, 34].

3.2.5 Other criteria

Many other criteria for entanglement detection have been proposed over the years. In this subsection, a brief overview of few of the proposed criteria will be provided.

Consider the Schmidt decomposition in Hilbert space of linear operators $\mathcal{L}(\mathcal{H}^A \otimes \mathcal{H}^B)$. For a density operator ϱ, orthonormal basis $\left\{G_j^A\right\} \subseteq \mathcal{L}(\mathcal{H}^A)$ and orthonormal basis $\left\{G_j^B\right\} \subseteq \mathcal{L}(\mathcal{H}^B)$, the Schmidt

7. Entanglement witness is decomposable if there are positive operators P_1, P_2 such that $\mathcal{W} = P_1 + P_2^{T^A}$.

decomposition of the operator ϱ is given by

$$\varrho = \sum_j \lambda_j G_j^A \otimes G_k^B \tag{3.16}$$

Consequently, one can formulate the *computable cross norm* or *realignment* (CCNR) criterion [22, 41]. If state ϱ is separable then it holds that the sum of all λ_j is at most 1, i.e. $\sum_j \lambda_j \leq 1$. Hence, if $\sum_j \lambda_j > 1$, then the state ϱ is entangled.

For the next criterion, let $(p_i)_{i=1}^n$ be a decreasingly ordered list of eigenvalues of a mixed state ϱ and $(q_i)_{i=1}^n$ be a decreasingly ordered list of eigenvalues of the reduced state $\varrho^A = Tr^B(\varrho)$, then *majorization* criterion [38] states that if ϱ is separable it holds for all $k \leq n$ that

$$\sum_{i=1}^{k} p_i \leq \sum_{i=1}^{k} q_i \tag{3.17}$$

Alternatively, the task of entanglement detection might be challenged algorithmically. In general, the algorithmic methods transform separability problem into optimization problems or semidefinite programs in order to derive algorithms for entanglement detection. In particular, the method of *symmetric extensions* [13,22] transforms separability problem into semidefinite programs. The concept of the method follows from the observation that if a state $\varrho^{AB} = \sum_i p_i \left|a_i\right\rangle\!\left\langle a_i\right| \otimes \left|b_i\right\rangle\!\left\langle b_i\right|$ is separable then there is a symmetric extension to three parties given by

$$\varrho^{ABC} = \sum_i p_i \left|a_i\right\rangle\!\left\langle a_i\right| \otimes \left|b_i\right\rangle\!\left\langle b_i\right| \otimes \left|a_i\right\rangle\!\left\langle a_i\right| \tag{3.18}$$

Consequently, from the extension it holds that the state ϱ^{ABC} is PPT with respect to each partition, reduced state of first two parties is given by ϱ and the state is symmetric under the exchange of partitions A and C. Hence, the task to find a symmetric extension that meets these three conditions can be formulated as a feasibility problem in semidefinite programming [49]. Furthermore, the generalization of the concept of symmetric extensions to n parties leads to hierarchy of separability criteria consecutively increasing in strength with n. Additionally, it was shown in Ref. [15] that for each entangled

state ϱ_e there is a symmetric extension to n parties detecting it. Hence, the criterion is complete in this sense.

For the last discussed criterion, let the range of a linear operator $L : \mathcal{H}^A \to \mathcal{H}^B$ be a set of all vectors $|\psi\rangle^B$ in Hilbert space $\mathcal{H}^B$ such that there is a vector $|\psi\rangle^A$ in Hilbert space $\mathcal{H}^A$ so that $|\psi\rangle^B = L\,|\psi\rangle^A$. Let $|a^*\rangle$ denote component-wise complex conjugation of a vector $|a\rangle$, the *range criterion* states that if a mixed state ϱ is separable then there is a set of product vectors $|a_i b_i\rangle$ that spans the range of ϱ while set $|a_i{}^* b_i\rangle$ spans the range of partial transpose ϱ^{T^B}. This criterion allows to detect entangled states that are not detected by PPT criterion and since it uses partial transpose it may be considered to be a next step after the application of PPT criterion for detection of entanglement in bipartite states.

3.3 Distillation

Let Alice and Bob be two distant parties sharing a bipartite mixed state ϱ^{AB}. If they want to perform one of many quantum protocols, it is highly likely that they will need a Bell state $|\Phi^+\rangle$. The question arises whether, given n copies of a state, it is possible for them to transform a mixed state ϱ^{AB} to the pure state $|\Phi^+\rangle\langle\Phi^+|^{AB}$ by the means of $LOCC$ transformations – whether the state ϱ^{AB} is *distillable* or not. Furthermore, from the classification of entanglement for pure two-qubit states, it follows that pure state $|\Phi^+\rangle$ is the most general two-qubit pure state and hence, it can be transformed into any other pure two-qubit state.

Since all the pure states are also mixed states, the existence of distillable states follows from the existence of Bell $|\Phi^+\rangle$ state. However, it is more difficult to show the existence of distillable mixed states that are not pure. This statement of the problem comes from the environment of laboratories and quantum channels where in general, only mixtures of pure states are being prepared and transferred. Additionally, the condition of optimality of an entanglement distillation protocol can be imposed. A distillation protocol is said to be *optimal* if it maximizes the ratio of the number of distilled states to the number of copies of the mixed states. Given a mixed state ϱ, E_D denotes the maximal ratio corresponding to an optimal distillation protocol

for the mixed state ϱ.

Several protocols to tackle this task have been designed over the years. In order to demonstrate the existence of impure distillable mixed states and in order to provide an example of distillation protocol, the first protocol that was proposed in this context known as recurrence protocol [6] will be presented. Let Alice and Bob share n copies of a Werner state ϱ_W. The Werner state ϱ_W is a probabilistic mixture of Bell states and it is given by

$$\varrho_W = W\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1-W}{3}\left(\left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) \tag{3.19}$$

If Alice and Bob take first two Werner states, Alice will be in possession of first and third qubit and Bob will be in possession of second and fourth qubit. Since they can perform local operations on the two qubits that they possess, it is advisable to change the order of the second and third qubit making it possible to use local operations of form $U^A \otimes U^B$. This can be done with help of $SWAP$ operator. The operator that modifies the order of qubits as can be seen from its definition

$$SWAP = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \tag{3.20}$$

In particular, to change the order of second and third qubit, operator $\mathbb{I}_2 \otimes SWAP \otimes \mathbb{I}_2$ may be applied. Consequently, Alice and Bob may both apply $CNOT$ operators (Eq. 2.13) on their respective qubits by application of several unitary operators resulting in bilateral $CNOT$ unitary operator ($BCNOT$)

$$BCNOT = (\mathbb{I}_2 \otimes SWAP \otimes \mathbb{I}_2)\,(CNOT \otimes CNOT)\,(\mathbb{I}_2 \otimes SWAP \otimes \mathbb{I}_2) \tag{3.21}$$

Furthermore, from the linearity of unitary operators, the application of the operator $BCNOT$ to a mixed state reduces to application of $BCNOT$ to every pure state and hence, it can be described by table of all the possible pure state cases that can occur (Table 3.1). Following the application of $BCNOT$ operator, per qubit measurements with respect to the computational basis are performed on third and fourth qubit. Consequently, they communicate the results of measurements to differentiate $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$

$BCNOT$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
$\|\Phi^+\rangle$	$\|\Phi^+\rangle \otimes \|\Phi^+\rangle$	$\|\Phi^-\rangle \otimes \|\Phi^+\rangle$	$\|\Psi^+\rangle \otimes \|\Psi^+\rangle$	$\|\Psi^-\rangle \otimes \|\Psi^+\rangle$
$\|\Phi^-\rangle$	$\|\Phi^-\rangle \otimes \|\Phi^-\rangle$	$\|\Phi^+\rangle \otimes \|\Phi^-\rangle$	$\|\Psi^-\rangle \otimes \|\Psi^-\rangle$	$\|\Psi^+\rangle \otimes \|\Psi^-\rangle$
$\|\Psi^+\rangle$	$\|\Phi^+\rangle \otimes \|\Psi^+\rangle$	$\|\Phi^-\rangle \otimes \|\Psi^+\rangle$	$\|\Psi^+\rangle \otimes \|\Phi^+\rangle$	$\|\Psi^-\rangle \otimes \|\Phi^+\rangle$
$\|\Psi^-\rangle$	$\|\Phi^-\rangle \otimes \|\Psi^-\rangle$	$\|\Phi^+\rangle \otimes \|\Psi^-\rangle$	$\|\Psi^-\rangle \otimes \|\Phi^-\rangle$	$\|\Psi^+\rangle \otimes \|\Phi^-\rangle$

Table 3.1: Table of all possible cases of $BCNOT$ unitary operator applied to a Werner state. The column states describe first and second qubit, row states describe third and fourth qubit.

states. Whenever one of the states $|\Psi^{\pm}\rangle$ occurs, all the qubits get discarded. Hence, only the four states in upper left quarter of Table 3.1 and the four states in lower right quarter of the table will remain after this step. Computing the probabilities, one gets the probability W' of getting state $|\Phi^+\rangle$ after application of $BCNOT$ operator to Werner state ϱ_W by

$$W' = \frac{W^2 + \left(\frac{1-W}{3}\right)^2}{W^2 + 5\left(\frac{1-W}{3}\right)^2 + 2W\frac{1-W}{3}} \tag{3.22}$$

The denominator in the equation serves as a normalization factor and it is a sum of the probabilities of each of the eight states that does not get discarded occurring. Consequently, solving the equation $W' - W > 0$, one gets that the probability W' is higher than probability W in Werner state ϱ_W for W in interval $(0.5, 1)$. Furthermore, the state after the application of $BCNOT$ operator may be transformed to Werner state by equalization of probabilities of remaining pure states in the mixture [7] and the protocol may be applied ad infinitum resulting in a mixture ϱ_W with W arbitrarily close to 1. However, this protocol is relatively lavish and does not achieve the optimal distillation ratio E_D.

The subsequent research in this area yielded remarkable results showing the relation between distillable and entangled states. All states violating reduction criterion are distillable [24, 27] and even more remarkably all PPT states are not distillable [29]. Since the PPT criterion is not complete for arbitrary bipartite quantum states, from the statement it implies that there are entangled states that are not distillable. These states are referred to as *bound entangled states*. The construction of bound entangled states may be demonstrated by the

states forming *unextendible product basis*.

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle) \qquad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|2\rangle$$
$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|2\rangle(|1\rangle - |2\rangle) \qquad |\psi_3\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)|0\rangle$$
$$|\psi_4\rangle = \frac{1}{3}(|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle)$$

All the pure states $|\psi_i\rangle$ are mutually orthogonal and no other pure product state is orthogonal to all of them. Consequently, consider the mixed state ϱ_e given by

$$\varrho_e = \frac{1}{4}\left(\mathbb{I} - \sum_{i=0}^{4}|\psi_i\rangle\langle\psi_i|\right) \tag{3.23}$$

The partial transpose $\varrho_e^{T^B}$ of the state is equal to the original state and hence the state is PPT. However, by the range criterion, there is no product vector in the range of the mixed state and hence, the state ϱ_e is bound entangled.

The set of bound entangled states as the set of states that cannot be transformed to pure entangled states suggests that the states may have no practical applications. However, amazingly, it was shown in Ref. [25, 26] that bound entangled states may be used for secure quantum key distribution. Consequently, one might wonder whether there is a classical counterpart of bound entangled states in cryptography. Are there classical probability distributions between several parties that require secrecy for their creation but the secrecy can not be distilled back? [20] Deriving the probability distributions from a bound entangled state, it was shown that there are probability distributions such that the secrecy is not distillable [3].

4 Tripartite entanglement

In this chapter, we will discuss the entanglement of three parties and the current state of the tasks of entanglement classification, detection and distillation in the case when three parties are involved. Consequently, the definitions of entanglement need to be refined in order to include the possibility of three parties. For a pure tripartite state $|\psi\rangle^{A|B|C}$ in Hilbert space $\mathcal{H}^{ABC} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C$, we define the notion of full separability. The pure state $|\psi\rangle^{A|B|C}$ is *fully separable* if there are pure states $|\psi\rangle^A \in \mathcal{H}^A$, $|\psi\rangle^B \in \mathcal{H}^B$, $|\psi\rangle^C \in \mathcal{H}^C$ such that

$$|\psi\rangle^{A|B|C} = |\psi\rangle^A \otimes |\psi\rangle^B \otimes |\psi\rangle^C \tag{4.1}$$

Consequently, one might group two out of the three possible parties making a pure tripartite state bipartite. In this case, the definition of biseparability follows from the definition of separability in bipartite entanglement and the relation between the partitions is given by | sign. Hence, a pure state $|\psi\rangle^{A|BC}$ is biseparable with respect to the bipartition $\left\{\mathcal{H}^A, \mathcal{H}^B \otimes \mathcal{H}^C\right\}$ if it is separable with respect to the bipartition. Since there are three ways to group two of the partitions together, for the remaining two cases, the states $|\psi\rangle^{B|AC}$ and $|\psi\rangle^{C|AB}$ are biseparable with respect to bipartitions $\left\{\mathcal{H}^B, \mathcal{H}^A \otimes \mathcal{H}^C\right\}$ and $\left\{\mathcal{H}^C, \mathcal{H}^A \otimes \mathcal{H}^B\right\}$ respectively if they are separable with respect to the respective bipartitions. Finally, a pure state $|\psi\rangle \in \mathcal{H}^{ABC}$ is *tripartite entangled* if it is not biseparable with respect to an arbitrary bipartition.

The extension to mixed states yields the necessity of convex mixtures for the definition of their separability. A mixed state ϱ^{fs} is fully separable if it can be written as a convex combination of fully separable pure states $|\psi_i\rangle^{A|B|C}$.

$$\varrho^{fs} = \sum_i p_i \, |\psi_i\rangle\langle\psi_i|^{A|B|C} \tag{4.2}$$

Consequently, biseparable mixed states are convex mixtures of biseparable pure states $|\psi_i\rangle$. Furthermore, it is allowed to mix all the bipartitions of the pure states in a single mixed state and hence, this definition does not differentiate the bipartitions. Finally, a mixed state ϱ_e is tripartite entangled if it is not biseparable.

4.1 Classification

For the task of classification of entanglement of tripartite entanglement, it is again possible to consider the classification with respect to the LOCC transformations. However, already in bipartite case, the transformations yielded infinitely many classes. As there was a state that could be transformed to any other state, this classification was sufficient for bipartite case. However, for tripartite entanglement such a state is non-existent. Hence, for tripartite case, we will further refine the classification method by introducing stochastic LOCC (SLOCC) transformations.

The strict LOCC transformations require absolute certainty of the transformations and hence, they do not allow any error in transformation protocol. Therefore the strict LOCC transformations do not allow measurements that would introduce such an error to occur and in particular, they are equivalent solely to local unitary transformations. However, a measurement may provide an outcome such that the consequent protocol may branch with respect to the outcome. The class of stochastic LOCC transformations allows each such a branch to be treated as a separate transformation protocol. For each branch, there is a probability of the branch occurring. Hence, two states are related by SLOCC transformations if they may be utilized for same class of tasks, however, the probability of success of the task in the class is permitted to differ.

Mathematically, SLOCC transformations may be represented by invertible local operators (ILO) as will now be demonstrated. Let $|\psi\rangle$, $|\phi\rangle$ be two vectors in Hilbert product space $\mathcal{H}^A \otimes \mathcal{H}^B$ and let d^A, d^B be the dimensions of the partitions. If there is an operator A such that

$$|\phi\rangle = A \otimes \mathbb{I}^B |\psi\rangle \tag{4.3}$$

then for the ranks of reduced density matrices it always holds that $rk(|\psi\rangle\langle\psi|^A) \geq rk(|\phi\rangle\langle\phi|^A)$ and $rk(|\psi\rangle\langle\psi|^B) \geq rk(|\phi\rangle\langle\phi|^B)$. In order to demonstrate this, consider an arbitrary operator A and a Schmidt decomposition of $|\psi\rangle$

$$A = \sum_{i=1}^{d^A} |\chi_i\rangle\langle i^A| \qquad\qquad |\psi\rangle = \sum_{i=1}^{rk(|\psi\rangle)} \lambda_i |i^A\rangle |i^B\rangle \tag{4.4}$$

where $|\chi_i\rangle$ are arbitrary vectors over $\mathcal{H}^A$. Therefore, the computation of reduced density matrices yields $|\psi\rangle\langle\psi|^A = \sum_i \lambda_i^2 \left|i^A\right\rangle\left\langle i^A\right|$ and $|\phi\rangle\langle\phi|^A = A\,|\psi\rangle\langle\psi|^A\,A^\dagger = \sum_i \lambda_i^2\,|\chi_i\rangle\langle\chi_i|$. Therefore, the first inequality holds and in particular, $rk(|\psi\rangle\langle\psi|^A) \geq rk(|\phi\rangle\langle\phi|^A)$. The second inequality follows from the fact that ranks of reduced density matrices are invariant. In particular, it holds that $rk(|\psi\rangle\langle\psi|^A) = rk(|\psi\rangle\langle\psi|^B)$ and $rk(|\phi\rangle\langle\phi|^A) = rk(|\phi\rangle\langle\phi|^B)$.

Furthermore, let $I = \{A, B, C, \ldots\}$ be a finite set of partitions and let $|\psi\rangle$, $|\phi\rangle$ be states over Hilbert product space of the partitions $\bigotimes_{i\in I} \mathcal{H}_i$, then there are numerous bipartitions to be considered. Hence, as a corollary of the bipartite case, this generalization for states $|\psi\rangle$, $|\phi\rangle$ yields the set of inequalities over index set I where for all $i \in I$, $rk(|\psi\rangle\langle\psi|^i) \geq r(|\phi\rangle\langle\phi|^i)$. Consequently, from the invertibility of local operators, it follows that the ranks of reduced density matrices are invariant under ILO. Finally, this leads to the theorem showing the relation between SLOCC transformations and invertible local operators.

Theorem 10. *Let $\mathcal{H} = \bigotimes_{i\in I} \mathcal{H}_i$ be a Hilbert product space of parties $I = \{A, B, C, \ldots\}$. Two pure states over the Hilbert space $\mathcal{H}$ are equivalent with respect to SLOCC transformations if and only if there is an invertible local operator relating them.*

Proof. ($\Leftarrow$) Let linear operator $L \in \mathcal{L}(\mathcal{H})$ be an arbitrary local linear operator $L = \bigotimes_{i\in I} L_i$ relating states $|\psi\rangle$, $|\phi\rangle \in \mathcal{H}$

$$|\phi\rangle = \left(\bigotimes_{i\in I} L_i\right)|\psi\rangle \tag{4.5}$$

Consequently, it is possible to design a set of local measurement operators for each partition $i \in I$ by normalization of linear operators corresponding to the partition i. For partition i, the set given by $\left\{\sqrt{p_i}L_i, \sqrt{\mathbb{I}_i - p_i {L_i}^\dagger L_i}\right\}$ where $p_i {L_i}^\dagger L_i \leq \mathbb{I}_i$ and $0 \neq p_i \leq 1$ forms the set of measurement operators for partition i. Hence, this protocol transforms $|\psi\rangle$ to $|\phi\rangle$ by stochastic LOCC. Conversely, from the assumption, that the operators are invertible, there is a linear operator $L^{-1} = \bigotimes_{i\in I} L_i^{-1}$ relating the two states in reversed order. Hence, the

set of measurement operators transforming state $|\phi\rangle$ to $|\psi\rangle$ may be designed. Therefore, $|\psi\rangle$ and $|\phi\rangle$ are in same equivalence class.

($\Rightarrow$) If $|\psi\rangle$ can be transformed to $|\phi\rangle$ by SLOCC, then there is a series of rounds of local operations intersected by classical communication preceded by application of measurement operators and hence, there is a local operator relating them. We will now proceed to demonstrate that there is an invertible local operator relating them. For each linear operator L_i we can consider local linear operator $L = \bigotimes_{j\in I} L_j$ acting solely on partition i having identity operators for every other partition given by

$$L_j = \begin{cases} \mathbb{I}_j & \text{if } i \neq j \\ L_i & \text{if } i = j \end{cases} \tag{4.6}$$

Consequently, Hilbert space $\mathcal{H}$ may be treated as bipartite grouping all the partitions where $L_j = \mathbb{I}_j$ to a single partition. Hence, the Schmidt decomposition of states $|\psi\rangle$ and $|\psi'\rangle = L\,|\psi\rangle$ yields

$$|\psi\rangle = \sum_{j=1}^{rk(|\psi\rangle)} \lambda_j\,|j\rangle\,|\tau_j\rangle \qquad\qquad |\psi'\rangle = \sum_{j=1}^{rk(|\psi'\rangle)} \lambda'_j(U_i\,|j\rangle)\,|\tau_j\rangle$$

where U_i is a unitary operator relating the orthonormal bases before and after the application of linear operator L and τ_j form an orthonormal basis. Furthermore, the ranks of the states are invariant as was discussed earlier. Therefore, $rk(|\psi\rangle) = rk(|\psi'\rangle)$. Consequently, this provides the necessary form of linear operator L given by $L = U_i(M + N)$ where M and N are linear operators such that

$$M = \sum_{j=1}^{rk(|\psi\rangle)} \frac{\lambda'_j}{\lambda_j}\,|j\rangle\langle j| \qquad\qquad N = \sum_{j=rk(|\psi\rangle)+1}^{d_i} |\chi_j\rangle\langle j| \tag{4.7}$$

where $|\chi_j\rangle$ are arbitrary vectors and d_i is the dimension of partition i. Since operator N does not modify the original state, then operator N' such that the vectors $|\chi_j\rangle$ are chosen to be exactly $|j\rangle$ states is equivalent to operator L and eminently, $U_i(M + N')$ is invertible. Finally, composition of invertible operators designed for all the L_i operators yields an invertible operator equivalent to the original operator that transformed $|\psi\rangle$ to $|\phi\rangle$. Therefore if two states are equivalent with respect to SLOCC, there is an ILO relating them. □

The equivalence of SLOCC transformations and invertible local operators provides a valuable mathematical framework for entanglement classification. Hence, we can finally analyse the entanglement relations of three qubits. The simplest case yields the class of fully separable states $|\psi\rangle^{A|B|C} = |\psi\rangle^{A} |\psi\rangle^{B} |\psi\rangle^{C}$. Analogously to two-qubit case, all the fully separable three-qubit states are related by local unitary operations $U^A \otimes U^B \otimes U^C$ and hence, they are related by invertible local operators. Furthermore, the reduced density matrices of all qubits correspond to the density matrices of the consecutive qubits and hence, the ranks are invariant and of unit one.

Consequently, it is possible to consider all the biseparable but not fully separable states that may occur. For three qubits, this yields three mutually inequivalent classes depending on the qubit that is not entangled with the remaining two qubits. In order to demonstrate this it is necessary to observe that for biseparable but not fully separable states, there are always two partitions such that the states are separable with respect to the partitions. The first partition consists of a single qubit and the latter consists of an entangled pair. Consequently, we may study the ranks of all three qubits to demonstrate that there are at least three inequivalent biseparable but not full separable classes. The singled out separable qubit is always of rank one while the remaining two qubits are mutually entangled and hence, they are of rank two. Since the ranks of the qubits are invariant under SLOCC and there are three possibilities to single out a qubit from a triplet of qubits, there are at least three inequivalent biseparable but not fully separable classes of states. Furthermore, since all the entangled two-qubit pairs are equivalent under SLOCC and all the single qubits are equivalent under SLOCC, two biseparable but not fully separable states are separable with respect to same partitions if they are equivalent under SLOCC. Therefore, there are exactly three biseparable but not fully separable classes.

Finally, all the biseparable states have been classified and hence, solely genuinely entangled three-qubit states are left to be analysed and classified. In particular, it will be shown that two three-qubit genuinely entangled states, GHZ and W, are of a special interest for the task of classification of genuinely entangled three-qubit states.

The description of the states follows.

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{4.8}$$

$$|W\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right) \tag{4.9}$$

Initially, we note that minimal number of terms in product decomposition of a three-qubit state is invariant under SLOCC as the local operators are invertible and hence, they preserve linear independence. It follows from the fact that entangled states must have at least two product states in their product decomposition and Equation 4.8 that the minimal number of terms in product decomposition of GHZ state is two. Furthermore, the Equation 4.9 yields the upper bound on minimal number of terms in product decomposition of W state. As W state is also entangled, the minimal number of terms in product decomposition is either two or three.

Consequently, let $\sum_{i=1}^{i} \alpha_i |a_i\rangle |b_i\rangle$ be a product decomposition of a bipartite state $|\psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$, then the set of states $\{|a_i\rangle\}_{i=1}^{n}$ spans the range of reduced density matrix $|\psi\rangle\langle\psi|^A$ as will now be shown. From the definition of trace out operation and linearity it follows that

$$|\psi\rangle\langle\psi|^A = \sum_{i,j} \alpha_i \alpha_j \langle b_i|b_j\rangle |a_j\rangle\langle a_i| \tag{4.10}$$

A state $|\chi\rangle$ is in range of a density matrix ϱ if and only if there is a state $|\phi\rangle$ such that $|\chi\rangle = \varrho |\phi\rangle$. Finally, for density matrix $|\psi\rangle\langle\psi|^A$, computation of range of the matrix yields the set of states that is spanned by states in $\{|a_i\rangle\}_{i=1}^{n}$

$$|\psi\rangle\langle\psi|^A |\phi\rangle = \sum_{i,j} \alpha_i \alpha_j \langle b_i|b_j\rangle \langle a_i|\phi\rangle |a_j\rangle \tag{4.11}$$

In particular, the trace out operation on first qubit of W state yields state $|W\rangle\langle W|^{BC}$ (Eq. 4.12). Hence, the range of the matrix is spanned by set $\{|01\rangle + |10\rangle, |00\rangle\}$ and thus by the previous lemma, there is only one product state in range of W state.

$$|W\rangle\langle W|^{BC} = \frac{1}{3}\left(|01+10\rangle\langle 01+10| + |00\rangle\langle 00|\right) \tag{4.12}$$

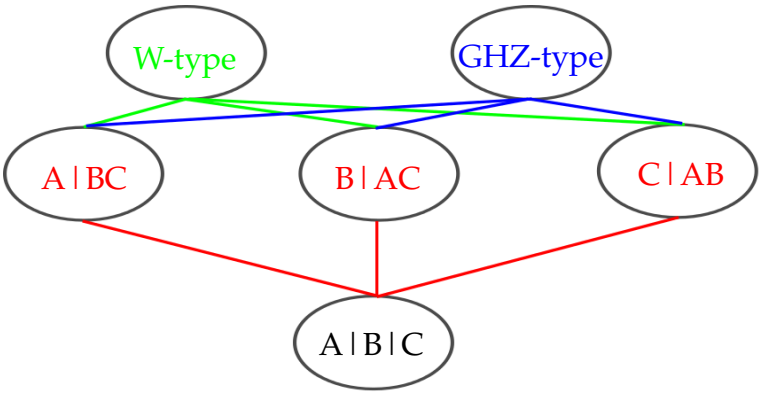

Figure 4.1: The 6 inequivalent classes of three pure qubits under SLOCC.

Consequently, we may proceed to show that the minimal number of terms in product decomposition of W state is exactly three and hence, from the invariance of the number under SLOCC, it will follow that W state and GHZ state are not equivalent under SLOCC. A general minimal product decomposition of two terms of a state $|\psi\rangle$ is given by two linearly independent vectors

$$|\psi\rangle = |a_1\rangle\,|a_2\rangle\,|a_3\rangle + |b_1\rangle\,|b_2\rangle\,|b_3\rangle \tag{4.13}$$

In particular, for W state, it follows that set $\{|a_2\rangle\,|a_3\rangle\,, |b_2\rangle\,|b_3\rangle\}$ have to span the range of $|W\rangle\langle W|^{BC}$. Furthermore, the vectors $|a_2\rangle\,|a_3\rangle$ and $|b_2\rangle\,|b_3\rangle$ have to be linearly independent for genuinely entangled states, since otherwise, the state would be separable. Hence, there must be two product states in range of $|W\rangle\langle W|^{BC}$. However, it was already shown that the range of $|W\rangle\langle W|^{BC}$ contains only one product state and thus, the minimal number of terms in product decomposition of W state may not be of value two. Therefore, the minimal number is exactly three and state W is not equivalent with state GHZ under SLOCC.

Finally, as was shown in Ref. [16], any genuinely entangled three-qubit state with two product terms in minimal product decomposition is equivalent to the GHZ state under SLOCC and any other genuinely entangled three-qubit state is equivalent to the W state under SLOCC. Hence, there are no more classes of genuine three-

qubit entangled states under SLOCC and in particular, there are no more classes of three-qubit states under SLOCC. The complete classification is depicted in Figure 4.1. The arrows in figure are given by non-invertible local operators that allow to lower ranks. If there is an arrow from higher level to lower level then the states of set in higher level may be transformed by SLOCC to states of set in lower level. However, the opposite transformation is not possible as the rank would have to grow in these cases. The absence of arrows connecting W-type and GHZ-type states implies the mutual exclusiveness of the states in respective classes.

Furthermore, it may be shown that the W-type pure states are of measure zero in set of all pure states. This statement follows from a generalization of Schmidt decomposition for three qubits [1]. The generalization states that any pure three-qubit state may be transformed by local unitary operators to state

$$\alpha_0 |000\rangle + \alpha_1 e^{i\theta} |100\rangle + \alpha_2 |101\rangle + \alpha_3 |110\rangle + \alpha_4 |111\rangle \tag{4.14}$$

where all α_i are non-negative, sum in squares to one and $\theta \in [0, \pi]$. However, the decomposition of W-type states yields $\theta = \alpha_4 = 0$ and hence, the class is of measure zero in set of all pure states.

4.2 Detection

In contrast to bipartite entanglement, the task of detection of entanglement for tripartite states is more comprehensive. If it were to suffice to simply detect whether a given tripartite state is entangled or separable, the task could be in fact tackled by criteria designed for detection of bipartite entanglement with respect to all the possible bipartitions. However, the requirement of detection of particular entanglement class is imposed and therefore, the answer to this task in tripartite case includes the type of entanglement that occurred.

Consequently, it is crucial to note that for mixed states, the division of the state space yields distinct results. There are still two classes of genuinely entangled states. The first being the set of genuinely entangled convex combinations of pure W-type states known as mixed W-type states and the latter being the set of all the other

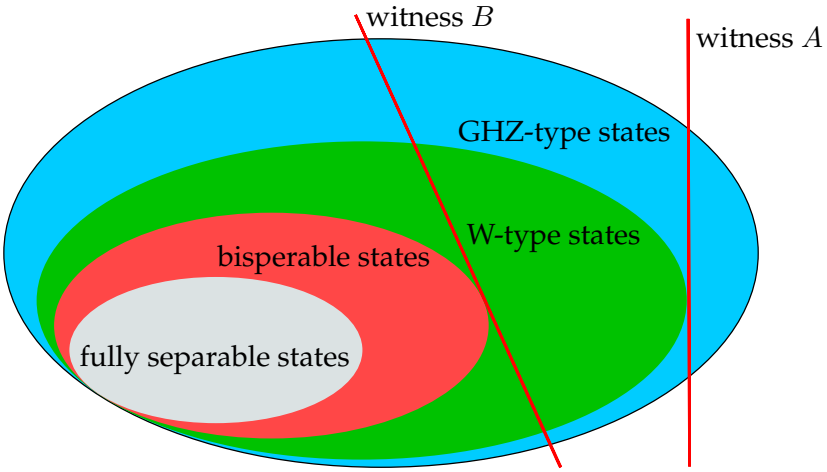

Figure 4.2: The convex relations of mixed tripartite states and application of witnesses for detection of genuine tripartite entanglement classes.

genuinely entangled tripartite mixed states known as mixed GHZ-type states. However, the set of mixed W-type forms a convex set inside the set of GHZ-type mixed states and is no longer of measure zero in comparison to GHZ class [2].

In bipartite case, entanglement witnesses were introduced as a valuable and complete tool for the task of detection of bipartite entanglement. Furthermore, this tool may be refined for detection of entanglement of three qubits. In bipartite case, all separable states must have yielded non-negative expectation values. However, the case expected there to be solely two convex classes. As depicted in Figure 4.2, for three qubits we deal with finer allocation of state space. Hence, in order to detect GHZ-type entangled states, we need to refine the condition to rule out all W-type, biseparable and fully separable states as depicted by witness A in Figure 4.2. Therefore for all such states, the witness must yield non-negative expectation value. Consequently, if the witness yields negative expectation value, the state is a GHZ-type state. The following observable may serve as an example of a witness detecting solely GHZ-type states.

$$\mathcal{W}_{GHZ} = \frac{3}{4}\mathbb{I} - |GHZ\rangle\langle GHZ| \tag{4.15}$$

The construction of such a witnesses will be further discussed in Section 5.2. Furthermore, it is also possible to detect genuinely entangled three-qubit states by softening the condition for three-qubit witnesses and allowing W-type mixed states to be detected as depicted by witness B in Figure 4.2. However, witnesses were originally designed to prove that a state lies outside of a convex set. Hence, while witness A successfully detects GHZ-type states, witness B can not be applied directly for detection of W-type entangled states as it detects also GHZ-type entangled states. The application of witnesses for detection of W-type states may have not seen to be very promising. However, we will now proceed to outline the idea that makes the witnesses a practical tool for detection of mixed W-type states.

The task to detect W-type mixed states may be divided into two subtasks. The first, showing that a state lies outside of the convex set of biseparable states by entanglement witnesses and the latter, showing that the state lies inside of the convex set of W-type states. Hence, the task reduces to the task of showing that a given state lies inside of a convex set, in particular the convex set of W-type states in this case. Initially, an algorithm to show that a state is separable was designed in Ref. [4]. Consequently, the algorithm was generalized to provide a tool to show that a state belongs to a more general convex set $conv(C)$ of convex combinations of pure states over a set C [30]. The algorithm employs two crucial facts. First, the convexity of the set as it holds that any convex combination of the states of set $conv(C)$ lies in set $conv(C)$. Hence, if mixed states ϱ_1, ϱ_2 are in $conv(C)$ then also state $\varrho = p\varrho_1 + (1-p)\varrho_2$ is in $conv(C)$. In particular, it follows that state ϱ_2 may be expressed by

$$\varrho_2 = \frac{1}{1-p}\left(\varrho - p\varrho_1\right) \tag{4.16}$$

Consequently, one can show that state ϱ is in $conv(C)$ if a state that arises by subtraction of a state in $conv(C)$ is in $conv(C)$. Afterwards, the second fact states that highly mixed states are in $conv(C)$ and is highly dependent on the structure of set C. This fact acts as a criterion to decide whether a state obtained by subtraction of a state in $conv(C)$ is in fact in $conv(C)$. Finally, an outline of the algorithm may be presented.

1. Find a pure state $|\psi\rangle\langle\psi|$ in C with high overlap with input state ϱ.

2. Find a probability p (Eq. 4.16) that brings the state ϱ_2 closer to the set of highly mixed states.

3. Check if the state ϱ_2 is a highly mixed state. On success, output that the state is in $conv(C)$ and halt.

4. Repeat the algorithm with the subtracted state ϱ_2 as an input.

The completeness of such a process is certainly doubtful. However, in the paper that introduced this algorithm, it was demonstrated that the algorithm shows promising experimental results.

4.3 Distillation

The task of entanglement classification relies on a single copy of a state to perform necessary operations. However, the task of entanglement distillation provides the possibility to use several copies of the state. Amazingly, with just two copies of W-type states, it is possible to probabilistically reconstruct GHZ state as will now be demonstrated. By SLOCC, one can obtain two copies of $|W\rangle$ state from two copies of arbitrary W-type states. Hence, after the application of invertible local operators relating the states, there are two copies of state $|W\rangle$ shared among three parties A, B, C. This yields the state $|W\rangle \otimes |W\rangle$ that after the permutation of qubits may be written as

$$\begin{aligned}
&\frac{1}{3}\left|00^A\right\rangle\left(\left|00^B11^C\right\rangle+\left|11^B00^C\right\rangle+\left|01^B10^C\right\rangle+\left|10^B01^C\right\rangle\right)\\
&+\frac{1}{3}\left|01^A\right\rangle\left(\left|00^B10^C\right\rangle+\left|10^B00^C\right\rangle\right)\\
&+\frac{1}{3}\left|10^A\right\rangle\left(\left|00^B01^C\right\rangle+\left|01^B00^C\right\rangle\right)\\
&+\frac{1}{3}\left|11^A\right\rangle\left(\left|00^B00^C\right\rangle\right)
\end{aligned}$$

Consequently, Alice may perform measurement defined by set of measurement operators $\{|01\rangle\langle 01|+|10\rangle\langle 10|, |00\rangle\langle 00|+|11\rangle\langle 11|\}$ and

continue only if the outcome indicates that the first measurement operator was applied. Hence, the state gets transformed to state

$$\frac{1}{2}\left|01^A\right\rangle\left(\left|00^B10^C\right\rangle+\left|10^B00^C\right\rangle\right)+\frac{1}{2}\left|10^A\right\rangle\left(\left|00^B01^C\right\rangle+\left|01^B00^C\right\rangle\right) \tag{4.17}$$

Similarly, Bob may perform measurement defined by set of measurement operators $\{|00\rangle\langle 00|+|10\rangle\langle 10|,|01\rangle\langle 01|+|11\rangle\langle 11|\}$ and continue only if first measurement operator was applied. The application of the operator may be seen as an operation that filters the state $\left|10^A01^B00^C\right\rangle$ out of decomposition in Eq. 4.17. Charlie may perform filtering measurement defined by set of measurement operators $\{|00\rangle\langle 00|+|01\rangle\langle 01|,|10\rangle\langle 10|+|11\rangle\langle 11|\}$ continuing only if the first measurement operator was applied. Hence, the state gets transformed to state

$$\frac{1}{\sqrt{2}}\left(\left|01^A10^B00^C\right\rangle+\left|10^A00^B01^C\right\rangle\right) \tag{4.18}$$

Finally, by local unitary operators reversibly mapping $\left|01^A\right\rangle$ to $\left|00^A\right\rangle$, $\left|10^B\right\rangle$ to $\left|00^B\right\rangle$ and $\left|01^C\right\rangle$ to $\left|10^C\right\rangle$, this state may be transformed to a single copy of GHZ state

$$\frac{1}{\sqrt{2}}\left(\left|00^A00^B00^C\right\rangle+\left|10^A10^B10^C\right\rangle\right)=\left|GHZ^{ABC}\right\rangle\otimes\left|0^A0^B0^C\right\rangle \tag{4.19}$$

Conversely, it was shown in Ref. [51] that one may obtain W state out of GHZ state with arbitrary precision and hence, the two states are equivalent with respect to the task of entanglement distillation. Therefore, there is no need to divide the task of tripartite entanglement distillation to two subtasks. Finally, the task may be formulated as the task to decide whether the transformation of numerous copies of mixed state ϱ to state $|GHZ\rangle\langle GHZ|\otimes\varrho'$ is possible by LOCC.

Consequently, one may study the relation between distillability and genuine entanglement. Analogously to the bipartite case, there are genuinely entangled tripartite states that are not distillable [35]. Furthermore, amazingly, there are biseparable three-qubit states that are tripartite distillable. In order to demonstrate this fact, one may consider the state ϱ^{bs} given by the following convex combination of

three biseparable states

$$\varrho^{bs} = \frac{1}{3}\Big(\big|\Phi^+\big\rangle\big\langle\Phi^+\big|^{AB} \otimes |0\rangle\langle 0|^C + \big|\Phi^+\big\rangle\big\langle\Phi^+\big|^{AC} \otimes |0\rangle\langle 0|^B + \big|\Phi^+\big\rangle\big\langle\Phi^+\big|^{BC} \otimes |0\rangle\langle 0|^A\Big)$$

The state violates the PPT criterion in each bipartition and hence, it is two-qubit distillable. Therefore, the three parties may distill entangled Bell pairs $|\Phi^+\rangle^{AB}$ and $|\Phi^+\rangle^{AC}$. Finally, Alice may prepare the GHZ state locally and by extension of the entanglement swapping protocol discussed in Subsection 2.5.2, Alice may swap the second qubit from entangled pair $|\Phi^+\rangle^{AB}$ with second qubit of GHZ state and the second qubit from entangled pair $|\Phi^+\rangle^{AC}$ with third qubit of GHZ state. Hence, Alice, Bob and Charlie will each possess a single qubit of state GHZ. Thus, the state may be distilled from several copies of biseparable state ϱ^{bs}. This finally leads to the conclusion that the notions of genuine tripartite entanglement and entanglement distillability are mutually incomparable.

5 Multipartite entanglement

The notion of multipartite entanglement is concerned with the entanglement of more than two parties. Hence, a special instance of multipartite entanglement was already discussed in previous chapter. As it was already shown by tripartite entanglement, the structure of entanglement becomes more complex with the increasing number of parties that are involved. Furthermore, the structure there did not become more complex simply by consideration of all the bipartitions. The complexity was also influenced by existence of mutually incomparable classes of genuinely entangled states. However, it remains vital to take into consideration even the finer structure of all the bipartitions, tripartitions, and so forth, through to n-partitions.

Initially, for a Hilbert product space $\mathcal{H}$ given by set of indices of n partitions $I = \{A, B, C, \ldots\}$, the term k-partition denotes a set $P = \{P_1, \ldots, P_k\}$ of k subsets of set of indices I such that the subsets P_i are mutually disjoint and they sum up in unification to the set of indices I. Consequently, one might define the notion of k-separability. A pure state $|\psi\rangle$ over Hilbert product space of n partitions given by set of indices $I = \{A, B, C, \ldots\}$ is *k-separable* with respect to a *k-partition* $P = \{P_1, \ldots, P_k\}$ if there is a set of k states $\left\{\left|\psi^{P_1}\right\rangle, \ldots, \left|\psi^{P_k}\right\rangle\right\}$ with $\left|\psi^{P_i}\right\rangle \in \bigotimes_{j \in P_i} \mathcal{H}_j$ such that

$$|\psi\rangle = \bigotimes_{i=1}^{k} \left|\psi^{P_i}\right\rangle \tag{5.1}$$

The question arises how many distinct k-partitions of an n-partite state there are. Mathematically, by the definition of k-partitions, the question reduces to the question of divisibility of a set of cardinality n to k mutually disjoint non-empty parts that sum up in unification to the original set. Consequently, it turns out that the number is precisely the definition of the Stirling number of second kind [53] denoted by $S(n, k)$. Hence, the formulae to compute the number of k-partitions of an n-partite Hilbert space is given by equation

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n, \qquad \binom{k}{i} = \frac{k!}{(k-i)!i!} \tag{5.2}$$

For tripartite Hilbert spaces, the equation yields the expected results as there is a single tripartition, three bipartitions and a single 1-partition where all the genuinely entangled states live. Consequently, the number of all partitions[1] of a given set may be computed as the sum of Stirling numbers of second kind. However, there is a more elegant way to compute the number of partitions provided by the following recurrence relation

$$B_n = \sum_{i=0}^{n-1} \binom{n-1}{i} B_i \tag{5.3}$$

There are two kinds of partitioning that always stand out as for given n and k they represent the unique partitioning, respectively. The first being the partitioning of fully separable states as the set where the number of partitions is equal to the maximal number of partitions. It is unique partitioning as it holds for all n that $S(n,n) = 1$. The latter being the partitioning of genuinely entangled states as the set where the number of partitions is minimal. It is again unique as it holds for all n that $S(n,1) = 1$. Finally, a pure state $|\psi\rangle$ in n-partite Hilbert space is fully separable if it is n-separable. A pure state is genuinely entangled if it is not biseparable for any of the possible bipartitions.

The generalization of the definitions to mixed states yields the convex combinations of pure states of a given property. Hence, a mixed state ϱ is n-separable if it is a convex combination of pure n-separable states with respect to possibly diverse n-partitions. For mixed states, similarly to definition of biseparable mixed states for tripartite entanglement, convex combinations of all n-separable pure states are permitted. In order to justify this definition, it was already demonstrated in Section 4.3 that important mixed states may arise as mixtures of biseparable states with respect to diverse bipartitions. It was a biseparable mixed state made from biseparable pure states with respect to diverse bipartitions that was used for reconstruction of GHZ state.

Finally, in order to conclude the terminology used for multipartite entanglement, a mixed state ϱ over an n-partite Hilbert space

1. The number of all partitions of a set of cardinality n is known as Bell number B_n.

$\mathcal{H}$ is fully separable if it is n-separable. A mixed state ϱ is genuinely entangled if it is not biseparable. There is no need to exclude n-separability in the definition of genuinely entangled states as all n-separable states for $n \geq 2$ are biseparable. If a mixed state is n-separable, then one may obtain $(n-1)$-separable state out of the n-separable state if he groups any two separable partitions to one. Consequently it follows by induction that for $n \geq 2$ every n-separable state is biseparable.

5.1 Classification

For the task of classification of multipartite entanglement, the lower bound on number of entanglement classes with respect to SLOCC transformations will be presented, specific case of four qubits will be outlined and consequently, several families of genuinely entangled states will be identified.

A general n-qubit n-partite state lives in Hilbert space $\bigotimes_{i=1}^{n} \mathbb{C}^2$. The number of complex parameters necessary for description of such a pure state grows exponentially with respect to the number of qubits provided. Since the last parameter may always be derived from the normalization condition[2], one needs $2^n - 1$ complex parameters to fully describe a general n-qubit state. Consequently, this yields the necessity of $2 \cdot (2^n - 1)$ continuous real parameters for the description of the general pure state.

On the other hand, a general invertible local operator is a tensor product of n one-party invertible operators. For n qubits, each of the n invertible operators is fully determined by 2×2 invertible matrix M with a non-vanishing determinant. Since kM will transform a state $|\psi\rangle$ to $k(M|\psi\rangle)$ and the normalization condition abstracts from the multiples of states, the determinant of the matrix M may be fixed to one. Consequently, a 2×2 matrix $M = (M_{ij})$ with determinant one depends only on three complex parameters as the fourth parameter may be obtained from the equation $M_{11}M_{22} - M_{12}M_{21} = 1$. Hence, the general invertible local operator depends on $2 \cdot 3n$ real parameters.

The study of the numbers of parameters provides a way to estim-

2. The normalization condition is given by the fact that the complex parameters must always sum up in square of absolute value to one.

ate the lower bound on number of classes with respect to SLOCC. It is only possible to cover linear $6n$ real parameters out of all exponential $2(2^n - 1)$ real parameters necessary for description of general n-qubit n-partite state. Hence, the number of equivalence classes with respect to SLOCC depends at least on $2(2^n - 1) - 6n$ continuous parameters. The number is negative for three-qubit tripartite states and allows for a finite number of equivalence classes. However, for four qubits and four parties, the number is positive and hence, it yields the continuous number of equivalence classes.

However, there were attempts to provide classification of four-qubit quadripartite[3] states with respect to SLOCC by consideration of diverse families of four-qubit states. The first classification was presented in [50] and yielded up to a permutation of qubits nine distinct families of four-qubit pure states. The families were further subdivided to a single family containing four-qubit genuinely entangled states and eight families containing usually the W-type entanglement distributed among four qubits.

Another attempt [31] at classification of four-qubit quadripartite states with respect to SLOCC introduced the inductive approach to the classification. The application of inductive approach in this context lies in the requirement of knowledge of classification of $(n - 1)$-qubit states in order to provide the classification of n-qubit states. Hence, contrary to the first approach, this approach respects the way entangled classes were divided in case of lower number of qubits. As a result of this approach, there are 18 families of degenerate[4] four-qubit states. Furthermore, there are 16 genuinely entangled classes making the total of 34 families of classes of four-qubit quadripartite states. However, it is vital to remark that if one is to abstract from the permutations among qubits, the classification yields 8 families of classes of genuinely entangled states.

The inductive approach also made it possible to obtain an upper bound on the number of families for five qubits. For the estimation of such an upper bound, it suffices to consider all the combinations of families for less than five qubits and rule out the obvious symmetries

3. The prefix quadri refers to the case where the number of partitions that are considered is four.

4. A multipartite quantum state is degenerate if it is not genuinely entangled.

that occurs. After the application of this technique, the estimation of the upper bound yields at most 170 families for degenerate entangled states and at most 595 families of genuinely entangled states.

For the classification of states in more general multipartite quantum systems, certain kinds of families of the multipartite states will be identified and presented. Two specific representatives of these families were already introduced in the classification of tripartite entanglement. The first being W state and the latter being GHZ state. If basis states that create the W state are ordered by the first occurrence of qubit $|1\rangle$, the matrix given by 0 and 1 identifications of the qubits corresponds to identity matrix. Hence, one may use Kronecker delta function δ for description of more general W_n states

$$|W_n\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \bigotimes_{j=1}^{n} |\delta_{ij}\rangle \tag{5.4}$$

The further generalization of W_n states yields the states that are a superposition[5] of all permutations of states with exactly k out of n qubits being $|1\rangle$ states known as Dicke states $|D_k^n\rangle$. Interestingly, Dicke states were originally investigated by R. H. Dicke in 1954 in his studies of light emissions from a cloud of atoms [12].

Another family whose representative has already been presented in tripartite classification of entanglement is the family of GHZ_n states. In particular, GHZ_3 state corresponds to GHZ state and was shown to be a representative of one of two distinct tripartite entanglement classes under SLOCC. The state $|GHZ\rangle$ may be seen as a pure state that connects the two most diverse basis states. Indeed, the vector representation of GHZ state in computational basis yields vector with only two non-zero elements, one at the beginning of the vector and one at the end of the vector. Hence, the direct generalization to n qubits yields the family of $|GHZ_n\rangle$ states

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}} \left(\bigotimes_{i=1}^{n} |0\rangle + \bigotimes_{i=1}^{n} |1\rangle \right) \tag{5.5}$$

The importance of GHZ_n states arises from their numerous applications in various areas of quantum mechanics and quantum inform-

5. A superposition of n pure quantum states is complex combination of the states that forms a pure quantum state.

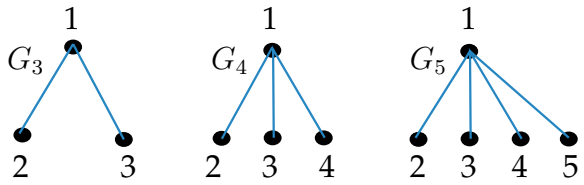

Figure 5.1: Examples of graphical representations of graphs giving rise to various graph states.

ation theory including quantum secret sharing [23] and quantum computation [21].

The next family of quantum states that can be classified and regarded as a possible generalization of the GHZ_n states is the family of graph states. In order to classify this set, let V be a set of elements and let $E \subseteq V \times V$ be a set of symmetric relations[6] over V, then the pair (V, E) is a *graph*. For each graph (V, E) there is a graphical representation given by the elements of V that denote the points in the representation and the elements of relation E that denote the lines connecting the elements of E as depicted in Fig. 5.1. Consequently, a *graph state* is an n-qubit pure quantum state $|\psi\rangle$ corresponding to a graph (V, E) such that V is a set of n elements that correspond to the consecutive qubits of the state $|\psi\rangle$, each qubit is initialized to the dual basis state $|+\rangle$ and each symmetric pair (u, v), (v, u) of elements in relation E denotes the application of control phase gate operator

$$U_{C-phase} = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_z \tag{5.6}$$

to qubits corresponding to u and v. The choice of the order of the two qubits for application of $U_{C-phase}$ operator is arbitrary since a permutation of the order does not change the state that is prepared by this scheme. Consequently, to demonstrate the relation between GHZ_n states and graph states, consider the graph G_3 in Fig. 5.1. The application of control phase gate operators as described in the definition of graph states transforms the initial state $|+++\rangle$ to state $\frac{1}{\sqrt{2}}(|0++\rangle + |1--\rangle)$ and this state is up to a choice of basis[7] for

6. A relation E over a set V is a subset of set of all pairs of elements in V. The relation is symmetric if it holds for all pairs $(u, v) \in E$ that $(v, u) \in E$.
7. The choice of basis is a local operation and preserves LOCC equivalence.

the respective qubits equivalent to $|GHZ_3\rangle$ state. Similarly, graphs G_4 and G_5 in Fig. 5.1 give rise to states that are LOCC-equivalent to $|GHZ_4\rangle$ and $|GHZ_5\rangle$ states respectively [22].

Consequently, one might wonder if the procedure for generation of graph states may yield any GHZ_n-inequivalent graph states. It is known that for two qubits there are no entangled states that would be inequivalent to $|GHZ_2\rangle = |\Phi^+\rangle$ state. However, for three qubits the procedure will not generate the $|W\rangle$ state. On the other hand, for four qubits, the procedure yields the state LOCC-equivalent to four-qubit cluster state $|CL_4\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)$ [22]. From this point on, the number of SLOCC-inequivalent graph states grows very swiftly with the increasing number of qubits [22].

Furthermore, there is an alternative definition of graph states. For a graph (V, E), a graph state $|G\rangle$ may be defined as the simultaneous eigenstate of unit eigenvalue of stabilizing operators $K_G^{(u)}$ for all elements u of set V. Each stabilizing operator $K_G^{(u)}$ is uniquely identified by the set of its neighbours $\mathcal{N}(u)$ as the set of all v such that (u, v) are in relation E and the set of non-neighbours $\overline{\mathcal{N}}(u)$ as the set of all v such that u, v are not in relation E. The stabilizing operator $K_G^{(u)}$ is given as a tensor product of Pauli operator $\sigma_x^{(u)}$ acting on the qubit u, $\sigma_z^{(v)}$ acting on all the qubits v that are connected to qubit u by graph (V, E) and identity operator $\mathbb{I}^{(v)}$ acting on the ones that are not connected to the qubit

$$K_G^{(u)} = \sigma_x^{(u)} \bigotimes_{v \in \mathcal{N}(u)} \sigma_z^{(v)} \bigotimes_{v \in \overline{\mathcal{N}}(u)} \mathbb{I}^{(v)}, \qquad K_G^{(u)} |G\rangle = |G\rangle \tag{5.7}$$

5.2 Detection

The task of entanglement detection is in general tackled by separability criteria and the formalism of entanglement witnesses. Unlike bipartite or tripartite entanglement, the task of detection of multipartite entanglement is not understood very well. However, several separability criteria and techniques concerning entanglement witnesses were already designed to confront this task.

In section 4.2, it was discussed that separability criteria for each bipartition may be applied for detection of entanglement in tripartite

entanglement. Since, in case of tripartite entanglement there are only three bipartitions, the application of such a method is indeed relatively simple. However, the number of bipartitions of a multipartite system grows exponentially with the number of partitions as it holds for all n that $S(n,2) = 2^{n-1} - 1$. It follows from the equation that an eleven-partite quantum system already yields over thousand bipartitions. Hence, even criteria for detection of mere presence of entanglement in multipartite systems are of importance for detection of multipartite entanglement.

The family of *permutation criteria* serves as an example of such criteria for multipartite states. The family can be viewed as a generalization of PPT and CCNR criterion. Analogously to bipartite case (Eq. 3.4), every n-partite mixed state ϱ may be obtained as a combination of product basis states

$$\varrho = \sum_{i_1 j_1 \ldots i_n j_n} \varrho_{i_1 j_1 \ldots i_n j_n} \bigotimes_{k=1}^{n} |i_k\rangle\langle j_k| \tag{5.8}$$

Every such a state is then fully determined by coefficients corresponding to the product basis states. For bipartite PPT criterion these are coefficients $\varrho_{i_1 j_1 i_2 j_2}$ and the criterion is given by positivity of partial transpositions that are in fact the specific permutations of the order of coefficients. Consequently, it is noted that a general permutation of the coefficients is denoted by $\pi(i_1 j_1 i_2 j_2)$. Finally, the generalization of the overall concept is provided by trace norm operator $\|X\|_1 = Tr(\sqrt{XX^\dagger})$ as it holds for all separable states that matrix given by $\varrho_{\pi(i_1 j_1 \ldots i_n j_n)}$ coefficients is of trace norm at most one

$$\left\| \left(\varrho_{\pi(i_1 j_1 \ldots i_n j_n)} \right) \right\|_1 \leq 1 \tag{5.9}$$

If two partitions are considered, the permutations yield precisely PPT and CCNR criteria as all the other permutations yield criteria equivalent to one of them. However, for three partitions, there are six unique criteria and for four partitions, there are already twenty-two unique criteria [11, 55].

Interestingly, even Bell inequalities as already briefly presented in Section 2.4 serve as a practical tool for detection of entanglement. Furthermore, they may be applied for detection of multipartite entanglement. In particular, the notion of *Quadratic Bell-type inequalities* is of importance for the task [48]. Unlike permutation criteria, the

statistical nature of quadratic Bell-type inequalities allows to differentiate the finer structure of multipartite entanglement as it makes it possible to impose different conditions for different classes of separability. Moreover, in Ref. [42, 43], a more general procedure for derivation of quadratic inequalities for different classes of separability was recently described.

A promising result was obtained by algorithmic approach based upon the method of symmetric extensions already presented in Subsection 3.2.5 for the bipartite entanglement. Initially, a generalization of the method to multipartite systems was introduced [14]. Consequently, it was shown that the separability problem may be viewed as an optimization problem with polynomial constraints and that the hierarchy of criteria that is obtained by the generalization of the approach to n parties is complete [18, 32]. However, the complexity of the method makes it unfit for practical applications.

The importance of entanglement witnesses for the task of entanglement detection has already been emphasized in previous two sections on detection of bipartite and tripartite entanglement. In particular, a specific example of GHZ-class witness was presented in section on detection of tripartite entanglement (Eq. 4.15). The witness was constructed by application of a more general technique that will be further discussed, now. For a desired state $|\psi\rangle$, one considers a preliminary observable

$$\mathcal{W} = \alpha\mathbb{I} - |\psi\rangle\langle\psi| \tag{5.10}$$

Consequently, it is necessary to estimate the value of α. A good criterion for the value is the maximal overlap between the state $|\psi\rangle$ and the convex class that shall be ruled out by the witness. In particular, for GHZ witness $\mathcal{W}_{GHZ}$ (Eq. 4.15) this value was $\frac{3}{4}$ and it represented the maximal overlap between the state $|GHZ\rangle$ and the class of W-type states [2]. The process of estimation of the maximal overlap with the class of biseparable states is relatively undemanding as for bipartite states, the Schmidt decomposition allows for a relatively simple computation of the value [10]. In this case it holds that the maximal overlap is given by the square root of maximal Schmidt coefficient over all bipartitions. The estimation of the overlap with different classes is generally much more difficult and much less is known for those cases. However, there are exceptions and one of

them is given by a witness for W states excluding full separability $\mathcal{W}_W^{fs} = \frac{4}{9}\mathbb{I} - |W\rangle\langle W|$. There are also other techniques for construction of witnesses. An overview of the techniques was presented by Otfried Gühne in [22]. In order to conclude this section, a brief overview of witnesses and maximal overlaps with biseparable states will be presented. In particular, the witnesses for the general GHZ_n states, graph G_n states [19] and W_n states [47] yield

$$\mathcal{W}_{GHZ_n}^{bs} = \frac{1}{2}\mathbb{I} - |GHZ_n\rangle\langle GHZ_n|$$
$$\mathcal{W}_{G_n}^{bs} = \frac{1}{2}\mathbb{I} - |G_n\rangle\langle G_n|$$
$$\mathcal{W}_{W_n}^{bs} = \frac{n-1}{n}\mathbb{I} - |W_n\rangle\langle W_n|$$

5.3 Distillation

Very little is known concerning the task of distillation of multipartite systems. The sole choice of the state to which to distil is not clear. The answer to this question is hidden partially due to the absence of classification for general multipartite systems. However, it is possible to define the distillability simply as the task to distil several copies of an entangled state out of a multipartite state. Another popular distillation targets include tensors of Bell pairs $\bigotimes_{i=1}^{k} |\Phi^+\rangle$ for a positive k and $|GHZ_n\rangle$ states. A connection between Bell pair distillation and $|GHZ_n\rangle$ state distillation was found in Ref. [46]. In particular, a more powerful statement was demonstrated in the paper showing that a Bell pair can be distilled from an arbitrary multipartite entangled pure state.

Another important result concerning multipartite entanglement distillation was already presented in Section 4.3. In particular, it was shown that there are biseparable tripartite mixed states such that an arbitrary genuinely entangled tripartite state may be distilled out of them. Furthermore, the technique provides a way to obtain arbitrary multipartite state from similar biseparable states by distillation of Bell pairs and consequent application of an extension of entanglement swapping protocol described in Subsection 2.5.2. However, the efficiency of such a multipartite distillation protocol is in general

worse than that of a dedicated multipartite protocol [36].

It was already discussed that if a mixed state is PPT, then it is not distillable. The generalization of this concept to multiple parties yields the necessary condition for distillability of a multipartite state. If a mixed state ϱ is distillable then it must violate PPT criterion for all bipartitions. From this it directly follows that there are multipartite bound entangled states as the PPT criterion fails to detect entangled states already for quantum systems of dimensions 2×4. The systems of these dimensions are in fact bipartitions of three-qubits systems of dimensions $2 \times 2 \times 2$. Hence, there are multipartite bound entangled states. Consequently, for more parties, an interesting bound entangled state is four-qubit Smolin states [44]

$$\varrho_S = \frac{1}{4}\left(\left|\Psi^{\pm}\right\rangle\left\langle\Psi^{\pm}\right| \otimes \left|\Psi^{\pm}\right\rangle\left\langle\Psi^{\pm}\right| + \left|\Phi^{\pm}\right\rangle\left\langle\Phi^{\pm}\right| \otimes \left|\Phi^{\pm}\right\rangle\left\langle\Phi^{\pm}\right|\right) \tag{5.11}$$

The state ϱ_S is an equal mixture of tensors of all four Bell states. As it was already stated, the state is bound entangled. However, if two parties that possess one of the two Bell pairs meet, the other two parties will be able to distil an entangled Bell pair.

The notion of distillability and in particular bound entanglement remains to be an important task in multipartite systems. It is hoped for that the notion of bound entanglement may provide a better understanding of entanglement in general. However, only a very limited knowledge of the phenomena in this area has been obtained. Since there still remains a lot to be known, the area undergoes an extensive research and many researchers hope to bring more light into this mostly unlit area.

6 Conclusion

The core element of all the phenomena presented in this thesis is quantum entanglement. In order to present and outline the phenomena related to the quantum entanglement, the mathematical framework of quantum mechanics was presented in first chapter. Consequently, the idea of entanglement along with the uniqueness of this resource and brief application of this resource were outlined in next chapter. The entanglement of two parties followed and it was demonstrated that the structure of bipartite entanglement is well understood as a lot of important results that capture the structure of bipartite entanglement were presented in the chapter. The case of three parties followed and it was shown that the structure of tripartite entanglement is much more complex than that of bipartite entanglement. However, the area was extensively researched and answers to many questions were presented in the chapter. Hence, the structure of tripartite entanglement is understood reasonably well. Finally, more general multipartite entanglement was discussed and it was remarked that the understanding of the structure is very limited. There were attempts to capture an essence of the multipartite entanglement and few of them were even successful to a certain extent but overall, a lot remains to be discovered in this area.

Most of the topics presented in the thesis were original authorial work of many researchers. However, many protocols, arguments and ideas along with their proofs were modified to better fit the state of presented knowledge and better suit the taste of the author of this thesis. For instance, the recurrence protocol presented in Section 3.3 and the task of classification of three-qubit entanglement (Section 4.1) were heavily modified in comparison to their original presentation. There were also ideas, protocols and examples that I designed all the way to their bottom. In particular, the entanglement swapping protocol (Subsection 2.5.2) was designed from the knowledge of existence of such a protocol and the notion and the form of most general bipartite state (Section 3.1) was designed from the knowledge of relation between LOCC transformations and majorization.

There is much more knowledge that remains to be discovered about entanglement theory that was already explored by researchers

in the field of quantum mechanics and quantum information science. In particular, the further studies could include the task of quantification of entanglement. The task of activation of entanglement in bound entangled states could also provide for an interesting area for the subsequent studies and the techniques of construction of witnesses could be further studied as well.

Bibliography

[1] A. Acin, A. Andrianov, L. Costa, E. Jane, J. I. Latorre, and R. Tarrach. Generalized Schmidt decomposition and classification of three-quantum-bit states. *Phys. Rev. Lett. 85, 1560*, 2000.

[2] A. Acin, D. Bruß, M. Lewenstein, and A. Sanpera. Classification of mixed three-qubit states. *Phys. Rev. Lett. 87, 040401*, 2001.

[3] A. Acin, J. I. Cirac, and L. Masanes. Multipartite Bound Information exists and can be activated. *Phys. Rev. Lett. 92, 107903*, 2004.

[4] J. T. Barreiro, P. Schindler, O. Gühne, T. Monz, M. Chwalla, C. F. Roos, M. Hennrich, and R. Blatt. Experimental multiparticle entanglement dynamics induced by decoherence. *Nature Physics 6, 943*, 2010.

[5] John S. Bell. On the Einstein Podolsky Rosen Paradox. *Physics 1 3, 195*, 1964.

[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett. 76, 722-725*, 1996.

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed State Entanglement and Quantum Error Correction. *Phys. Rev. A 54, 3824-3851*, 1996.

[8] F. Bodoky, O. Gühne, and M. Blaauboer. Decay of Entanglement for Solid-State Qubits. *J. Phys.: Cond. Mat. 21 395602*, 2009.

[9] D. Bohm. A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. *Phys. Rev. 85, 166*, 1952.

[10] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera. Experimental Detection of Multipartite Entanglement using Witness Operators. *Phys. Rev. Lett. 92, 087902*, 2004.

[11] L. Clarisse and P. Wocjan. On independent permutation separability criteria. *Quant. Inf. Comp. 6, 277*, 2006.

[12] R. H. Dicke. Coherence in Spontaneous Radiation Processes. *Phys. Rev. 93, 99*, 1954.

[13] A.C. Doherty, P.A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett. 88 (18), 187904*, 2002.

[14] A.C. Doherty, P.A. Parrilo, and F. M. Spedalieri. Detecting multipartite entanglement. *Phys. Rev. A 71, 032333*, 2005.

[15] A.C. Doherty, P.A. Parrilo, and F.M. Spedalieri. Complete family of separability criteria. *Phys. Rev. A 69 (2), 022308*, 2004.

[16] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A 62, 062314*, 2000.

[17] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev. 47 (10), 777*, 1935.

[18] J. Eisert, P. Hyllus, O. Gühne, and M. Curty. Complete hierarchies of efficient approximations to problems in entanglement theory. *Phys. Rev. A 70, 062317*, 2004.

[19] O. Gühne G. Tóth. Detecting Genuine Multipartite Entanglement with Two Local Measurements. *Phys. Rev. Lett. 94, 060501*, 2005.

[20] N. Gisin and S. Wolf. Linking classical and quantum key agreement: is there bound information? *Lecture Notes in Computer Science 1880, 482-500*, 2000.

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

[22] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports 474, 1*, 2009.

[23] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A59, 1829*, 1999.

[24] T. Hiroshima. Majorization criterion for distillability of a bipartite quantum state. *Phys. Rev. Lett. 91, 057902*, 2003.

[25] K. Horodecki, M.Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Phys. Rev. Lett. 94, 160502*, 2005.

[26] K. Horodecki, L. Pankowski, M.Horodecki, and P. Horodecki. Low-Dimensional Bound Entanglement With One-Way Distillable Cryptographic. *IEEE Trans. Inf. Theory 54, 2621*, 2008.

[27] M. Horodecki and P. Horodecki. Reduction Criterion of Separability and Limits for a Class of Distillation Protocols. *Phys. Rev. A 59, 4206*, 1999.

[28] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of Mixed States: Necessary and Sufficient Conditions. *Phys. Lett. A 223, 1*, 1996.

[29] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-State Entanglement and Distillation: Is there a Bound Entanglement in Nature? *Phys. Rev. Lett. 80, 5239*, 1998.

[30] Hermann Kampermann, Otfried Gühne, Colin Wilmott, and Dagmar Bruß. Algorithm for characterizing stochastic local operations and classical communication classes of multiparticle entanglement. *Phys. Rev. A 86, 032307*, 2012.

[31] L. Lamata, J. Leon, D. Salgado, and E. Solano. Inductive Entanglement Classification of Four Qubits under SLOCC. *Phys. Rev. A 75, 022318*, 2007.

[32] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization 11, 796*, 2001.

[33] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki. Optimization of Entanglement Witnesses. *Phys. Rev. A 62, 052310*, 2000.

[34] M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac. Characterization of separable states and entanglement witnesses. *Phys. Rev. A 63, 044304*, 2001.

[35] C. E. Mora M. Piani. Class of positive-partial-transpose bound entangled states associated with almost any set of pure entangled states. *Phys. Rev. A 75, 012305*, 2007.

[36] M. Murao, M.B. Plenio, S. Popescu, V. Vedral, and P. L. Knight. Multi-Particle Entanglement Purification Protocols. *Phys.Rev. A 57, 4075*, 1998.

[37] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett., 83 (2), 436*, 1999.

[38] M. A. Nielsen and J. Kempe. Separable states are more disordered globally than locally. *Phys. Rev. Lett. 86, 5184-7*, 2001.

[39] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[40] T. Rowland. Riesz Representation Theorem, 2013. Available online at `http://mathworld.wolfram.com/RieszRepresentationTheorem.html`.

[41] O. Rudolph. Further results on the cross norm criterion for separability. *Quant. Inf. Proc. 4, 219*, 2005.

[42] M. P. Seevinck. Parts and Wholes. An Inquiry into Quantum and Classical Correlations. *Utrecht University PhD. Thesis*, 2008.

[43] M. P. Seevinck and J. Uffink. Partial separability and entanglement criteria for multiqubit quantum states. *Phys. Rev. A 78, 032101*, 2008.

[44] J. A. Smolin. A four-party unlockable bound-entangled state. *Phys. Rev. A 63 , 3*, 2001.

[45] J. Sperling and W. Vogel. Necessary and sufficient conditions for bipartite entanglement. *Phys. Rev. A 79, 022318*, 2009.

[46] A. V. Thapliyal and J. A. Smolin. The Power of LOCCq State Transformations. *arXiv:quant-ph/0212098*, 2002.

[47] G. Tóth. Detection of multipartite entanglement in the vicinity of symmetric Dicke states. *J. Opt. Soc. Am. B 24, 275*, 2007.

[48] J. Uffink. Quadratic bell inequalities as tests for multipartite entanglement. *Phys. Rev. Lett. 88, 230406*, 2002.

[49] L. Vandenberghe and S. Boyd. Semidefinite Programming. *SIAM Review 38(1), 49-95*, 1996.

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

[51] P. Walther, K.J. Resch, and A. Zeilinger. Local conversion of GHZ states to approximate W states. *Phys. Rev. Lett. 94, 240501*, 2005.

[52] E. W. Weisstein. Axiom of Choice, 2013. Available online at `http://mathworld.wolfram.com/AxiomofChoice.html`.

[53] E. W. Weisstein. Stirling Number of the Second Kind, 2013. Available online at `http://mathworld.wolfram.com/StirlingNumberoftheSecondKind.html`.

[54] E. W. Weisstein. Vector Space, 2013. Available online at `http://mathworld.wolfram.com/VectorSpace.html`.

[55] P. Wocjan and M. Horodecki. Characterization of combinatorially independent permutation separability criteria. *Open Syst. Inf. Dyn. 12, 331*, 2005.