DIPLOMARBEIT

Titel der Diplomarbeit

Quantum Entanglement and Geometry

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag. rer.nat.)

Verfasserin / Verfasser:	Andreas Gabriel
Matrikel-Nummer:	0406353
Studienrichtung (lt. Studienblatt):	411 Physik
Betreuerin / Betreuer:	Ao. Univ. Prov. Dr. Reinhold A. Bertlmann

Wien, am 23.06.2009

Abstract

The phenomenon of quantum entanglement is thoroughly investigated, focussing especially on geometrical aspects and on bipartite systems. After introducing the formalism and discussing general aspects, some of the most important separability criteria and entanglement measures are presented. Finally, the geometry of 2x2- and 3x3-dimensional state spaces is analysed and visualised.

Quantum Entanglement and Geometry

Diplomarbeit
zur Erlangung des akademischen Grades
,,Magister der Naturwissenschaften"
an der
Universität Wien

eingereicht von
Andreas Gabriel

betreut von
Ao. Univ. Prof. Dr. Reinhold A. Bertlmann

Wien, Juni 2009

Contents

1 Introduction

Entanglement is one of the most nonclassical phenomenae in quantum physics, in the sense of being responsible for many effects that strongly contradict the very foundations of classical physics (such as local realism).
There are many different definitions of entanglement, some of which are very mathematical, others being rather close to the experiment and practical aplication. Simply speaking, two (or more) particles are entangled, if each of them cannot be fully described without the other, so that the combined system contains more information than the individual systems do.

The concept of quantum entanglement was first perceived by Erwin Schrödinger (who called it 'Verschränkung' in German, which only later was translated to 'Entanglement') in the early years of quantum mechanics in 1935[1]. Soon Einstein, Podolsky and Rosen (EPR) discovered some of the extraordinary properties that followed from this strange new feature (so extraordinary in fact, that they believed quantum mechanics to be 'incomplete', rather than to consider these consequences to be real[2]). However, for a very long time both the works by Schrödinger and EPR were not taken seriously.
Almost 30 years later, in 1964, John Bell conceived a gedankenexperiment[3] which should turn out to be the means to settle this discussion once and for all, proving EPR's doubts to be wrong and making way for a huge new field of research in doing so.
Soon more and more highly interesting, sometimes intriguingly contraintuitive and often technologically very promising applications of entanglement, in particular the field of quantum information, were discovered.
Today entanglement and quantum information theory are very popular and steadily advancing subjects. While the first practical applications (such as quantum cryptography[4]) are already about to make their way into everyday use, some areas (such as multipartite entanglement) of this field are merely beginning to be understood.

When studying entanglement and related topics, one soon finds that geometry plays a very important role in many of these and often allows a highly intuitive and vivid understanding.
The aim of this work is to give a structured basic overview over the field

of quantum entanglement and quantum information theory, concentrating mainly on this geometric viewpoint and on bipartite systems.

After giving an introduction into the mathematical formalism of quantum information theory in section 2, the very nature of entanglement will be discussed (3), followed by a detailed explanation of the most common and useful means to detect (4) and quantify (5) entanglement (with focus on the geometrical aspects). Finally, these tools will be used to thoroughly analyse the Hilbert spaces of quantum states, paying special attention to two of the most important classes of systems in quantum information theory (6), namely systems of two QuBits ($2 \otimes 2$ dimensions, e.g. two spin-$\frac{1}{2}$-particles) and systems of two QuTrits ($3 \otimes 3$ dimensions, e.g. two spin-1-particles).

2 Formalism and Basics

2.1 Hilbert Spaces and State Vectors

2.1.1 Bits, Dits, Qubits and Qudits

In classical information theory, one usually deals with bits (i.e. variables that can assume the values 0 or 1) and – less often – also with higher dimensional generalisations thereof, dits (which can assume the values 0, 1, ..., $d-2$ and $d-1$). In quantum mechanics, superpositions of different states are also physically realised, which turns out to offer whole new possibilities, thus making quantum information theory a completely new field that can only remotely be compared to classical information theory.

The quantum analogy to a bit – a quantum bit or qubit – is a (normalised) complex superposition of the values 0 and 1. Hence, unlike a state of a classical bit (which can only have two different values), a state $|\Psi\rangle$ of a qubit can assume infinitely many different values of the form

$$|\Psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.1}$$

with the normalisation $|a|^2 + |b|^2 = 1$. Since the states $|0\rangle$ and $|1\rangle$ need to be orthogonal, the underlying Hilbert space is $\mathcal{H} = \mathbb{C}^2$.

The classical generalisation of a bit to a dit also has a quantum analogue, the quantum dit or qudit, which can consequently assume all values that are superpositions of d different states and lives on the Hilbert space $\mathcal{H} = \mathbb{C}^d$. Apart from the qubit, especially the qutrit ($d = 3$) also plays a very important role in quantum information theory..

2.1.2 State Vectors

Since the state of a qubit is described by a vector $|\Psi\rangle \in \mathbb{C}^2$, it can be realised for example as the spin components of a spin-$\frac{1}{2}$ particle or the polarisation components of a photon. Therefore, the basis $\{|0\rangle, |1\rangle\}$ is also often denoted by $\{|\uparrow\rangle, |\downarrow\rangle\}$ or $\{|H\rangle, |V\rangle\}$ (where the latter stands for 'horizontal' and 'vertical' polarisation).

For convenience reasons, the basis vectors are usually chosen such that $|0\rangle$ is the first standard unit-vector and $|1\rangle$ is the second (in the case of qudits, this can easily be generalised to $|n\rangle$ being the $(n+1)$st standard unit vector). This choice of basis is called the computational basis.

The scalar product of two state vectors $|\Psi\rangle$ and $|\Phi\rangle$ is defined as

$$\langle\Phi|\Psi\rangle = (|\Phi\rangle)^* \cdot |\Psi\rangle \tag{2.2}$$

where '·' is the standard scalar product and the asterisk denotes complex conjugation.

2.1.3 Product Spaces

In quantum information theory, it is of central interest to describe several particles with a single state. These states are elements of a product space $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes ... \otimes \mathcal{H}^X$, where $\mathcal{H}^\alpha$ are the state spaces of the individual systems, respectively. This work concentrates on bipartite systems, therefore the considered Hilbert spaces will be of the form $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$.

The dimension of such product spaces is

$$\dim\mathcal{H} = \dim\mathcal{H}^A \dim\mathcal{H}^B = d_1 d_2 \tag{2.3}$$

where $d_{1,2}$ are the dimensions of the subspaces $\mathcal{H}^{A,B}$. In short notation, the space $\mathcal{H} = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ is also often referred to as $d_1 \otimes d_2$.

Clearly, each pair of unipartite states $\{\left|\Psi^A\right\rangle, \left|\Psi^B\right\rangle\}$ corresponds to a bipartite state $\left|\Psi^{AB}\right\rangle = \left|\Psi^A\right\rangle \otimes \left|\Psi^B\right\rangle$. However, there are elements of the product space, which are not products of elements of the respective subspaces (but linear combinations of such). The individual parts of such states can obviously not be described by individual, mutually independant state vectors. Such states are called entangled and will be the main topic of this work.

Bases of product spaces are induced by bases of the subspaces. These are usually denoted by

$$\left|i,j\right\rangle = \left|i\right\rangle \otimes \left|j\right\rangle \tag{2.4}$$

where $\left|i\right\rangle$ is a basis vector in the first subspace and $\left|j\right\rangle$ is a basis vector in the second subspace.

2.2 Operators

Operators acting on a Hilbert space $\mathcal{H}$ are represented by $d \times d$-dimensional matrices (where $d = \dim\mathcal{H}$). All operators on $\mathcal{H}$ form the Hilbert-Schmidt space $\mathcal{B}$, which is a Hilbert space itself (and therefore also often denoted by $\mathcal{H}$). It is equipped with the scalar product

$$\langle A|B\rangle = \mathrm{Tr}\left(A^\dagger \cdot B\right) \tag{2.5}$$

which induces the norm

$$\|A\| = \sqrt{\langle A|A\rangle} \tag{2.6}$$

However, there also are other relevant norms on the Hilbert-Schmidt space. The n-norm is defined by

$$\|A\|_n = \sqrt[n]{\mathrm{Tr}\left((A^\dagger A)^{\frac{n}{2}}\right)} \tag{2.7}$$

where the dagger † denotes hermitean conjugation.

Most importantly, the 1-norm $\|.\|_1$ is also called the trace (class) norm, which obviously equals the sum of the absolute eigenvalues, and the 2-norm $\|.\|_2$ is equal to the standard Hilbert-Schmidt norm (2.6).

An operator A is said to be positive semidefinite ($A \geq 0$), if all of its eigenvalues are greater than or equal to zero. For simplicity, these operators are often simply called positive operators.

2.3 Density Matrices

2.3.1 Definition

In order to use the vector state formalism, complete knowledge of a quantum state is required. If for example the phase of an investigated state was unknown, the remaining information would be useless, as a state with 'averaged' phase would vanish. This problem can be solved by using the density matrix formalism, which includes the whole vector state formalism and also offers additional features.

The density matrix ρ of a state $|\Psi\rangle$ is the operator defined as the outer product

$$\rho = |\Psi\rangle \langle\Psi| \tag{2.8}$$

This case, in which full information about the state is at hand and the density matrix assumes the above form, is called a pure state.

If however a state is not completely known, but only the probabilities $\{p_i\}$, with which it is one out of several states $\{|\Psi_i\rangle\}$ is known, it is called a mixed state and the density matrix assumes the form

$$\rho = \sum_i p_i |\Psi_i\rangle \langle\Psi_i| \tag{2.9}$$

where evidently $p_i \geq 0$ and $\sum_i p_i = 1$.

All density matrices have the following properties:

- Hermiticity: $\rho = \rho^\dagger$

- Normalisation: $\mathrm{Tr}(\rho) = 1$

- Positivity: $\rho \geq 0$

Furthermore, for pure states it follows from the definition (2.8) that $\rho^2 = \rho$ and thus $\mathrm{Tr}(\rho^2) = 1$, while for mixed states $\mathrm{Tr}(\rho^2) < 1$. In fact, the quantity

$$M = \frac{d}{d-1}\left(1 - \mathrm{Tr}(\rho^2)\right) \tag{2.10}$$

can be considered a measure for the mixedness of a state (where $d = \dim\mathcal{H}$). It is known as the linear entropy and assumes its minimal value of zero for all pure states and its maximal value of one for the state $\omega = 1/d\,\mathbb{1}$, which evidently is the maximally mixed state and is also referred to as the trace state.

It also follows from the definition (2.8), that density matrices of pure states are projectors onto the corresponding state vector, which is their eigenvector to the eigenvalue one, while all other eigenvalues vanish.

Since density matrices are a more general class of objects that vector states (in the sense, that all vector states can be written as density matrices, but not vice versa), most of the time density matrices are used in quantum information theory. For convenience reasons, the word 'state' will refer to density matrices throughout this work, in contrast to vector states.

2.3.2 Correlations

Multipartite systems can be described by density matrices very much in the same way it can be described by vector states, that is, if two systems are described by the density matrices ρ^A and ρ^B, the state of the composite system is

$$\rho^{AB} = \rho^A \otimes \rho^B \tag{2.11}$$

Since this work concentrates on bipartite systems, the superscripts for these states will mostly be omitted – it will always be clear from the context, what kind of state is meant.

Like in the case of vector states, also the Hilbert-Schmidt product space $\mathcal{B} = \mathcal{B}^A \otimes \mathcal{B}^B$ contains states, that cannot be expressed as products like in (2.11). In the case of density matrices however, this can have two reasons. Firstly, analogously to the vector states, a state can be entangled, i.e. consist of entangled vector states (this will be discussed in further detail throughout this work). Secondly, the subsystems of a state can be classically correlated by mixing of product states. Consider for example the state

$$\rho = \frac{1}{2}\left(|0,0\rangle\langle 0,0| + |1,1\rangle\langle 1,1|\right) \tag{2.12}$$

which is a convex sum of two product states. It is correlated in the sense that any measurement in the basis $|0\rangle, |1\rangle$ in either subsystem will always yield the same result. This is a purely classical effect and must not be confused with entanglement (i.e. quantum correlations).

2.3.3 Reduced Density Matrices

Evidently, the opposite operation to combining two Hilbert spaces to a product space is to reduce a composite state to one of its subsystems, discarding the other one. This is achived by tracing over the discarded subsystem, thus averaging over all correlations (if there are any) and being left with a unipartite state that in general contains less information about the corresponding subsystem than the composite state did, described by the reduced density matrices

$$\rho^A = \text{Tr}_B(\rho)$$
$$\rho^B = \text{Tr}_A(\rho)$$

(2.13)

where Tr_X is the partial trace over the subsystem X.

In the case of product states, this operation is fully reversible, i.e. the composite state can always be recovered by combining the reduced density matrices

$$\rho = \rho^A \otimes \rho^B$$

(2.14)

while for other states, the tensor product

$$\rho^{AB} = \rho^A \otimes \rho^B$$

(2.15)

will yield a different state $\rho^{AB} \neq \rho$, which contains less information than the original one, since all correlations were traced out and lost.

2.3.4 Decompositions

The definition of mixed density matrices

$$\rho = \sum_i p_i |\Psi_i\rangle \langle \Psi_i|$$

(2.16)

is not bijective in the sense that there is no unique decomposition of ρ into an ensemble $(\{p_i\}, \{|\Psi_i\rangle\})$, except for pure states. In most cases, there are in fact infinitely many such decompositions, such that it makes only little

sense to speak of a mixed state consisting of a certain set of pure states, but only that a mixed state can be represented by such an ensemble.

Apart from decompositions into pure states, density matrices can of course also be decomposed mathematically into any basis of the underlying Hilbert-Schmidt space. Since this concept finds many applications in quantum information theory, the most important of these bases shall be presented here[5].

Pauli matrices

The most simple such basis consists of the Pauli matrices, which together with the identity matrix form a basis for all 2×2-dimensional matrices (or all hermitean 2×2-dimensional matrices, if all coefficients are held real). The three Pauli matrices are defined as

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \ , \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.17}$$

Apart from their function as a basis, the Pauli matrices are also the observables corresponding to spin-measurements in the x-, y- and z-direction, respectively, for spin-$\frac{1}{2}$ particles and are also the generators of the SU(2).

Gell-Mann matrices

Originally, the Gell-Mann matrices (GMMs) were introduced as a basis (together with the identity matrix) for 3×3-dimensional hermitean matrices, however, later they were generalised to arbitrary dimensions.

For $d \times d$ dimensional matrices, there are $d(d-1)/2$ symmetric GMMs

$$\lambda_s^{j,k} = |j\rangle \langle k| + |k\rangle \langle j| \tag{2.18}$$

as well as $d(d-1)/2$ antisymmetric GMMs

$$\lambda_a^{j,k} = -i |j\rangle \langle k| + i |k\rangle \langle j| \tag{2.19}$$

and $(d-1)$ diagonal GMMs

$$\lambda_d^l = \sqrt{\frac{2}{l(l+1)}} \left(\sum_{m=1}^{l} |m\rangle \langle m| - l |l+1\rangle \langle l+1| \right) \tag{2.20}$$

with $1 \leq j < k \leq d$ and $1 \leq l \leq d-1$.

For $d = 2$, the GMMs are equal to the Pauli matrices. For $d = 3$, they read

10

$$\lambda_s^{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} , \; \lambda_s^{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} , \; \lambda_s^{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} ,$$

$$\lambda_a^{1,2} = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} , \; \lambda_a^{1,3} = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix} , \; \lambda_a^{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix} , \quad (2.21)$$

$$\lambda_d^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} , \; \lambda_d^2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

The generalisations to higher dimensions are straightforward.
Since all GMMs are hermitean themselves, all coefficients in a decomposition are real.

Weyl operators

Another basis for $d \times d$-dimensional matrices that has proven to be quite useful in quantum information theory is the Weyl operator basis, which consists of d^2 unitary and mutually orthogonal matrices $W_{m,n}$, defined as

$$W_{m,n} = \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d} kn} |k\rangle \langle k + m| \tag{2.22}$$

where $0 \leq m, n \leq d - 1$ and $(k + m)$ is to be understood modulo d. Note that $U_{0,0} = \mathbb{1}$.

For $d = 2$, the four Weyl operators correspond to the identity and the three Pauli matrices: $U_{0,0} = \mathbb{1}$, $U_{0,1} = \sigma_1$, $U_{1,0} = \sigma_3$, $U_{1,1} = i\sigma_2$.

For $d = 3$, the Weyl operators assume the form

$$W_{0,1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \ W_{0,2} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$W_{1,0} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2\pi i}{3}} & 0 \\ 0 & 0 & e^{-\frac{2\pi i}{3}} \end{pmatrix}, \ W_{1,1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & e^{\frac{2\pi i}{3}} \\ e^{-\frac{2\pi i}{3}} & 0 & 0 \end{pmatrix}, \ W_{1,2} = \begin{pmatrix} 0 & 0 & 1 \\ e^{\frac{2\pi i}{3}} & 0 & 0 \\ 0 & e^{-\frac{2\pi i}{3}} & 0 \end{pmatrix},$$

$$W_{2,0} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{-\frac{2\pi i}{3}} & 0 \\ 0 & 0 & e^{\frac{2\pi i}{3}} \end{pmatrix}, \ W_{2,1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & e^{-\frac{2\pi i}{3}} \\ e^{\frac{2\pi i}{3}} & 0 & 0 \end{pmatrix}, \ W_{2,2} = \begin{pmatrix} 0 & 0 & 1 \\ e^{-\frac{2\pi i}{3}} & 0 & 0 \\ 0 & e^{\frac{2\pi i}{3}} & 0 \end{pmatrix}$$

$$(2.23)$$

The Schmidt decomposition

Apart from decompositions for density matrices, there is also an important decomposition for composite vector states, known as the Schmidt decomposition[6]. It decomposes a bipartite state vector $|\Psi\rangle$ into a product basis, minimising the number of terms, i.e.

$$|\Psi\rangle = \sum_{i=1}^{k} \left|\phi_i^A\right\rangle \otimes \left|\phi_i^B\right\rangle \tag{2.24}$$

The minimised number of terms k is known as the Schmidt-rank of $|\Psi\rangle$. It is easy to see that $1 \leq k \leq d_{min}$, where $d_{min} = \min(d_1, d_2)$ is the lower of the two subsystem's dimensions.

The Schmidt rank of a state also equals the rank of its reduced density matrices.

3 Entanglement and Distillation

3.1 Entanglement

There are various ways in which entanglement can be seen and characterised[7] – for example it would usually be described very differently by an experimental and a mathematical physicist. In this section, it shall primarily be seen as a resource for performing various tasks, such as quantum computation[8] or quantum cryprography[4], thus avoiding philosophical and mathematical difficulties and concentrating on the applicational point of view (providing motivation for dealing with quantum information theory in the first place and in particular the motivation for this work).

In all these applications, quantum states are needed to be exchanged between two or more parties (usually refered to as Alice, Bob, Charlie, etc.). In general however, one does not have the means to transmit these states perfectly loss-free – quantum channels are mostly noisy and quantum states are rather fragile. In classical communications, error correction protocols enable faithful communication even through imperfect channels by sending multiple copies of the data. Since it is impossible to copy a quantum state (as stated in the no-cloning-theorem[9]), this is not an option in quantum communication. Instead, it appears to be a good way to use quantum teleportation[10] (thus, not sending the particle through a quantum channel, but using entanglement aided by a classical communications channel to transmit it), to send the state without losses. The obvious problem here is, that faithful teleportation requires maximally entangled pure states to be shared between the acting parties. Which ever of the parties creates these states, as soon as one of the entangled particles is sent to another party, the state will become mixed and less entangled – again, due to noisy quantum channels and interaction with the environment.

So, under certain conditions, it is rather easy for Alice and Bob to get any number of nonmaximally entangled mixed states (since they can create and share these states arbitrarily many times), where they actually need maximally entangled ones. Hence, there is need for a means to 'distill' these mixed states back to maximally entangled pure states.

3.2 Distillation

The problem was solved by Bennet et al.[11], who thought of a way for Alice and Bob to increase both entanglement and purity at cost of the number of their shared states. Since this first work, many others have been published in

this field, providing several different protocols for distilling entangled states. Still, all follow the same basic way:

1. Alice and Bob share a number of nonmaximally entangled states

2. They both perform local measurements on their particles

3. They tell each other the outcomes of these measurements (via a classical channel)

4. Depending on these outcomes being equal or odd, they either discard the measured pair of particles or keep them. In the latter case, the particles are now more strongly entangled than they were before.

5. These steps can be repeated as often as necessary, increasing the entanglement per pair of particles each time.

Although the optimal protocol for distilling a state (i.e. the protocol requiring the least input states per maximally entangled output state) in general may depend on the state itself, an upper bound for the efficiency of all such protocols can be given[12], since – considering entanglement as a resource – the total entanglement in any system can not increase (under the given circumstances, i.e. only allowing Alice and Bob to perform local operations). Hence, if (in an appropriate measure, which will be discussed in section 5) the combined entanglement of all input states for any protocol equals the entanglement of one maximally entangled output state, this protocol is maximally efficient and cannot be exceeded by any other distillation protocol.

The BBPSSW-Protocol

The best known distillation protocol (and the only one that shall be discussed in this work) is the so called BBPSSW-protocol[12], which is designed for distillation of two-qubit-states (nevertheless, it can be generalised to higher dimensions). It works as follows:

1. Alice and Bob share n pairs of mixed entangled states ρ $(\rho^{\otimes n})$

2. They first apply random unitary rotations to all pairs

$$\rho \mapsto U_{rot} \, \rho \, U_{rot}^\dagger \tag{3.1}$$

thus transforming these states into rotationary invariant states of the form

$$W_F = F \left| \Psi^- \right\rangle \left\langle \Psi^- \right| \; + \; \frac{1-F}{3} \left| \Psi^+ \right\rangle \left\langle \Psi^+ \right| \; + $$
$$+ \; \frac{1-F}{3} \left| \Phi^- \right\rangle \left\langle \Phi^- \right| \; + \; \frac{1-F}{3} \left| \Phi^+ \right\rangle \left\langle \Phi^+ \right| \tag{3.2}$$

for some F, where

$$\left| \Psi^\pm \right\rangle = \frac{1}{\sqrt{2}} (\left| 01 \right\rangle \pm \left| 10 \right\rangle)$$
$$\left| \Phi^\pm \right\rangle = \frac{1}{\sqrt{2}} (\left| 00 \right\rangle \pm \left| 11 \right\rangle) \tag{3.3}$$

are the Bell states, which are maximally entangled.

The state W_F is called a Werner state[13] of purity F and – since only local unitary operations were performed – is equivalent to the original state (thus in particular containing the same amount of entanglement).

3. Alice and Bob now pick two pairs on which to perform further transformations in the following way:

(a) Alice performs rotations by π rad around the y-axis on both her particles, converting the $\left| \Psi^- \right\rangle$ fraction into $\left| \Phi^+ \right\rangle$ and vice versa.

$$W_F \mapsto W_F' \tag{3.4}$$

where

$$W_F' = F \left| \Phi^+ \right\rangle \left\langle \Phi^+ \right| \; + \; \frac{1-F}{3} \left| \Psi^+ \right\rangle \left\langle \Psi^+ \right| \; + $$
$$+ \; \frac{1-F}{3} \left| \Phi^- \right\rangle \left\langle \Phi^- \right| \; + \; \frac{1-F}{3} \left| \Psi^- \right\rangle \left\langle \Psi^- \right| \tag{3.5}$$

(b) Alice and Bob apply a biliteral XOR (or BXOR[14]) on these two pairs.

$$W_F' \mapsto (U_{XOR} \otimes U_{XOR}) \; W_F' \; (U_{XOR} \otimes U_{XOR})^\dagger \tag{3.6}$$

with the XOR-quantum-gate[12]

$$U_{XOR} := \left| \uparrow_{source} \uparrow_{target} \right\rangle \left\langle \uparrow_{source} \downarrow_{target} \right| + \left| \uparrow_{source} \downarrow_{target} \right\rangle \left\langle \uparrow_{source} \uparrow_{target} \right| +$$
$$+ \left| \downarrow_{source} \downarrow_{target} \right\rangle \left\langle \downarrow_{source} \downarrow_{target} \right| + \left| \downarrow_{source} \uparrow_{target} \right\rangle \left\langle \downarrow_{source} \uparrow_{target} \right| \tag{3.7}$$

(c) Both perform spin measurements along the z-axis on the pair that was used as target in the previous step. Note that this step is the only nonunitary (i.e. irreversible) action performed in the protocol.

(d) Alice and Bob communicate their measurement results to each other classically. If they match, the source pair is kept (otherwise it is discarded).

(e) Finally, Alice may perform another rotation around the y-axis in order to transform the resulting state back into a Werner state.

4. The resulting state now has the new purity

$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} \tag{3.8}$$

which is satisfies $F' > F$ for all $F > \frac{1}{2}$ (see Fig. 1).

5. Step 3 can be repeated arbitrarily often, increasing the purity (i.e. the entanglement per pair) each time.
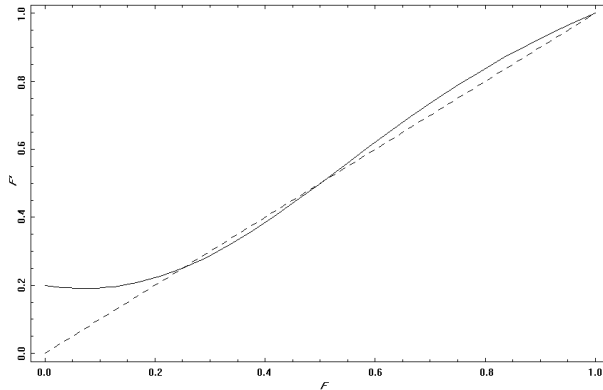

Fig. 1: Efficiency of the BBPSSW-protocol. The solid line shows the purity F' after applying the protocol, whereas the dashed line represents the purity F before.

Note that although the efficiency of this process, i.e. the number of distilled maximally entangled states per less entangled input state, tends to zero, there are methods to achieve nonzero distillation rates by more complicated protocols, allowing to distill any number of maximally entangled states from a finite number of input states[12].

The question remains, whether mixed entangled states can always be distilled to maximally entangled pure states and if not so, how these undistillable ('bound') entangled states can be recognised.

16

3.3 Bound Entanglement

Questions about the existence and identification of bound entangled states are rather complicated, since there are infinitely many possible distillation protocols and there is no reason why a state that cannot be distilled by one of them should not be distillable by any other one.

Fortunately, a general necessary and sufficient criterion for distillability of a state can be given via its partial transposition (i.e. a transposition in one of its subsystems, while the other subsystem is left unchanged). The partial transposition of a state ρ is defined by[15]

$$\rho^{T_A} = \sum_{i,j=1}^{d_A} \sum_{k,l=1}^{d_B} \langle i,k | \rho | j,l \rangle \ | j,k \rangle \langle i,l |$$ (3.9)

where d_A and d_B are the dimensions of the subspaces A and B, respectively. A state ρ is distillable iff there is an integer n such that the inequality

$$\langle \Psi | (\rho^{T_A})^{\otimes n} | \Psi \rangle \geq 0$$ (3.10)

(where $\rho^{\otimes n} = \rho \otimes \rho ... \otimes \rho$ is the n-fold copy of ρ) is violated by a Schmidt rank 2 vector $|\Psi\rangle$[16].

From this follows the much more simple (although weaker) condition, that ρ^{T_A} must be a nonpositive operator if ρ is free entangled (i.e. distillable). Such a state ρ is called a NPT-state (nonpositive partial transposition), while otherwise it is called a PPT-state (positive partial transposition).

Note that since the eigenvalues of a matrix do not depend on the choice of basis, neither does the positivity (while the eigenvectors do). Also it does not matter, which of the subsystems is being transposed, since an overall transposition does not change the eigenvalues.

Using this, one just has to find an entangled PPT-state (which as well is not a trivial task, but nevertheless is possible) in order to prove the existence of bound entanglement. The first state proven to be bound entangled was the two-qutrit state[16]

$$\rho_a = \frac{1}{8a+1} \begin{pmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{pmatrix}$$ (3.11)

with $0 < a < 1$. However, many more examples followed, making sure that bound entangled states are not at all rare (although hard to detect, as will be seen in the next section) and do not form a set of measure zero on the underlying Hilbert space.

An even more difficile task is to prove the existence or nonexistence of NPT bound entanglement. Since the nonpositivity of the partially transposed density matrix is not a sufficient criterion for distillability, this question cannot be trivially answered and has not been definitely solved yet. There exists evidence however, that strongly suggests the existence of NPT bound entanglement[17, 18].

It seems quite obvious, that bound entanglement is not very useful, since it is a rather weak kind of entanglement (as mentioned previously, all Werner states with purity $F > \frac{1}{2}$ can be distilled, hence, all bound entangled states have to be states of lower purity – similar bounds exist for higher dimensional generalisations of the discussed Werner state) and cannot be distilled to higher purity. Surprisingly, even this weak form of entanglement suffices for various quantum-informational tasks[19, 20]. Also, there still seems to be a chance to "quasi-distill" bound entangled states[21].

Quasi-Distillation of Bound Entanglement

If Alice and Bob share only a small number of (or even only one) nonmaximally free entangled states but a large pool of bound entangled states, there is a possibility for them to transfer some of the entanglement from these bound entangled states into the free entangled ones. The main difference between this procedure and genuine distillation is that the probability of success is not equal to 1 in this case, assuming a limited supply of free entangled states. While in original entanglement distillation two copies of the same state were subjected to local measurements at a time, here it is one copy of the bound entangled state and one copy of the free entagled one. Hence, if the measurement outcome is unsatisfactory, the used free entangled state is lost.

Nevertheless, this concept allows bound entanglement to be much more useful than it might seem at first glance, even if it still does not compare to free entanglement.

It is now obvious, how knowledge about different kinds of entangled states can be useful in order to be able to understand quantum information theory and to practically apply it. Therefore it is necessary to find various means to detect entanglement and to find out which of these are useful in respect to the different types of entanglement.

4 Detecting Entanglement

From now on, entanglement shall be viewed from a more theoretical and mathematical point of view.

In order to detect entanglement in quantum states, one obviously first needs to define it properly.

4.1 Defining Entanglement

A bipartite pure state $|\Psi\rangle$ is called separable iff it can be written as a single tensor product of states in the subsystems A and B (that is, if its Schmidt rank equals one):

$$|\,\Psi\,\rangle = |\,\Psi^A\,\rangle \otimes |\,\Psi^B\,\rangle \tag{4.1}$$

Every nonseparable state vector is called entangled and has the form

$$|\,\Psi\,\rangle = \sum_{i=1}^{d_A}\sum_{j=1}^{d_B} c_{ij} |\,\Psi_i^A\,\rangle \otimes |\,\Psi_j^B\,\rangle \tag{4.2}$$

with at least two nonzero complex coefficients c_{ij}.

Equivalently, a pure state is called separable iff its reduced density matrices correspond to pure states.

A state is maximally entangled, if it is pure and its reduced density matrices are maximally mixed. Equivalently, a pure state is maximally entangled iff it has full Schmidt rank and each term is equally weighted.

While the situation is rather simple for pure states, analysing mixed states can be very difficult due to the nonuniqueness of decompositions of density matrices into pure states. A mixed state is called separable iff it can be written in the form

$$\rho = \sum_{i=1}^{d_A}\sum_{j=1}^{d_B} p_{ij}\ \rho_i^A \otimes \rho_j^B \tag{4.3}$$

where d_A and d_B are the dimesions of the subspaces, the ρ_i^A and ρ_j^B are density matrices of the respective subspaces and the p_{ij} are probabilities, such that

$$p_{ij} \geq 0, \quad \text{and} \quad \sum_{i,j} p_{ij} = 1 \tag{4.4}$$

For reasons of convenience, the indices can be chosen such that eq. (4.3) assumes the form

$$\rho = \sum_i p_i\ \rho_i^A \otimes \rho_i^B \tag{4.5}$$

For mixed states, the form of an entangled state cannot be explicitly formulated other than by saying that it cannot be written in the form (4.3). That is why it is rather difficult to decide, if a given state is separable or entangled.

4.2   Pure States

As mentioned, for pure states, detecting entanglement is a rather simple task and can be done in various ways.

1. According to the definition of entangled pure states (4.1), a separable state's Schmidt rank equals one. Hence, iff any state has a Schmidt rank greater than one, it is entangled.

2. From the definition of entanglement follows, that the composite system contains more information (i.e. purity) than the subsystems. In particular, the reduced density matrices of a pure state are pure states themselves iff the state is separable. Consequently, a pure state ρ is separable iff one of the following equivalent statments is true:

$$\mathrm{Tr}((\rho^A)^2) = 1$$

$$S(\rho^A) > 0 \tag{4.6}$$

where

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \tag{4.7}$$

is the von Neumann entropy, which is a measure for the mixedness of a quantum state.

3. Of course every separability criterion for general states can be applied to a pure state as well, although this is generally not the most economic way to study pure states. Still, iff a pure state is separable, it satisfies any of the separability criteria that will be discussed in this section.

4.3   Positive and Completely Positive Maps

A map $\Lambda : \mathcal{B} \to \mathcal{B}$ is called a positive map (PM) iff it maps all positive operators ρ onto positive operators

$$\rho \geq 0 \Rightarrow \Lambda(\rho) \geq 0 \quad \forall \rho \in \mathcal{B} \tag{4.8}$$

A PM is called completely positive (CP) iff it remains positive under extensions to all higher dimensions

$$\rho \geq 0 \Rightarrow (\Lambda \otimes \mathbb{1}_d)(\rho) \geq 0 \quad \forall \rho \in \mathcal{B} \otimes \mathbb{C}^d, \quad \forall d \in \mathbb{N} \qquad (4.9)$$

Interestingly, not all PMs have this property, which allows maps that are positive but not CP to detect entangled states.

It is easy to see that any PM leaves a separable state ρ positive, since

$$(\Lambda \otimes \mathbb{1})(\rho) = (\Lambda \otimes \mathbb{1}) \left(\sum_i p_i \; \rho_i^A \otimes \rho_i^B \right) = \sum_i p_i \; \Lambda(\rho_i^A) \otimes \rho_i^B \geq 0 \quad (4.10)$$

which is not true for general states. In fact, for each entangled state ρ there exists a PM Λ such that[22]

$$(\Lambda \otimes \mathbb{1})(\rho) \not\geq 0 \qquad (4.11)$$

Conversely, a state ρ is separable iff it satisfies

$$(\Lambda \otimes \mathbb{1})(\rho) \geq 0 \qquad (4.12)$$

for all PMs Λ.

Although this is a necessary and sufficient separability criterion, its strength cannot be used to its full extent, since there is no way to apply it to any given state. Presently, knowledge about non-CP PMs is rather limited. However, as far as known, non-CP PMs can be used to formulate necessary separability criteria.

4.3.1 PPT (Peres-Horodecki) Criterion

The probably "strongest" PM (in the sense of being able to detect most entangled states) is the transposition T. Due to the arguments given in the previous subsection, the partial transposition $T \otimes \mathbb{1}$ of a seperable state is positive, while there are entangled states that behave differently (as mentioned in section 3.3). Hence, a state with nonpositive partial transposition (NPT) has to be entangled, while a state with positive partial transposition (PPT) can be either separable or (bound) entangled[23]. This is called the PPT-criterion (or Peres-Horodecki criterion) of separability.

In low dimensions, this criterion is much stronger. For systems of two qubits[24] and systems of one qubit and one qutrit[25] the transposition is

the only relevant PM, since here all PMs Λ are decomposable, i.e. can be written in the form

$$\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} T \tag{4.13}$$

where the Λ_i^{CP} are CP maps.

From this follows that any state that is nonpositive under any of these maps must also be NPT, since

$$(\Lambda \otimes \mathbb{1})(\rho) = (\Lambda_1^{CP} \otimes \mathbb{1})(\rho) + (\Lambda_2^{CP} \otimes \mathbb{1})(\rho^{T_A}) \tag{4.14}$$

can only be nonpositive if ρ^{T_A} is.

Consequently, in these cases the PPT criterion is both necessary and sufficient for separability, thus providing a very simple procedure to determine without a doubt if any given state in these dimensions is separable or entangled.

Partial Transposition of Expansions of Given States

Consider states ρ' on the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{aux} = \mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B^{\otimes l}$, such that ρ' is an extension of ρ (i.e. $\text{Tr}_{\mathcal{H}_{aux}}(\rho') = \rho$) that is symmetrical under exchange of any copies of the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$.

If ρ is seperable, such an expansion is of the form

$$\rho' = \sum_i p_i \left(\left| \Psi_i^A \right\rangle \left\langle \Psi_i^A \right| \right)^{\otimes k} \otimes \left(\left| \Psi_i^B \right\rangle \left\langle \Psi_i^B \right| \right)^{\otimes l} \tag{4.15}$$

and hence is positive under any partial transposition.

Consequently, if there exists an expansion ρ' of a state ρ that satisfies the above symmetry conditions and has nonpositive partial transposition, ρ is entangled[26].

Note that this is a stronger criterion than the normal PPT-criterion, since if a state is NPT, there automatically exists a NPT expansion, while the converse of this statement is not true (as can be seen from examples in ref. [26]).

In order to determine if a given state is entangled, this criterion can by used stepwise. If the partial transposition itself is positive, it can be expanded to a higher dimensional Hilbert space. If this expansion is still positive, it can be expanded further, and so on. Means to find suitable expansions have been shown in ref. [26].

4.3.2 Reduction Criterion

Another example for non-CP PMs is the reduction criterion[27], which consists of applying the positive map

$$\Lambda(\sigma) = \mathbb{1}\,\mathrm{Tr}(\sigma) - \sigma \tag{4.16}$$

to one of the subsystems, resulting in the separability criteria

$$\begin{aligned}
(\Lambda \otimes \mathbb{1})(\rho) &= \mathbb{1} \otimes \rho_B - \rho \geq 0 \\
(\mathbb{1} \otimes \Lambda)(\rho) &= \rho_A \otimes \mathbb{1} - \rho \geq 0
\end{aligned} \tag{4.17}$$

Although the reduction criterion is necessary and sufficient for separability for systems in $2\otimes 2$ and $2\otimes 3$, it follows from the discussion in (4.3.1) that it is a weaker criterion than the PPT criterion, since it does not detect all NPT states in higher dimensions. However, violation of the reduction criterion is equivalent to distillability via a special class of distillation protocols, that is a straightforward generalisation of the usual $2 \otimes 2$ dimensional one. In particular, any state violating it can be distilled (while a state satisfying it may still be distillable by a different protocol) and is hence free entangled.

4.4 Cross-Norm- and Realignment Criterion

The cross-norm criterion of separability[28] states, that a state ρ is separable iff $\|\rho\|_\gamma = 1$, where the cross-norm $\|.\|_\gamma$ of a density matrix is defined by

$$\|t\|_\gamma = \inf_{\{u_i, v_i\}} \sum_i \|u_i\|_1 \|v_i\|_1 \tag{4.18}$$

where the infimum is taken over all sets of weighted density matrices $\{u_i, v_i\}$ satisfying $t = \sum_i u_i \otimes v_i$.
This norm is also often refered to als the greatest cross norm, since it majorises any subcross norm (a norm is said to be subcross, if $\|a \otimes b\| \leq \|a\| \|b\|$ and is called cross if the equality holds).
Although the cross-norm criterion is necessary and sufficient for separability, it is in general not applicable, since the infimum is hard to compute. However, it implies a weaker criterion, that is not sufficient for separability, but easily computable.

It follows from the cross-norm criterion[29], that if a state ρ is separable, then

$$\|\rho_R\|_1 \leq 1 \tag{4.19}$$

where the realigned density matrix ρ_R is defined by

$$\rho_R = \sum_{i,j,k,l} \langle i,k| \, \rho \, |j,l\rangle \; |i,j\rangle \langle k,l| \tag{4.20}$$

Note that despite the formal similarity between the definitions of the realigned density matrix and the partially transposed density matrix, they are completely different objects. In particular, ρ_R is not hermitian. This realignment criterion is – since it is a consequence of the cross-norm criterion – also often referred to as the computable cross-norm (CCN) criterion.

The realignment criterion was proven[30] to be independent from (i.e. neither stronger nor weaker than) the PPT criterion, as it is capable of detecting certain PPT entangled states, whereas it is not sufficient in the $2 \otimes 2$ case[30] (there are however whole sets of states, for which it is sufficient, such as all pure states or states of $2 \otimes 2$ systems with maximally mixed subsystems).

Due to the mathematical similarity between the realigned density matrix and the partially transposed density matrix, it seems reasonable that an expansion to higher spaces could lead to a more powerful hierachical set of separability criteria, like it does for the PPT criterion.

4.5 Majorisation Criterion

A completely different approach can be given by considering the mixedness of a given quantum state and its reductions (i.e. reduced density matrices), thus generalising the entropic separability criterion for pure states (4.6). Many criteria were formulated using the von Neumann entropy of both these objects and relating them to each other, it turns out however, that a stronger separability criterion can be given.

If a state ρ is separable, then is satisfies[31]

$$\begin{aligned} \lambda(\rho) \prec \lambda(\rho_A) \\ \lambda(\rho) \prec \lambda(\rho_B) \end{aligned} \tag{4.21}$$

where $\rho_{A,B}$ are the reduced density matrices, $\lambda(\sigma)$ is the vector of σ's eigenvalues (where there are zeroes appended to the $\lambda(\rho_{A,B})$, such that all vectors

have the same dimension). A vector $x = (x_1, ..., x_d)$ is said to be majorised by a vector $y = (y_1, ..., y_d)$ (i.e. $x \prec y$) if

$$\sum_{i=1}^{k} x_i^{\downarrow} \leq \sum_{i=1}^{k} y_i^{\downarrow} \quad \forall k \tag{4.22}$$

where $x^{\downarrow}$ is the vector x with sorted components, i.e. $x_1 \leq ... \leq x_d$ (and analogously for y).

Note that if a state ρ satisfies the majorisation criterion, it follows that it also satisfies weaker entropic criteria, for example

$$\begin{aligned} S(\rho) &\geq S(\rho_A) \\ S(\rho) &\geq S(\rho_B) \end{aligned} \tag{4.23}$$

where $S(\sigma)$ is the von Neumann entropy (4.7).

4.6 Range Criterion

A separability criterion seemingly independant from all the ones mentioned above can be given via the range of density matrices and their partial transpositions[32]. The range of ρ is defined as the set of all vectors $|\Psi\rangle$ for which there is another vector $|\Phi\rangle$ such that

$$|\Psi\rangle = \rho |\Phi\rangle \tag{4.24}$$

If a state ρ on a Hilbert space $\mathcal{H}$ with $\dim\mathcal{H} = m$ is separable, then there exists a set of product vectors $\{\psi_i \otimes \phi_j\}, \{i, j\} \in I$ (where I is a set of N pairs of indices with $N = \#I \leq m^2$) and probabilities $\{p_{i,j}\}$ such that

1. the ensembles $\{\psi_i \otimes \phi_j, p_{i,j}\}$, $\{\psi_i^* \otimes \phi_j, p_{i,j}\}$ and $\{\psi_i \otimes \phi_j^*, p_{i,j}\}$ correspond to the matrices ρ, ρ^{T_A} and ρ^{T_B}

2. the ranges of ρ, ρ^{T_A} and ρ^{T_B} are spanned by the vectors $\{\psi_i \otimes \phi_j\}$, $\{\psi_i^* \otimes \phi_j\}$ and $\{\psi_i \otimes \phi_j^*\}$, respectively

where the asterisk denotes complex conjugation.
It was shown[32] that this criterion is independant from the PPT criterion, as there are PPT entangled states that violate the range criterion and there also are NPT states satisfying it.

4.7 Entanglement Witnesses

From the definition of seperable states

$$\rho = \sum_i p_i \left| \Psi_i^A \right\rangle \left\langle \Psi_i^A \right| \otimes \left| \Psi_i^B \right\rangle \left\langle \Psi_i^B \right| \tag{4.25}$$

it follows immediately that the set of separable states S is a convex and closed subset of the set of all states on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Also, of course a set containing only one state is convex, compact and closed.

If there are two convex and compact sets of which at least one is closed, then there exists a hyperplane that separates these sets from each other, i.e. one set lies completely on one side of the plane, while the other set lies completely on the other side. This is a corollary from the Hahn-Banach theorem[33].

From this now follows the entanglement witness theorem, which states that for each entangled state ρ there exists a hermitian operator W such that

$$\mathrm{Tr}(\rho W) < 0 \tag{4.26}$$

while

$$\mathrm{Tr}(\sigma W) \geq 0 \quad \forall\, \sigma \in S \tag{4.27}$$

This operator is called an entanglement witness. If in addition there exists a separable state $\tilde{\rho}$ such that

$$\mathrm{Tr}(\tilde{\rho} W) = 0 \tag{4.28}$$

then W is called an optimal entanglement witness[22].

This is a direct consequence of the above statement, since all states ρ with $\mathrm{Tr}(\rho W) = 0$ form a hyperplane (remember that $\mathrm{Tr}(AB) = \langle A | B \rangle$ is the scalar product in the Hilbert-Schmidt space for hermitian operators A and B), and all states ρ_+ satisfying $\mathrm{Tr}(\rho_+ W) > 0$ are located on one side of it, while all states ρ_- with $\mathrm{Tr}(\rho_- W) < 0$ are located on the other side. If W is an optimal entanglement witness (often denoted by W_{opt}), the corresponding hyperplane is a tangent plane to S (for illustration see Fig. 2). Note that W and αW are the same witness for any complex number α.

Of course, optimal entanglement witnesses are of high interest, since they can detect more entangled states than nonoptimal ones and give a deep insight into the geometrical structure of a Hilbert space. In particular, the set of separable states S is fully characterised by the set of all optimal entanglement witnesses (since these form the border of S[34]).

Obviously, it is rather difficult to check wether an arbitrary operator satisfies condition (4.27). However, in some cases there are means to check this.
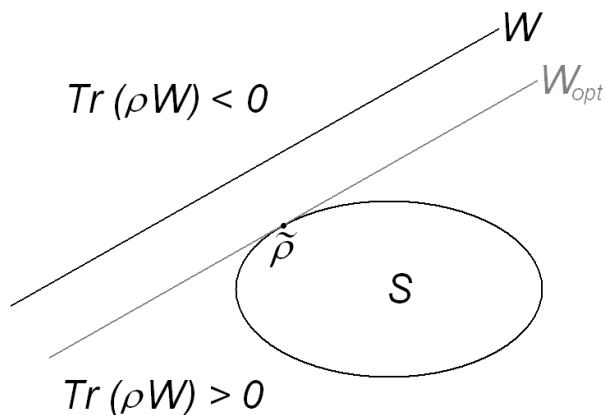
Fig. 2: Illustration of entanglement witnesses

Is a given operator an entanglement witness?

In order to see if a given operator is indeed an entanglement witness, and in particular satisfies condition (4.27), it is useful to investigate decompositions of general separable states into generlaised Gell-Mann matrices λ_i (or any other basis of the respective Hilbert space, see 2.3.4). Any state can be decomposed in the following way:

$$\sigma = \frac{1}{d^2}\left(\mathbb{1}\otimes\mathbb{1} + \sum_{i=1}^{d^2-1} a_i\lambda_i\otimes\mathbb{1} + \sum_{i=j}^{d^2-1} b_j\mathbb{1}\otimes\lambda_j + \sum_{i,j=1}^{d^2-1} c_{i,j}\lambda_i\otimes\lambda_j\right) \quad (4.29)$$

with adequate bounds on the coefficients a_i and b_i (depending on the dimension d). The bounds on $c_{i,j}$ for separable states are much tighter than those for general states. Thus, the quantity $\mathrm{Tr}(\sigma W)$ can be computed for all separable states, allowing to check if it is positive.

Geometric entanglement witnesses

A geometrically very intuitive way of constructing entanglement witnesses is the method of geometric entanglement witnesses[35]. Given an entangled state ρ the operator

$$C = \tilde{\rho} - \rho - \langle\tilde{\rho}|\tilde{\rho} - \rho\rangle\,\mathbb{1} \quad (4.30)$$

is an entanglement witness detecting ρ for certain states $\tilde{\rho}$. In particular, C is an optimal entanglement witness iff $\tilde{\rho}$ is the separable state closest to ρ in the Hilbert-Schmidt metric (methods to find the closest separable states are discussed in section 5.3.1). This can be easily understood regarding

the illustration in Fig. 3: Due to the construction of C, the corresponding hyperplane is orthogonal to the line between ρ and $\tilde{\rho}$ and also contains $\tilde{\rho}$ itself, since

$$
\begin{aligned}
0 = \mathrm{Tr}(\rho_p C) = \mathrm{Tr}(\rho_p(\tilde{\rho} - \rho - \langle \tilde{\rho} | \tilde{\rho} - \rho \rangle \, \mathbb{1})) \\
= \langle \rho_p | \tilde{\rho} - \rho \rangle - \langle \tilde{\rho} | \tilde{\rho} - \rho \rangle \\
= \langle \rho_p - \tilde{\rho} | \tilde{\rho} - \rho \rangle
\end{aligned}
\tag{4.31}
$$

where the last equality holds since ρ_p per definition lies on the plane (and in particular if $\rho_p = \tilde{\rho}$).
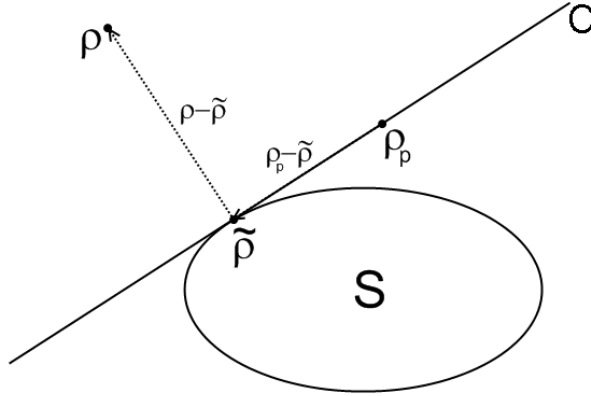

Fig. 3: Illustration of an optimal geometric entanglement witness

Geometric entanglement witnesses can be used very effectively to iteratively construct the complete set of separable states[36] (as illustrated in Fig. 4). To start, one needs a number of separable states $\alpha_{1,...,n}$, whose convex hull evidently forms a polytope containing only separable states (black triangle in Fig. 4). Each of this polytope's borderplanes can be described by a geometric operator A_i (i.e. a operator of the form 4.30) that is not an entanglement witness, since its expectation value is not positive for all separable states. These operators can now be shifted towards the edge of the set of separable states S, whilst observing the entanglement witness criterion eq. (4.27) (by means of decomposition coefficients, as discussed above) until they become optimal entanglement witnesses corresponding to tangent hyperplanes of S (grey lines in Fig. 4) which contain a new separable state β_i each. The states α_i and β_i together now form a new polytope, containing more separable states.

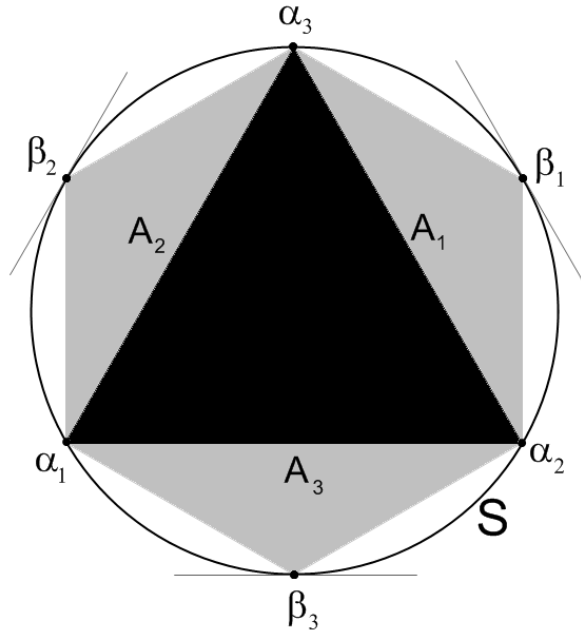This procedure is called inside-out-shifting and can be repeated arbitrarily

Fig. 4: Illustration of the procedure to construct the set of separable states (inside-out-shifting)

often. If S is a polytope, then the procedure is finite and ends as soon as all resulting entanglement witness planes contain more than one separable state, i.e. form the borderplanes of S. If S has a more complex shape (as in Fig. 4), the procedure can be repeated over and over until the desired precision is achieved.

In contrast to inside-out-shifting, the same result can be obtained by outside-in-shifting. In this case, one starts with a set of nonoptimal geometric entanglement witnesses and shifts them towards the set of separable states until they become optimal.

Relations between entanglement witnesses and other separability criteria

Since entanglement witnesses are very general objects, many other separability criteria can be written as such.

A very intuitive relation is the one between entanglement witnesses and positive maps. Since these both are necessary and sufficient separability criteria, there has to be both an (optimal) entanglement witness and a positive map for each nonseparable state to be detected, between which one might intuitively conjecture that there exists a kind of isomorphism (of course,

for each PM there need to be several entanglement witnesses due to the geometry of the set of states detected by the PM, which in general cannot be described by a single hyperplane). This isomorphism is called the Jamiolkowski-isomorphism[37, 38]. For each non-CP PM Λ there exists a family of entanglement witnesses

$$W = (\Lambda \otimes \mathbb{1}) \left(|\Psi\rangle \langle\Psi| \right) \tag{4.32}$$

where $|\Psi\rangle$ is any maximally entangled state.
Evidently, this makes any separability criterion formulated via positive maps (in particular the PPT criterion and the reduction criterion) possible to be considered as a set of entanglement witnesses.

Structure of entanglement witnesses

Since entanglement witnesses are a very general class of operators, their mathematical structure is rather general as well. Obviously, a product operator cannot be an entanglement witness, but already a sum of two product operators can be[34].
In order to yield positive and negative expectation values for different states, an entanglement witness evidently needs to be an indefinite operator. However, from the positivity for all separable states it follows, that all diagonal elements in the computational basis have to be positive semidefinite.

4.8   Entanglement Measures

In the following section, measures for entanglement will be discussed. Of course, if a quantum state possesses any nonzero amount of entanglement (in any suitable measure), it needs to be entangled. Hence, entanglement measures can, in a way, also be used to detect entanglement, although these are usually much more difficult to compute than the separability criteria discussed above. Also, most of the following entanglement measures are quantisations of existing separability criteria (as will be seen), so that the procedure of detecting entanglement by means of a measure is fully equivalent to using the corresponding separability criterion in the first place.

5 Entanglement Measures

Trying to quantify entanglement, one is immediately confronted with an important question: What properties does an entanglement measure need to have in order to be useful? This question cannot be answered completely objectively. While some properties seem to be necessary, others are only needed in order to preserve intuitive pictures which are not necessarily correct.
Usually, the following catalog of properties is wished to be fulfilled by a "good" entanglement measure $E(\rho)$[7]:

1. ρ is separable $\Leftrightarrow E(\rho) = 0$
   This is a very intuitive requirement. A measure should only yield no entanglement at all for separable states and should not yield any entanglement for any separable state.

2. ρ is maximally entangled $\Leftrightarrow E(\rho) = \max E(\omega)$ where the maximum is taken over all states ω. An entanglement measure should yield its maximal value for maximally entangled states and for maximally entangled states only.

3. No increase under LOCC: $E(\rho) \geq E(\Lambda_{LOCC}(\rho))$
   Since entangled states cannot be created by local operations and classical communications (LOCC), it seems reasonable, that the amount of entanglement in a quantum state cannot be increased by LOCC either.

4. Invariance under local unitary operations: $E(\rho) = E(U_1 \otimes U_2 \rho U_1^\dagger \otimes U_2^\dagger)$
   Since unitary operations can be regarded as changes of the basis, this is equivalent to the statement that the entanglement should not depend on the choice of basis. If this requirement is fulfilled, it induces equivalence classes of states containing the same amount of entanglement and being linked to each other via unitary transformations. This condition is in short also referred to as unitary invariance, omitting the "local"

5. Continuity: $||\rho_1 - \rho_2|| \to 0 \Rightarrow E(\rho_1) - E(\rho_2) \to 0$
   Any entanglement measure should be continuos on the Hilbert space of states, so that the entanglement cannot change dramatically for infinitesimal changes of the state.

6. Convexity: $E(\lambda\rho_1 + (1-\lambda)\rho_2) \leq \lambda E(\rho_1) + (1-\lambda)E(\rho_2)$
   for $0 < \lambda < 1$. The entanglement of any convex combination of two states should not exceed the convex sum of their single entanglements. This requirement is very intuitive in a geometric point of view, since

a state's distance from the set of separable states S intuitively corresponds to an entanglement measure itself. Now, since S is convex, any convex combination of two states $\notin S$ can only be closer to S than its components. Also, it seems obvious that the more mixed a state is, the less entanglement it can contain, since otherwise entanglement could be created simply by mixing states.

7. Additivity: $E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2)$
   Any two (or more) states should always contain exactly the same entanglement that is contained in each of them taken together, since these states can easily be separated from each other and be used to perform quantum tasks exploiting entanglement, the possibility of which should be contained in an entanglement measure.
   Often only a weaker form of this property is required, namely additivity for equal states and subadditivity for inequal states:
   $E(\rho^{\otimes n}) = nE(\rho)$ and $E(\rho_1 \otimes \rho_2) \leq E(\rho_1) + E(\rho_2)$

8. Normalisation: $0 \leq E(\rho) \leq \log d$ where d is the dimension of the Hilbert space. Usually, when dealing with only one particular Hilbert space, the logarithmic base is chosen to be d, such that $0 \leq E(\rho) \leq 1$. In general, the choice of the logarithmic base depends on the units in which the entanglement is measured, so called dits of entanglement (edits). In most cases, the base is chosen to be two, such that the entanglement is measured in ebits.

9. For an entanglement measure to be useful, there needs to be an operational way of computation for all states. This turns out to be the main problem very often.

It turns out, that finding an entanglement measure that fulfills all of the above criteria is extremely difficult, which is why there are many candidates, each of which does not satisfy all of the criteria.

5.1 Pure States

For pure states, it is very easy to quantify the separability criteria discussed in the previous section. Since entanglement can be seen as the amount of information that is contained in a system, but not in its subsystems taken together (i.e. the information that is lost when viewing not the composite system but its subsystems), the mixedness of the subsystems seems an

appropriate measure for entanglement:

$$E(\rho) = S(\rho^A) = S(\rho^B) \tag{5.1}$$

where $\rho^{A,B}$ are the reduced density matrices of ρ and S is any suitable entropy function, for example the von-Neumann-entropy $S(\sigma) = -\text{Tr}(\sigma \log \sigma)$ or the linear entropy $S(\sigma) = \frac{d}{d-1}(1 - \text{Tr}(\sigma^2))$.

This family of measures satisfies all of the properties discussed above and hence seems to be a very good measure for entanglement. However, it can only be applied to pure states.

5.2   Bell Inequalities

Historically, the first discrimination of quantum correlations as opposing to classical correlations was found by John S. Bell[3], who formulated a class of correlation-inequalities – Bell inequalities (BI) – that any local realistic theory necessarily has to satisfy. The terms "local" and "realistic" are here used in the sense of Einstein, Podolsky and Rosen[2]:

Locality: Any physical theory should be compatible with the theory of special relativity and especially not allow any faster than light transmission of information.

Realism: Any physical quantity which can be predicted with certainty and without disturbing the system, corresponds to an element of reality. Hence, if a quantity is considered to be physically real, its value should exist independently of any measurement.

Obviously, quantum mechanics violates these criteria (to be more precise: depending on the choice of interpretation, it violates at least one of them. According to the widely accepted Kopenhagen interpretation, both are violated, while for example the Bohmian interpretation[39] is only nonlocal but realistic) and also violates Bell's inequalities.

In accordance with the commonly used terminology, a quantum state is called nonlocal if it violates any Bell inequality, while else (if it satisfies all Bell-inequalities) it is called a local state. This however does not necessarily require it to be "nonlocal" in the actual sense, since the violation can also be explained by a local but nonrealistic model.

Note that there obviously have to be entangled states, which do not violate any Bell inequality, since these represent an upper bound to correlations and do not distinguish between classical correlations (which result from mixing of pure product states) and quantum correlations. If a state possesses a certain

amount of quantum correlations (i.e. entanglement) and just a very little amount of classical correlations, it may not violate any BI, since its total correlations are well within range of local realism.

Local Hidden-Variable Models

Any local realistic theory can be formulated via local hidden variables (LHV), i.e. a set of parameters λ that completely determine the outcome of any given measurement and are local (in the sense of there being no interaction or dependance between the parameters for systems that are spacially separated from each other), while the parameters themselves do not have to be accessable by any experiment.

It is obvious, that any quantum product state can be described by LHVs, but the question remains if the same holds for entangled states. As mentioned above, there are entangled states that violate Bell's inequalities (nonlocal states) and such that do not (local states). For pure states the situation is rather simple, as any entangled pure state is nonlocal and incompatible with all LHV models[40, 41]. For mixed states, the distinction is not that easy. Clearly, nonlocal states can never be fully reproduced by LHV models, however, surprisingly, there are local states for which there does not exist a suitable LHV-description[42], while there also are entangled states that can be modeled by LHVs[43].

The CHSH-Inequality

The by far most commonly used Bell inequality is the one for systems of $2 \otimes 2$ dimensions derived by Clauser, Horne, Shimony and Holt[44] (CHSH inequality). In a system of 2 qubits, the expectation value of a bilateral (e.g. spin-) measurement along the directions $\vec{a}$ in the first system $\vec{b}$ in the second can be defined in a LHV model by

$$E(\vec{a}, \vec{b}) = \int A(\vec{a}, \lambda) B(\vec{b}, \lambda) \rho(\lambda) d\lambda \qquad (5.2)$$

where $\rho(\lambda)$ is any distribution function for the hidden value λ and $A(\vec{a}, \lambda)$ and $B(\vec{b}, \lambda)$ are the functions determining the (normalised) measurement results in both systems, depending on the direction of measurement and the hidden parameter.

Using this definition, the CHSH inequality can be found, starting with the identity

$$E(\vec{a_1}, \vec{b_1}) - E(\vec{a_1}, \vec{b_2}) = E(\vec{a_1}, \vec{b_1})(1 \pm E(\vec{a_2}, \vec{b_2})) - E(\vec{a_1}, \vec{b_2})(1 \pm E(\vec{a_2}, \vec{b_1})) \qquad (5.3)$$

it follows by using the triangle inequality

$$\left| E(\vec{a_1}, \vec{b_1}) - E(\vec{a_1}, \vec{b_2}) \right| \leq \left| E(\vec{a_1}, \vec{b_1})(1 \pm E(\vec{a_2}, \vec{b_2})) \right| + \left| E(\vec{a_1}, \vec{b_2})(1 \pm E(\vec{a_2}, \vec{b_1})) \right|$$

$$\leq \left| 1 \pm E(\vec{a_2}, \vec{b_2}) \right| + \left| 1 \pm E(\vec{a_2}, \vec{b_1}) \right|$$

$$(5.4)$$

where the second line follows from the normalisation $-1 < E(\vec{a_i}, \vec{b_j}) < 1$. The inequality is strongest when the sign is chosen such that

$$I = \left| E(\vec{a_1}, \vec{b_1}) - E(\vec{a_1}, \vec{b_2}) \right| + \left| E(\vec{a_2}, \vec{b_2}) + E(\vec{a_2}, \vec{b_1}) \right| \leq 2 \qquad (5.5)$$

This is the CHSH inequality.

Evidently, for local realistic theories, the maximal value (maximised over all suitable states and all directions $\vec{a_i}$ and $\vec{b_i}$) for I is 2, while the maximal possible value for any theory is 4 (since the single expectation values cannot exceed ± 1). Quantum mechanics however predicts a maximal value of $2\sqrt{2}$, which is reached by maximally entangled states.

Entangled pure two qubit states always violate this inequality. In an appropriate basis they can always be written in the form $|\Psi\rangle = \alpha |\uparrow\uparrow\rangle + \beta |\downarrow\downarrow\rangle$ (with $\alpha, \beta \in \mathbb{R}$ and $\alpha^2 + \beta^2 = 1$), then the maximal value (optimised over all angles) of the Bell parameter is $I = 2\sqrt{1 + 4\alpha^2\beta^2}$[41].

Since mixed states are more complicated to deal with, it is fortunate that a constructive way was found[45] to compute the maximal value of the Bell parameter for any two qubit state. Any two qubit state ρ can be written as

$$\rho = \frac{1}{4}(\mathbb{1} + \vec{a}\vec{\sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \vec{b}\vec{\sigma} + \sum_{m,n=1}^{3} t_{mn}\sigma_m \otimes \sigma_n) \qquad (5.6)$$

where the t_{mn} form a real three by three matrix T_ρ. The maximal value for the Bell parameter then can be written as

$$I_{max} = 2(u_1 + u_2) \qquad (5.7)$$

where $u_{1,2}$ are the two larger eigenvalues of the matrix $T_\rho^T T_\rho$.

The CHSH inequality is – in $2 \otimes 2$ dimensions – optimal in the sense that there is no other Bell inequality that is either more resistant to noise or yields a higher maximal violation[46].

For many years there have not been useful Bell inequalities for systems of higher dimensions. Only recently, a generalisation of the CHSH inequality to $d \otimes d$ dimensions was found and studied[46, 47]. The corresponding quantity reads

$$
\begin{aligned}
I_d = \sum_{k=0}^{\lfloor d/2 \rfloor - 1} \{ &[P(A_1 = B_1 + k) + P(B_1 = A_2 + k + 1) + \\
&+ P(A_2 = B_2 + k) + P(B_2 = A_1 + k)] - \\
&- [P(A_1 = B_1 - k - 1) + P(B_1 = A_2 - k) + \\
&+ P(A_2 = B_2 - k - 1) + P(B_2 = A_1 - k - 1)]\}
\end{aligned}
\tag{5.8}
$$

where $P(A_i = B_j + k)$ is the probability for the i-th measurement in the first system to yield the value of the j-th measurement in the second system plus k modulo d and $\lfloor . \rfloor$ is the floor-function (i.e. the function yielding the integer part of its argument). Due to the very general formulation in terms of computational basis vectors (which are always to be understood as modulo d), any of these inequalities can be applied to any $d' \otimes d'$-dimensional system, even if $d \neq d'$. For $d = 2$ this quantity is bounded by 3 for LHV models. The corresponding inequality

$$
I_2 = P(A_1 = B_1) + P(B_1 = A_2 + 1) + P(A_2 = B_2) + P(B_2 = A_1) \leq 3 \tag{5.9}
$$

is fully equivalent to the original CHSH inequality.

For any higher dimension $d > 2$, the expression is bounded by $I_d \leq 2$ for local realistic theories (while in all cases completely nonlocal theories could reach values up to $I_d = 4$).

A very central question is, if these "generalised CHSH inequalities" are optimal Bell inequalities in the same sense the original CHSH inequality is. As of yet, this question cannot be answered definitely, although there are certain unexpected properties of the higher dimensional inequalities, that suggest that they may not be. For example, the maximal violation of these higher dimensional Bell inequalities occurs for nonmaximally entangled states, i.e. a maximally entangled state yields a smaller violation than certain less entangled ones (the higher the dimension of the system, the bigger this difference gets)[48, 49].

This result offers two possible interpretations. Either the inequalities are in fact not optimal and there are others that do not show this property, or there is a more fundamental difference between quantum nonlocality and quantum entanglement than was known so far. While the latter case will be

discussed later in reference to entanglement measures, the first case raises the further question of how to design better Bell inequalities. Using more general measurements, such as positive operator valued measurements (POVMs [50]) would lead to inequalities in which the maximal possible values could be attained even by separable states[51], so it seems that a more appropriate way of generalising the CHSH inequality would be applying more than two von Neumann measurements per system.

Bell Operators

Often it is much easier to work not with the scalar Bell inequality itself, but to construct the corresponding Bell operator B and formulate the inequality via this operator and the studied state, e.g.

$$\langle \Psi | B | \Psi \rangle \leq 2 \tag{5.10}$$

In the case of a two qubit system, the the single measurements correspond to observables of the form $\vec{a}\vec{\sigma} \otimes \vec{b}\vec{\sigma}$ (with $|\vec{a}| = |\vec{b}| = 1$), such that the CHSH inequality assumes the form (5.10) with[52]

$$B = \vec{a_1}\vec{\sigma} \otimes (\vec{b_1} + \vec{b_2})\vec{\sigma} + \vec{a_2}\vec{\sigma} \otimes (\vec{b_1} - \vec{b_2})\vec{\sigma} \tag{5.11}$$

while for higher dimensions, the observables have to be constructed via projectors instead of Pauli matrices (as in ref. [48]).
Bell operators can easily be rewritten as nonoptimal entanglement witnesses W[53, 54]

$$W = 2\mathbb{1} - B \tag{5.12}$$

since then the defining properties of an entanglement witness follow directly from the fact that all separable states are local.

Hidden Nonlocality

A somewhat puzzling feature of quantum nonlocality is that it can be "hidden" in states, such that the state itself is local (does not violate any Bell inequality), but local operations in the subsystems yield a nonlocal state[55, 51].
A very simple example is given by the two qubit state

$$\rho(\lambda, \alpha) = \lambda |\Psi_\alpha\rangle \langle\Psi_\alpha| + \frac{1-\lambda}{2}(|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + |\downarrow\downarrow\rangle\langle\downarrow\downarrow|) \tag{5.13}$$

where $|\Psi_\alpha\rangle = \alpha\,|\uparrow\downarrow\rangle + \beta\,|\downarrow\uparrow\rangle$ and β such that $\alpha^2 + \beta^2 = 1$. This state is local if $\lambda \leq (1 + \alpha^2\beta^2)^{-1}$.

If now the local polarisation dependant filters

$$F_A = \begin{pmatrix} \sqrt{\beta/\alpha} & 0 \\ 0 & 1 \end{pmatrix} \qquad F_B = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\beta/\alpha} \end{pmatrix} \tag{5.14}$$

are applied to both subsystems accordingly, the resulting state is

$$\rho'(\lambda, \alpha) = \frac{1}{N}\left[2\lambda\alpha\beta\,|\Psi^-\rangle\,\langle\Psi^-| + \frac{1-\lambda}{2}(|\uparrow\uparrow\rangle\,\langle\uparrow\uparrow| + |\downarrow\downarrow\rangle\,\langle\downarrow\downarrow|) \right] \tag{5.15}$$

where $N = 2\lambda\alpha\beta + (1 - \lambda)$ is a normalisation-factor and $|\Psi^-\rangle$ is the Bell singlet state (3.3).

For special choice of λ and α (for example $\lambda = 0.9$ and $\alpha\beta = 0.2$), the initial state ρ is local, while the final state ρ' is nonlocal. This result makes the identification of the term "local" with "not violating any Bell inequality" seem flawed, since nonlocality should not be creatable by local actions on any local state. However, there are a few open questions in this field which might lead to a different way to resolve this problem. Firstly, it is unknown whether local states containing such "hidden nonlocality" can be described by LHV models. Secondly, filtering and renormalising a state implies post-selection (i.e. discarding or keeping systems from an ensemble according to the result of certain measurements), which can generally be used to enforce correlations (as in entanglement distillation). This means that one should not consider a single state conversion $\rho \to \rho'$, but a conversion of ensembles $\rho^{\otimes n} \to \rho'^{\otimes m}$ with $m \leq n$. Since ρ being local does not involve $\rho^{\otimes n}$ being local[56], the question should be asked whether there is a case in which $\rho^{\otimes n}$ is local and $\rho'^{\otimes m}$ is nonlocal (for appropriate n and m). This however, turns out to be difficult, due to lack of trustworthy ways to determine if a high-dimensional state is local or nonlocal.

Bell Inequalities and Distillation

A priori, Bell inequalities do not show any special behaviour concerning distillable or undistillable states. It was conjectured, that any nonlocal quantum state should be distillable, this however turned out to be untrue, since there are examples where bound entangled states can violate certain Bell inequalities – even maximally[20]. Although this might be surprising at first, it is not too disturbing, since the used Bell inequality is not optimal for the used system (in the sense mentioned above) and also because even for optimal

setups, mixed states are known to yield maximal violations due to the degeneracy of the corresponding Bell operator[52].

There are, however, certain Bell inequalities that can only be violated by distillable states[48]. Also, often the Bell-witnesses are decomposable into completely positive and completely co-positive maps as in eq. (4.13), such that they can only detect NPT states.

Bell Inequalities as a Measure for Entanglement

After all this discussion, it can be said that the magnitude of violation of Bell inequalities does not seem to pose a good measure for entanglement, for a number of reasons:

- There are entangled states that do not violate any Bell inequality and that even admit LHV models[43], some of which are even useful for teleportation[57], such that only a weaker form of the first desired property is fulfilled, namely: ρ is separable $\Rightarrow E(\rho) = 0$, while the converse statement does not hold.

- The maximal violation can occur for nonmaximally entangled states, also there are mixed states that can reach this maximum. Hence this measure completely fails to identify maximally entangled states.

- Bell inequalities are not non-increasing under LOCC.

- Since no state can ever exceed the maximal value for any Bell inequality, the associated measure cannot be additive.

- For systems of higher dimension than qubits, the maximal violation of a Bell inequality for any given state is very hard to compute, since this task is a matter of multi-nonlinear numerical optimisation.

5.3 Geometric Measures

A whole class of geometrically highly intuitive measures for entanglement can be formulated via geometric distances[58]. These are a quantitative generalisation of entanglement witnesses in the sense that they are based on the convexity of the set of separable states, from which follows that there is exactly one closest separable state to each entangled state (in any metric, on which this state may depend). The idea is that this nearest separable state should reproduce the classical portion of the correlations contained in an entangled state, so that any remaining difference between the two states

is solely due to quantum entanglement.

This measure is simply defined by

$$E(\rho) = \min_{\sigma \in S} D(\rho, \sigma) \tag{5.16}$$

where $D(\rho, \sigma)$ is any measure of distance between the two density matrices ρ and σ and the minimum is taken over all separable states σ. Note that $D(\rho, \sigma)$ does not necessarily have to be a real metric (as will be seen in 5.3.2). Obviously, whether this represents a good measure for entanglement depends strongly on the choice of $D(\rho, \sigma)$. It was shown[59] that such a measure is invariant under unitary transformations, nonincreasing under LOCC and yields its minimal value of $E = 0$ for separable states and for separable states only, if the used distance measure satisfies the following criteria:

1. $D(\rho, \sigma) \geq 0$, where equality holds iff $\rho = \sigma$

2. $D(\rho, \sigma) = D(U\rho U^\dagger, U\sigma U^\dagger)$ for any unitary operation U

3. $D(\mathrm{Tr}_X \rho, \mathrm{Tr}_X \sigma) \leq D(\rho, \sigma)$ where Tr_X is a partial trace

4. $\sum_i p_i D(\rho_i/p_i, \sigma_i/q_i) \leq \sum_i D(\rho_i, \sigma_i)$ where $\rho_i = V_i \rho V_i^\dagger$, $\sigma_i = V_i \sigma V_i^\dagger$, the $\{V_i\}$ represent a POVM (i.e. are positive operators satisfying $\sum_i V_i V_i^\dagger = \mathbb{1}$) and $p_i = \mathrm{Tr}(\rho_i)$ and $q_i = \mathrm{Tr}(\sigma_i)$

5. $D(\sum_i P_i \rho P_i, \sum_i P_i \sigma P_i) = \sum_i D(P_i \rho P_i, P_i \sigma P_i)$ where the $\{P_i\}$ are any set of orthogonal projectors

6. $D(\rho \otimes P, \sigma \otimes P) = D(\rho, \sigma)$ for any projector P.

Obviously, condition (1) ensures $E(\rho) = 0$ iff ρ is separable and condition (2) ensures unitary invariance. Less trivially, conditions (2)-(6) are sufficient for the measure to be nonincreasing under LOCC.

5.3.1 Hilbert-Schmidt-Distance

The probably most obvious choice for $D(\rho, \sigma)$ is the standard Hilbert-Schmidt metric

$$D(\rho, \sigma) = \|\rho - \sigma\| = \sqrt{\mathrm{Tr}(\rho - \sigma)^2} \tag{5.17}$$

Although the conditions (3) - (6) have not been proven (or falsified) for this metric[59], it shows some remarkable features and is therefore one of the commonly used distance measures in entanglement quantification.

The Bertlmann-Narnhofer-Thirring theorem

The analogy between geometric entanglement measures and entanglement witnesses is most significant in the Hilbert-Schmidt metric. Restricting the set of entanglement witnesses to normalised operators, i.e. operators satisfying $\|A - \alpha \mathbb{1}\|_2 = 1$ (where $\alpha = \text{Tr}(A)/d$), the maximal value of the witness-inequality (4.26) for a given state

$$B(\rho) = \max_A \left[\min_{\sigma \in S} \langle \sigma | A \rangle - \langle \rho | A \rangle \right] \tag{5.18}$$

(where the maximum is taken over all normalised entanglement witnesses A and the minimum is taken over all separable states σ) equals the Hilbert-Schmidt distance $E_{HS}(\rho)$ of this state to the set of separable states[34]:

$$B(\rho) = E_{HS}(\rho) \quad \forall \rho \tag{5.19}$$

This is known as the Bertlmann-Narnhofer-Thirring theorem.

Since $B(\rho)$ is defined as a maximum and $E_{HS}(\rho)$ is defined as a minimum, upper and lower bounds are very easily obtained:

$$\min_{\sigma \in S} \left\langle \sigma - \rho | \frac{\omega - \rho}{\|\omega - \rho\|} \right\rangle \leq B(\rho) = E_{HS}(\rho) \leq \|\omega - \rho\| \quad \forall \omega \tag{5.20}$$

where the lower bound is attained for a geometric entanglement witness in which the minimum is taken over all separable states σ.

Finding the nearest separable state

Similar to other distance measures, the nearest separable state to any given entangled state is in general rather difficult to find in the Hilbert-Schmidt metric. However, there is a way to check if a "guessed" state happens to be the nearest separable state[60].

Namely, a separable state $\tilde{\sigma}$ is the closest separable state to a given entangled state ρ, iff the operator

$$C = \frac{\tilde{\sigma} - \rho - \langle \tilde{\sigma} | \tilde{\sigma} - \rho \rangle \mathbb{1}}{\|\tilde{\sigma} - \rho\|} \tag{5.21}$$

is an entanglement witness.

This follows from the construction of C, which is an (optimal) geometric entanglement witness if and only if $\tilde{\sigma}$ really is the nearest separable state to ρ, since otherwise the hyperplane spanned by C would intersect the set of separable states and hence C would not be an entanglement witness.

Even in cases with more complex or nonintuitive geometry, such that the nearest separable state can not be guessed, there is a very operational method for finding the closest PPT state (which in many cases is also the closest separable state, and else gives a good lower bound on the distance) by means of Lagrangean methods[61].

1. First, one has to find the eigenvalue decomposition of the partially transposed density matrix of the entangled state ρ

$$\rho^{T_A} = UDU^\dagger \tag{5.22}$$

   where D is a diagonal matrix and U is a unitary transformation.

2. One then defines the unique positive semidefinite normalised diagonal matrix E with diagonal entries

$$e_i = \max(d_i + \lambda, 0) \tag{5.23}$$

   where d_i are the elements of D and the value of λ is defined by the normalisation $\mathrm{Tr}\, E = 1$.

3. The nearest PPT-state to ρ is obtained as

$$\tilde{\sigma} = (UEU^\dagger)^{T_A} \tag{5.24}$$

Now, if $\tilde{\sigma}$ is in fact a state (i.e. $\tilde{\sigma} \geq 0$), then it is indeed the nearest PPT state to ρ. However, there are special cases in which the outcome yielded by this procedure does not happen to be positive. Even in these cases $\|\tilde{\sigma} - \rho\|$ is a useful lower bound on the actual distance.

5.3.2 Quantum Relative Entropy

The quantum relative entropy of two states (also called (relative) entropy of entanglement, when used as an entanglement measure) is a measure for the overlap of two density matrices (in the sense of statistical distinguishability[62]) defined by

$$D(\rho, \sigma) = \mathrm{Tr}(\rho \log \rho - \rho \log \sigma) \tag{5.25}$$

Obviously, the quantum relative entropy is not a metric (as it does not satisfy the triangle inequality and is not symmetric in ρ and σ), however, the

entropy of entanglement E_{RE} is a remarkable measure for entanglement, as it is closely related to the entanglement of formation E_F and the entanglement of distillation E_D[63], as will be discussed in section 5.4. Also, for pure states E_{RE} reduces to the von Neumann entropy of the subsystems, i.e. the entanglement measure for pure states (5.1)[59].

Explicit analytical computation of the quantum relative entropy is only possible in special highly symmetric cases[64], in which examples can be found that prove the measure to be nonadditive.

5.3.3 Bures-Distance

The last distance measure that shall be discussed here is the Bures-metric[59]

$$D(\rho, \sigma) = 2 - 2\sqrt{F(\rho, \sigma)} \qquad (5.26)$$

$$F(\rho, \sigma) = \left[\mathrm{Tr}(\sqrt{\sigma}\rho\sqrt{\sigma})^{\frac{1}{2}} \right]^2$$

Like the quantum relative entropy, the Bures-metric satisfies all of the conditions discussed for geometric entanglement measures. It is closely related to the question of experimentally distinguishing one state from another, as in the field of unambiguous state discrimination[65].

The Bures-distance can also be seen in context with LOCC, as F can also be written as[66]

$$F(\rho, \sigma) = \min_{\{A_i\}} \sum_i \sqrt{\mathrm{Tr}(A_i \rho A_i^\dagger)} \sqrt{\mathrm{Tr}(A_i \sigma A_i^\dagger)} \qquad (5.27)$$

where the minimum is taken over all sets of positive operators $\{A_i\}$ satisfying $\sum A_i^\dagger A_i = \mathbb{1}$, i.e. POVMs.

5.4 Entanglement of Formation and Entanglement of Distillation

Historically, the entanglement of formation E_F and the entanglement of distillation E_D were the first attempts to quantify quantum entanglement. Until today, they are the only measures for entanglement with a direct physical interpretation, making them incomparably important and meaningful measures and give them a unique perspective.

Entanglement of Distillation

The entanglement of distillation of a state ρ is defined as the maximal asymptotic (in the limit of high numbers of particles) yield of distilled maximally entangled states per copy of the input state ρ, i.e.[67].

$$E_D = \max \ \lim_{n \to \infty} \frac{m(n)}{n} \qquad (5.28)$$

where n is the number of input states ρ, m is the number of maximally entangled output states and the maximum is taken over all possible distillation protocols.

By definition, this measure obviously is normalised to $0 \leq E_D \leq 1$ and the upper bound is reached iff ρ is maximally entangled. Furthermore, the entanglement of distillation satisfies $E_D = 0$ for all separable states, but not for separable states only, since bound entangled states cannot be distilled and hence have $E_D = 0$ without being separable.

Since very little is known about distillation protocols apart from the few explicit examples that have been established, the entanglement of distillation is hardly computable. However, since it is defined as a maximum, lower bounds can easily be obtained by applying any particular protocol. Also, the entanglement of formation E_F (which will be discussed subsequently) always gives an upper bound on the entanglement of distillation.

Since there are distillation protocols that use only one-way communication, these define another form of entanglement of distillation E_{D_1}, which obviously cannot exceed the general entanglement of distillation, but is proven to be lower for certain states (there even are examples of states for which $E_{D_1} = 0 < E_D$), such that

$$E_{D_1} \leq E_D \leq E_F \qquad (5.29)$$

Also, when dealing with more complicated situations (e.g. more than two parties), the one-way entanglement of distillation can be nonsymmetric, i.e. can depend on the direction of the allowed communication: $E_{D_1}^{A \to B} \neq E_{D_1}^{B \to A}$. Due to phenomenae like the bound entanglement activation effect (as discussed in (3.3)) and the probable existence of NPT bound entanglement, the entanglement of distillation seems to be nonadditive[68].

Entanglement of Formation

The entanglement of formation of a state ρ is defined as the optimal asymptotic (in the limit of high particle numbers) conversion yield of the number

of maximally entangled input states needed per output state ρ[67]. In other words, it is the answer to the question: How many maximally entangled states are necessary, to form one copy of a mixed-entangled state ρ, i.e.

$$E_F = \min \lim_{m \to \infty} \frac{m}{n(m)} \qquad (5.30)$$

where m is the number of maximally entangled input states, n is the number of output states ρ and the minimum is taken over all means of preparing ρ from maximally entangled states.

Since the preparation entanglement cost for a pure state is given by the von Neumann entropy of one of its reduced density matrices (i.e. the entanglement measure for pure states (5.1)), it seems reasonable that the appropriate convex roof equals the entanglement of formation for a mixed state. Although on second thought it seems possible that there are more efficient ways of preparing an entangled state than to prepare each pure state in any optimal decomposition and mixing them, this was proven not to be the case[69], such that

$$E_F = \min_{\{p_i, |\Psi_i\rangle\}} \sum_i p_i S(\rho_i) \qquad (5.31)$$

where the minimum is taken over all decompositions $\{p_i, |\Psi_i\rangle\}$ satisfying $\rho = \sum_i p_i |\Psi_i\rangle \langle \Psi_i|$ and the ρ_i are the reduced density matrices of the states $|\Psi_i\rangle$.

The entanglement of formation satisfies all of the desired conditions discussed above, except additivity, which has not been proven as of yet.

While it may seem surprising at first, that the entanglement of distillation does in general not equal the entanglement of formation (while they are both measures for the entanglement contained in a quantum state), it becomes obvious when considering special cases, such as bound entanglement, which by definition has $E_D = 0 < E_F$.

Unfortunately, the entanglement of formation is in general not easily computable (although unlike the entanglement of distillation, it can be computed numerically from eq. (5.31) in principle), but there are special cases in which a closed form can be given via the so called concurrence.

Concurrence

The entanglement of formation can be computed analytically in several special cases via a quantity called the concurrence C: $E_F = E_F(C)$, where E_F ranges from 0 to 1 for C going through the values from 0 to 1 as well, making the concurrence a suitable measure for entanglement itself[70].

In this way, E_F can be computed for example for all states of two qubit systems:

$$E_F = h\left(\frac{1 + \sqrt{1 - C^2}}{2}\right) \tag{5.32}$$

where $h(x)$ is the binary entropy function

$$h(x) = -x \log x - (1 - x) \log(1 - x) \tag{5.33}$$

and the concurrence C is given by

$$C = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4) \tag{5.34}$$

with λ_i being the eigenvalues of the matrix

$$R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$$

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\, \rho * (\sigma_y \otimes \sigma_y) \tag{5.35}$$

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

in decreasing order and the asterisk denoting complex conjugation.
This concurrence can be generalised to higher dimensions[71]

$$C = \min_{\{p_i, |\Psi_i\rangle\}} \sum_i p_i \max_{\{U_i, V_i\}} \left| \langle \Psi_i | (U_i \otimes V_i)^T S (U_i \otimes V_i) | \Psi_i \rangle \right| \tag{5.36}$$

where the minimum is taken over all ensembles $\{p_i, |\Psi_i\rangle\}$ realising ρ and the maximum is taken over all $U_i \in SU(d_1)$ and $V_i \in SU(d_2)$, with $d_{1,2}$ being the dimensions of the two subsystems, and where

$$S = (\sigma_y \oplus 0_{d_1-2}) \otimes (\sigma_y \oplus 0_{d_2-2}) \tag{5.37}$$

is a generalised version of the spin-flip operator $\sigma_y \otimes \sigma_y$ from the $2 \otimes 2$-dimensional case. This generalisation however seems rather worthless, as it is exactly as difficult to compute as the entanglement of formation (5.31) itself.
There are several classes of states for which a closed form of C (or E_F itself) has been found (for example the isotropic state in arbitrary dimensions[72]), as well as multiple bounds (e.g. [73]) and methods to simplify the variational problem (5.31), reducing it for example to a variational problem over finite-sized matrices[71]. For general states however, there still exists no closed form of computation for the entanglement of formation.

Due to their direct physical interpretation, the entanglement of formation and the entanglement of distillation pose new restrictions on other entanglement measures. It is more than reasonable to demand

$$E_D \leq E \leq E_F \tag{5.38}$$

for any entanglement measure E, as a state cannot contain more entanglement than is needed to create it and can neither contain less entanglement than can be distilled from it. In the light of this it seems appropriate not to require entanglement measures to satisfy conditions that "seem" resonable (especially since quantum mechanics has proven to behave contra-intuitively on several other occasions), but to relate the demands to objectively good entanglement measures, which E_D and E_F are, regardless of which of the discussed conditions are satisfied.

For pure states, both equalities in (5.38) hold[63], such that the entanglement measure for pure states is uniquely given as discussed in 5.1. For mixed states however, the problem is more difficult. It seems, that a single quantity does not suffice to describe the entanglement contained in a quantum state (this is already suggested by the entanglement of formation not being equal to the entanglement of distillation).

An entanglement measure E was proven to satisfy (5.38), if it is additive, convex and reduces to the von Neumann entropy of the reduced density matrices for pure states[68]. The only entanglement measure known to satisfy condition (5.38) apart from E_F and E_D themselves, is the entropy of entanglement, i.e. the geometric entanglement measure induced by the quantum relative entropy (as discussed in 5.3.2).

5.5 Schmidt Numbers

The concept of Schmidt ranks for pure states can be generalised to mixed states[6]. The Schmidt number of a given density matrix ρ is defined as the maximal Schmidt rank, that is at least necessary to construct it, i.e. the number $k(\rho)$ such that

- There is no decomposition of ρ into pure states which all have Schmidt rank less than $k(\rho)$

- There is a decomposition of ρ into pure states which all have a Schmidt rank of at most $k(\rho)$

The Schmidt number of a state determines how many degrees of freedom are entangled within this state. Evidently, the lower bound $k(\rho) = 1$ is equivalent to ρ being separable, while the upper bound $k(\rho) = d_{min} = \min(d_1, d_1)$ indicates all present degrees of freedom being entangled.

For formal reasons, one might define $E = k(\rho) - 1$ as an entanglement measure, such that $E = 0$ iff ρ is separable. The Schmidt number of a state is nonincreasing under LOCC, convex (in the sense that $\lambda k(\rho_1) + (1-\lambda)k(\rho_2) \leq k(\lambda \rho_1 + (1-\lambda)\rho_2)$) and unitary invariant, it is however not additive.

From the first of these properties follow strong limits on interconvertibility of states. If for example $k(\rho^{\otimes n}) < k(\omega^{\otimes n})$ for a certain number n, this means that ρ cannot be converted to ω on a 1-to-1 basis, even if $k(\rho) = k(\omega)$. The behaviour of Schmidt numbers for high numbers of copies of a state can be very different, depending on the state – in some cases, they grow to very large numbers, while in others they do not grow at all, such that $k(\rho) = k(\rho^{\otimes n})$.

5.6 Robustness of Entanglement

The robustness of entanglement[74] R originated from the already discussed idea of describing mixed state entanglement not with a single measure, but with several parameters, in which context the robustness seems to be useful. It is a measure for how much a given quantum state ρ has to be mixed with a separable state σ, so that the resulting state is separable and thus all entanglement is "erased":

$$R\left(\rho||\sigma\right) = \min s \tag{5.39}$$

where the minimum is taken over s such that

$$\omega\left(s\right) = \frac{1}{1+s}\left(\rho + s\sigma\right) \in S \tag{5.40}$$

There are two different choices of σ that induce useful measures for entanglement. Firstly, the absolute robustness, where $R\left(\rho||\sigma\right)$ is minimised over all separable states σ:

$$R(\rho) = \min_{\sigma \in S} R\left(\rho||\sigma\right) \tag{5.41}$$

and secondly, the random robustness, where $\sigma = 1/d\,\mathbb{1}$ is the maximally mixed state.

Note that both these measures are well defined (since a neighborhood of the maximally mixed state is always separable and the geometry shown in Fig. 5 can always be achieved). Furthermore, both measures vanish iff ρ is separable.
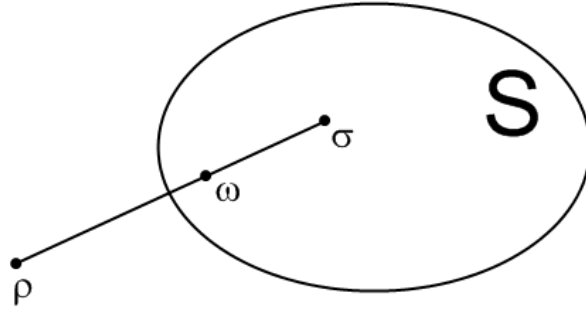
Fig. 5: Visualisation of $R(\rho||\sigma)$ (eq. (5.39)). The minimum is achieved when $\omega \in \partial S$. Note that the robustness measure is independant of any choice of metric.

The absolute robustness was shown to satisfy most of the discussed conditions, although it only is additive in the very weak sense that

$$R(\rho \otimes \sigma) = R(\rho) \; \forall \; \sigma \; \in \; S \tag{5.42}$$

The computation of $R(\rho)$ is simplified significantly by the fact, that $R(\rho||\sigma)$ is a convex function of σ, meaning that any local minimum is also a global minimum, such that the optimisation over σ can be done (numerically) in most cases. Hence, both the absolute and the random robustness of entanglement can be computed, given a means to faithfully detect entanglement in the given system. In several cases, they can even be calculated analytically. Surprisingly, the absolute robustness of entanglement turns out to be a quantification of the cross-norm criterion, as it can be written as[30]

$$R(\rho) = \|\rho\|_\gamma - 1 \tag{5.43}$$

Also, several bounds on the robustness are known[74].

5.7 Fidelity

The mathematically most simple and straightforward measure for entanglement might be the fidelity. It is defined as the conversion probability from a given state ρ to the set of maximally entangled states (which can be chosen to be real)

$$F = \max_{|\Psi\rangle} \langle\Psi| \rho |\Psi\rangle \tag{5.44}$$

where the maximum is taken over all maximally entangled states $|\Psi\rangle$. Although it is very useful to characterise quantum states (for example as a

49

parameter for a family of states, such as in the already discussed Werner state (3.5)), it is of rather little use in entanglement quantification, since is not nonincreasing under LOCC and is also nonzero for separable states. Thus, it cannot even be used to detect entanglement (except in special cases of families of states that are known to be separable/entangled for certain fidelities).

5.8   Negativity

Another direct quantification of an entanglement detection procedure is the so called negativity N. It is a simple quantification of the nonpositivity of the partially transposed density matrix of a state[75]

$$N = \frac{\left\| \rho^{T_A} \right\|_1 - 1}{2} \tag{5.45}$$

such that $N = 0$ for all PPT states and $N = 1$ for maximally entangled states.

This measure seems very useful, as it is very easily computable. Nevertheless, it vanishes for many entangled states and is only applicable for bipartite systems and thus in general is not a good measure.

	ρ separable $\Leftrightarrow E(\rho)=0$	ρ maximally entangled $\Leftrightarrow E(\rho)$ maximal	Nonincreasing under LOCC	Unitary invariant	Continuous	Convex	Additive
Pure States	✓	✓	✓	✓	✓	✓	✓
Bell Inequalities	∼[1]	✗	✗	✓	✓	✓	✗
Hilbert-Schmidt Distance	✓	?	?	✓	✓	✓	?
Quantum Relative Entropy	✓	?	✓	✓	✓	✓	✗
Bures Distance	✓	?	✓	✓	✓	✓	?
Entanglement of Distillation	∼[1]	✓	✓	✓	?	?	?
Entanglement of Formation	✓	✓	✓	✓	✓	✓	?
Schmidt Numbers	✓	✓	✓	✓	✗	✓	✗
Robustness of Entanglement	✓	✓	✓	✓	✓	✓	∼[2]
Fidelity	✗	✓	✗	✓	✓	✓	✗
Negativity	∼[1]	✓	✓	✓	✓	✓	✗[3]

Fig. 6: In the light of results on various entanglement measures, espcially on the entanglement of formation and the entanglement of distillation, it seems as if the discussed properties of entanglement measures are not as fundamental as they were considered to be at first. Nevertheless, they offer a good overview of the usefulness of the discussed measures. A green checkmark stands for the property being satisfied by the entanglement measure, while a red 'x' represents the measure failing to do so. Question marks indicate properties that have not been proven one way or the other. Waves symbolise a property that is only satisfied in a weaker form.

[1] : ρ is separable $\Rightarrow E(\rho) = 0$, but not vice versa.

[2] : Only a weak form of additivity is satisfied, as discussed in 5.6.

[3] : Since the negativity is only defined for bipartite systems, this property makes no sense.

6 Hilbert Space Geometry and Examples

One of the ultimate goals in quantum information theory is to completely characterise and fully understand the geometry of multipartite Hilbert spaces and the properties of quantum states therein.

6.1 Unipartite Systems

Unipartite Hilbert spaces can be visualised by the concept of Bloch vectors[5]. A $d \otimes d$-dimensional density matrix ρ can always decomposed in the form

$$\rho = \frac{1}{d}\mathbb{1} + \vec{b}\vec{\Gamma} \tag{6.1}$$

where $\vec{\Gamma}$ is a list of $(d^2 - 1)$ mutually orthogonal traceless matrices, which – together with the identity matrix – form a basis of the Hilbert-Schmidt space and $\vec{b}$ is a list of $(d^2 - 1)$ coefficients, the so called Bloch vector, such that $\vec{b}\vec{\Gamma}$ is a linear combination of all the basis matrices. Obviously, the state space of $d \otimes d$-dimensional density matrices has $d^2 - 1$ dimensions, since the coefficient of the identity matrix is given by $\text{Tr}\rho = 1$. Note that this map is not bijective, as for any choice of basis $\vec{\Gamma}$ any given density matrix ρ corresponds to a certain Bloch vector $\vec{b}$, but not every given $\vec{b}$ results in a density matrix, as the decomposition (6.1) does not necessarily provide positivity.

For a single qubit, i.e. a 2×2-dimensional density matrix, the state space is very simple. The commonly used matrix basis consists of the three Pauli matrices (2.17) and the decomposition (6.1) assumes the form

$$\rho = \frac{1}{4}\left(\mathbb{1} + \vec{a}\vec{\sigma}\right) \tag{6.2}$$

with $|\vec{a}| \leq 1$, where equality holds iff ρ is a pure state and $|\vec{a}|$ gets smaller the more mixed ρ is.

Already for 3×3-dimensional density matrices, i.e. states of a single qutrit, the Bloch sphere becomes more complicated and the choice of basis less obvious. The most commonly used basis matrices are the Gell-Mann matrices (2.18) and the Weyl operators (2.22), which each result in a certain allowed interval for $|\vec{b}|$ where all density matrices are found. However, unlike in the qubit case, there are Bloch vectors that do not correspond to states. Thus, the state space for a single qutrit is already rather complicated.

6.2 Bipartite Systems

Since the lowest-dimesional bipartite system (the system of two qubits, which is $(2 \times 2)^2 - 1 = 15$ dimensional) has already significantly more dimensions than a system of one qutrit ($3^2 - 1 = 8$ dimensions), which has already been found to be rather nontrivial, bipartite systems are generally more difficult to analyse. Furthermore, in bipartite systems the concept of entanglement

starts to play an important role, such that there are more properties of states that need to be taken into account and implemented into the picture.

In most cases, it is very difficult to understand the underlying geometry by studying mathematical properties. This is why often only 2- or 3-dimensional simplices (i.e. subspaces) are studied, since these can be visualised and help to gain an intuitive and geometrical understanding.

6.2.1 Classification of States

In the earlier sections of this work, a basic understanding of the different types of bipartite quantum states has been established. These types of quantum states shall now be reviewed and discussed in further detail.

There are four basic criteria (which are relevant in the context of quantum information theory) by which bipartite states can be categorised. Firstly, they can be either separable or entangled. Secondly, they can be either distillable (free entangled) or undistillable (separable or bound entangled). Thirdly, they can be either local or nonlocal (i.e. satisfy all Bell inequalities or violate some of them). Finally, they can be either PPT or NPT (i.e. remain positive under partial transposition or not).

While in each of these four distinctions a given quantum state has exactly one of the possible properties (e.g. it is either PPT or NPT, but not both and not neither), most combinations of these properties with properties from other categories are possible (such as 'PPT and entangled' or 'distillable and local'), as visualised in Fig. 7.

Separable and entangled states

The most important distinction in this context is the one between separable and entangled states. As was already thoroughly discussed throughout this work, this distinction is highly nontrivial, as the definition of separable states

$$\rho = \sum_i p_i \left| \Psi_i^A \right\rangle \left\langle \Psi_i^A \right| \otimes \left| \Psi_i^B \right\rangle \left\langle \Psi_i^B \right| \tag{6.3}$$

(where the $\{p_i\}$ are probabilities) is in general very difficult to check and there exists no closed definition for entangled states apart from not being separable.

Still, some properties of the set of separable states S and the set of entangled states S^C are known[34]:

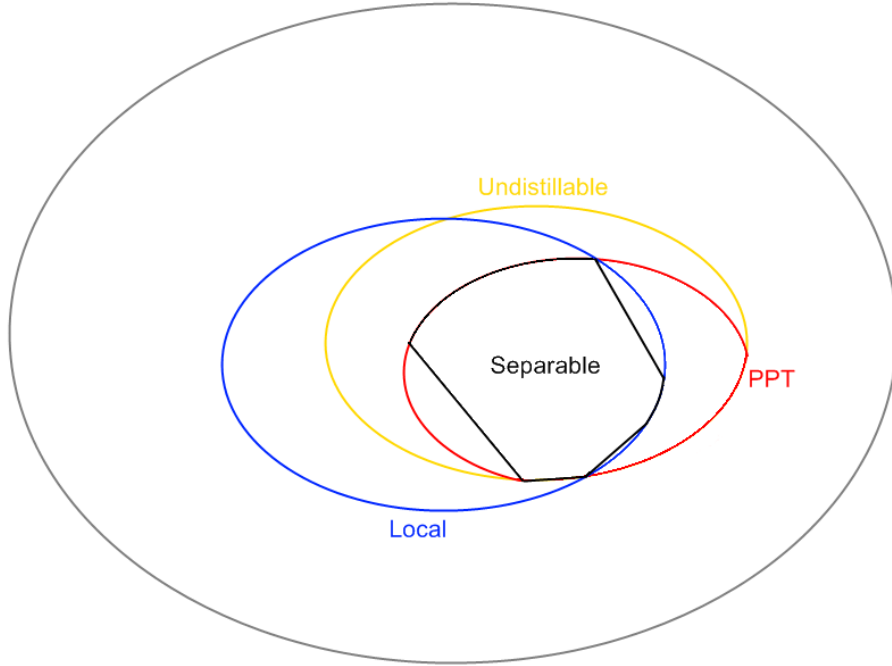- S is a convex set (consequently, S^C is not).

Fig. 7: Schematic picture of the different classes of states

- $\dim S = \dim S^C = D^2 - 1$, where $D = d_1\, d_2$ is the dimension of the composite system. This means that both S and S^C are thick everywhere on $\mathcal{H}$ and not sets of measure zero.

- All separable density matrices with rank one or two (i.e. pure states and mixtures of no more than two pure states) are located on the border of S, while density matrices of higher rank (i.e. mixtures of more than two pure states) form the interior of S, but can also be found on the border.

- Whereever there is a mixed state of n pure states on the border of S, there is an at least n-dimensional face of S. If the dimensions of the two subsystems are equal $(d_1 = d_2 = d)$, then there exist at least d^2-dimensional faces.

- S is invariant under transformations of the form $\Lambda^A \otimes \Lambda^B$, where Λ^i are positive maps (as discussed in 4.3).

Distillable and undistillable states

Since very little is known about distillation and distillation protocols, it is as of yet not possible to completely define the set of distillable states or the set of undistillable states for general systems. Nevertheless, in big parts of the state space the question can be answered, for example by means of the reduction criterion or the PPT-criterion (since violation of the reduction criterion implies distillability, while satisfaction of the PPT-criterion implies undistillability, as discussed in 4.3). Pure entangled states however are always distillable.

Since very little is known about the geometry of bound entanglement, it is still unknown if the set of undistillable states is convex.

Local and nonlocal states

Like distillability, nonlocality of a state (in the sense of violating Bell inequalities) is in general not completely characterised, as Bell inequalities for higher dimensions than $2 \otimes 2$ are merely beginning to be understood. While the $2 \otimes 2$ case is solved (as discussed in 5.2), for higher dimensions there are even less possibilities to answer this question for a given state as there are for distillability. Apart from all separable states being local and pure entangled states being nonlocal, there is no way to tell if a state is local, while nonlocality can only be proven by explicitly finding a Bell inequality that is violated by this state.

Since Bell inequalities are linear functions of states (since they can be written as expectation values of Bell operators), a convex sum of local states remains local. The set of local states is therefore a convex one.

PPT and NPT states

The question of positivity under partial transposition of a state lacks a direct physical meaning, nevertheless it is a very powerful tool, since it is very easily computable for all kinds of multipartite quantum states and offers a great deal of information on separability and distillability of a state. If a state is separable, it has to be PPT and a PPT state hast to be undistillable. Conversely, a distillable state has to be NPT and an NPT state has to be entangled.

Low dimensional cases

In certain lower dimensions, the geometry of the state space is much more simple and some of the four criteria become equivalent.

In $2 \otimes d_2$ dimensions (with d_2 being an arbitrary integer), nonpositivity under partial transposition is necessary and sufficient for distillability, i.e. the set of NPT states is the same as the set of distillable states (there is no NPT bound entanglement)[15].

In $2 \otimes 2$ and $2 \otimes 3$ dimensions, positivity under partial transposition is necessary and sufficient for separability[22], such that there is no PPT bound entanglement either. Consequently, in these cases there is no bound entanglement at all, PPT (NPT) is equivalent to separability (entanglement) and undistillability (distillability)[76]. Therefore, for these systems there are only two distinct criteria left (separability and locality) and the geometry is considerably simplified (see Fig. 8).
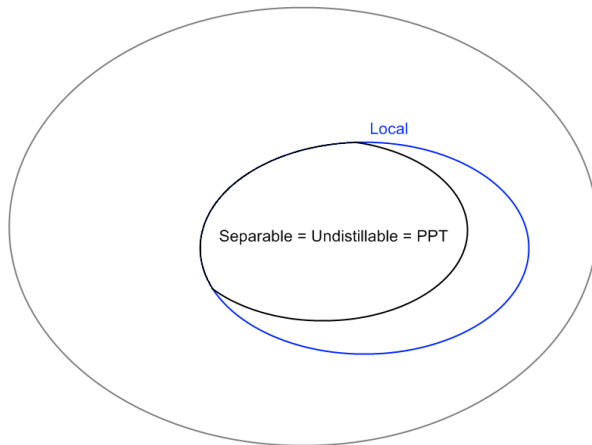
Fig. 8: Schematic picture of the state space in $2 \otimes 2$ and $2 \otimes 3$ dimensions

Schmidt classes

Apart from the classification above, density matrices can also be characterised in terms of their Schmidt numbers (as discussed in 5.5). The Schmidt class S_k is defined as the set of all states, whose Schmidt number does not exceed k, i.e. all states ρ satisfying $k(\rho) \leq k$.

Due to the convexity of Schmidt numbers, each Schmidt class forms a convex subset of the set of all states, such that

$$S_1 \subset S_2 \subset ... \subset S_{d_{min}} \qquad (6.4)$$

56

$S_1 = S$ is the set of separable states and $S_{d_{min}}$ is the complete set of states, apart from this however, there are hardly any known links between Schmidt classes and the other sets of states discussed above. Evidence has been found[77] that (at least in special cases) bound entangled states do not seem to have maximal Schmidt number, but further study in this area is needed. Due to their convexity, Schmidt classes can be described by appropriate witness operators – so called Schmidt witnesses[78], that separate a certain S_n from all states $\rho \notin S_n$.

6.2.2 Systems of two QuBits

Systems of two qubits and systems of one qubit and one qutrit are the only completely solved ones. Since systems consisting of equal subsystems are much more practical in use, the $2 \otimes 2$ case is of much more interest than the $2 \otimes 3$ one.

Since the PPT criterion is necessary and sufficient for separability in this case, it is very simple to find out if any given state is separable (and thus undistillable) or entangled (and distillable, as there is no bound entanglement in this case). The question of locality or nonlocality can be easily answered by means of the criterion (5.7).

Bloch decomposition for two qubits

As was already mentioned in eq. (5.6), any density matrix of a two qubit system can be written as

$$\rho = \frac{1}{4}(\mathbb{1} + \vec{a}\vec{\sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \vec{b}\vec{\sigma} + \sum_{m,n=1}^{3} t_{mn}\sigma_m \otimes \sigma_n) \qquad (6.5)$$

Since a single qubit state corresponds to a Bloch vector, i.e. a point of a three dimensional sphere, any product state of two qubits corresponds to two distinct Bloch vectors, i.e. $t_{mn} = a_m b_n$, spanning a 6-dimensional subspace of the 15-dimensional state space (hence, all product states of two qubits can be considered as points on a 6-dimensional sphere). As soon as the two qubits are correlated – either classically or via entanglement –, this picture does not hold anymore.

The magic simplex

Since the whole 15-dimensional state space can hardly be visualised, often lower dimensional simplices are studied. A region of special interest is the so called magic simplex, which is the subspace spanned by four mutually orthogonal maximally entangled states (which can without loss of generality be chosen to be the four Bell states (3.3)). Consequently, all of these states have maximally mixed subsystems, hence the local components $\vec{a}$ and $\vec{b}$ in the Bloch vector representation (6.5) equal zero. Since the matrix t_{mn} can be diagonalised, all these states are of the form

$$\rho = \frac{1}{4}\left(\mathbb{1} + \sum_{i=1}^{3} c_i \sigma_i \otimes \sigma_i\right) \tag{6.6}$$

where c_i are the elements of the diagonalised matrix t_{mn}. More explicitly, these states can also be written as

$$\rho = a_1 \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + a_2 \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + a_3 \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + (1-a_1-a_2-a_3)\left|\Phi^-\right\rangle\left\langle\Phi^-\right| \tag{6.7}$$

with $a_i \geq 0$ and $\sum a_i = 1$.

Since the four Bell states form the vertices of the magic simplex and are mutually equally distant from each other (in the Hilbert-Schmidt metric), the magic simplex has the shape of a tetrahedron[34]. The set of all matrices that satisfy the PPT-criterion form another tetrahedron, which however does not fully consist of states (as there are matrices that are not positive semidefinite, but become so after partial transposition). The intersection of these two tetrahedra forms the set of all separable states, which has the shape of an octahedron.

Thus, the magic simplex is a tetrahedron enclosing an octahedron, where the vertices of the tetrahedron are the maximally entangled states (which are the only pure states in the simplex) and the octahedron is formed by all separable states. The maximally mixed state is located in the middle of the octahedron (see Fig. 9).

6.2.3 Systems of two QuTrits

Despite much effort that has been put into the understanding of the geometry of two qutrit systems, there is still rather little known about it. The existence of PPT bound entangled states (which are hard to discriminate from separable states) as well as the assumed existence of NPT bound entanglement (which is very hard to distinguish from free entangled states) and the nonexistence of analytical means to detect nonlocality pose considerable
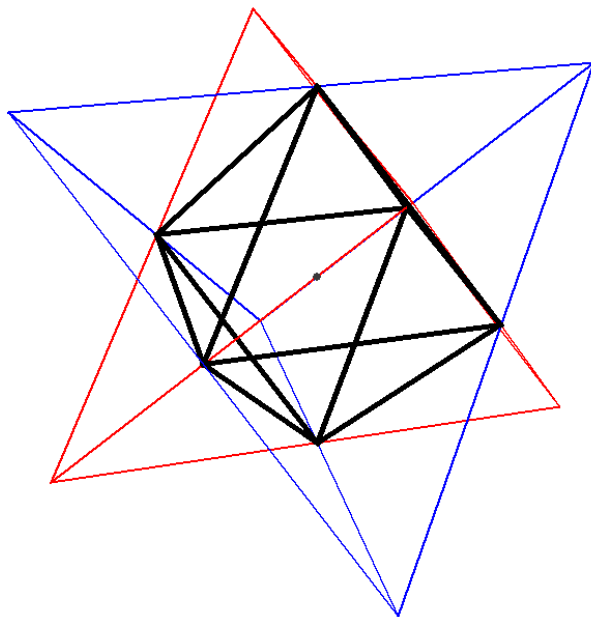
Fig. 9: Visualisation of the maxic simplex in a system of two qubits. The set of all states in the simplex form a tetrahedron (blue), so do all matrices that are positive under partial transposition (red). The intersection of these two tetrahedra is the set of PPT states, i.e. the set of separable states (black). The maximally mixed state is located in the middle of this set (gray dot), while the four Bell states are the states furthest away from it (i.e. the four vertices of the blue tetrahedron).

problems.

Construction of the magic simplex

It is possible to construct a magic simplex for $3 \otimes 3$ systems as well, analogously to the $2 \otimes 2$ case, as a mixture of a complete set of mutually orthogonal maximally entangled states. This works as follows[79]:

One first choses any maximally entangled state $|\Omega_{0,0}\rangle$ and choses the basis such that

$$|\Omega_{0,0}\rangle = \frac{1}{\sqrt{3}} \sum_{i=1}^{3} |i,i\rangle \tag{6.8}$$

One then defindes 8 other states

$$|\Omega_{k,l}\rangle = W_{k,l} \otimes \mathbb{1} |\Omega_{0,0}\rangle \tag{6.9}$$

via the Weyl operators $W_{k,l}$, which are defined in eq. (2.22).

Since the Weyl operators are unitary, these states are maximally entangled

as well and are defined such that all $|\Omega_{k,l}\rangle$ are mutually orthogonal. Now, the magic simplex $\mathcal{W}$ can be defined as the set of all states that can be written as

$$\rho = \sum_{k,l} c_{k,l} P_{k,l} \tag{6.10}$$

where $P_{k,l} = |\Omega_{k,l}\rangle \langle \Omega_{k,l}|$ and the $c_{k,l}$ are probabilities, i.e. $c_{k,l} \geq 0$ and $\sum c_{k,l} = 1$.

Geometrical properties of the magic simplex

Since the Weyl operators, that were used to define the vertices of $\mathcal{W}$ form a discrete group, $\mathcal{W}$ itself is highly symmetrical. Repetitive application of any $W_{k,l} \otimes \mathbb{1}$ to any one of the $|\Omega_{k,l}\rangle$ always forms a set of three different states $|\Omega_{k,l}\rangle$, $|\Omega_{m,n}\rangle$ and $|\Omega_{2m-k,2n-l}\rangle$. These states can be visualised as being located on a line, while all maximally entangled states form a periodic lattice (Fig. 10). Obviously, any two states automatically form a line, while a third
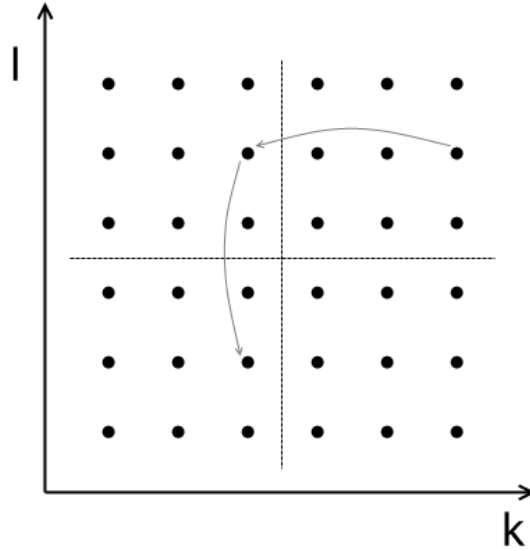
Fig. 10: The magic simplex in a system of two qutrits has a periodic symmetry in the form of a lattice, where each point corresponds to a maximally entangled state $P_{k,l}$. Each of the cells containing 9 states is fully equivalent to each other such cell, such that it suffices to study states $P_{k,l}$ with indices $k,l \in \{0,1,2\}$. This structure is commonly referred to as a phase space structure.

state can either be on this line or not. Thus, out of all the 84 sets that contain

three of the nine maximally entangled states, there are 12 that represent a line. These have several special properties, most importantly, to each of the 12 lines corresponds one of the 12 furthest outward separable states

$$\sigma_{out} = \frac{1}{3} \sum_{(k,l) \in \text{line}} P_{k,l} \tag{6.11}$$

Evidently, each of the nine maximally entangled states is equivalent to another (as long as they are considered by themselves and not in the context of specific other states). Since any two of the states automatically form a line and thus have similar geometric properties, there is also only one equivalence class for pairs of states. For triplets of states, there obviously exist two equivalence classes, one for all triplets that form a line and one for all that do not. For quadruplets of states there also exist two distinct equivalence classes, one in which three out of the four states form a line and one in which there is no line at all. For the complementary sets, the same statements hold (i.e. there are two equivalence classes of sets of five states each, two classes of sets of six states each, one class of septuplets and one class of octuplets).

<center>Mathematical properties of the magic simplex</center>

By definition, all states in $\mathcal{W}$ have maximally mixed subsystems. However, unlike in the $2 \otimes 2$ case, the converse statement is not true: There are states with maximally mixed subsystems, that do not belong to $\mathcal{W}$, for example the state

$$\rho = \frac{1}{3} |\Psi\rangle \langle\Psi| + \frac{2}{3} |\Phi\rangle \langle\Phi|$$
$$|\Psi\rangle = |0,0\rangle \tag{6.12}$$
$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|1,1\rangle + |2,2\rangle)$$

Also, the magic simplex is not unique, as it is in the $2 \otimes 2$ case. There exist several inequivalent sets of maximally entangled states, that result in different geometrical properties of the simplex formed by them. Due to the symmetry, choice of three different maximally entangled states that do not form a line determines the simplex.

Since $\mathcal{W}$ is 8-dimensional and it is thus not possible to graphically visualise it, further subsets of dimension two or three are of great interest. Usually, mainly mixtures of two or three maximally entangled states and the maximally mixed state are investigated, since these seem to offer most information about the geometry of the system.

Considering for example a mixture of three maximally entangled states on a line and the maximally mixed state[80]

$$\rho = \frac{1 - \alpha - \beta - \gamma}{9}\mathbb{1} + \alpha P_{k,l} + \beta P_{m,n} + P_{2m-k,2n-l} \qquad (6.13)$$

with $\alpha, \beta, \gamma \geq 0$ and $\alpha + \beta + \gamma \leq 1$, one finds that these states are still rather simple, since they do not contain any bound entanglement and have a very high symmetry. If however one also admits pseudomixtures (i.e. allows all values for α, β and γ that correspond to density matrices, in particular also negative values), small regions of bound entanglement appear (see Fig. 11).
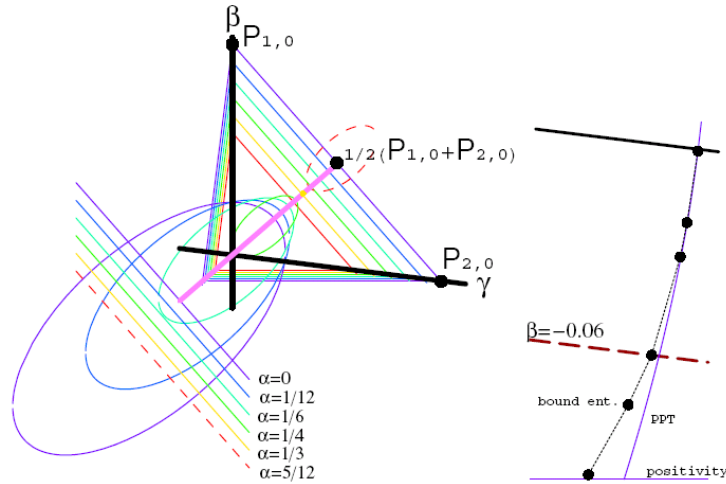
Fig. 11: States of the form (6.13) – here, without loss of generality $k = l = n = 0$ and $m = 1$ – exhibit bound entanglement only for negative parameter values. The triangles indicate areas of positivity, i.e. the set of states. PPT areas are ellipses cut by lines (or simply ellipses, for higher values of α). For $\alpha = 0$, the small area of bound entanglement is enlarged in the right picture, where the dots correspond to points where the used entanglement witnesses are optimal[80].

Even more complex sets of states can be found by considering states that are not located on a line

$$\rho = \frac{1 - \alpha - \beta - \gamma}{9}\mathbb{1} + \alpha P_{k,l} + \beta P_{m,n} + P_{o,p} \qquad (6.14)$$

where either $o \neq 2m - k$ or $p \neq 2n - l$ or both. Here the regions of bound entanglement are much bigger and the space shows comperatively complex structures (see Fig. 12).
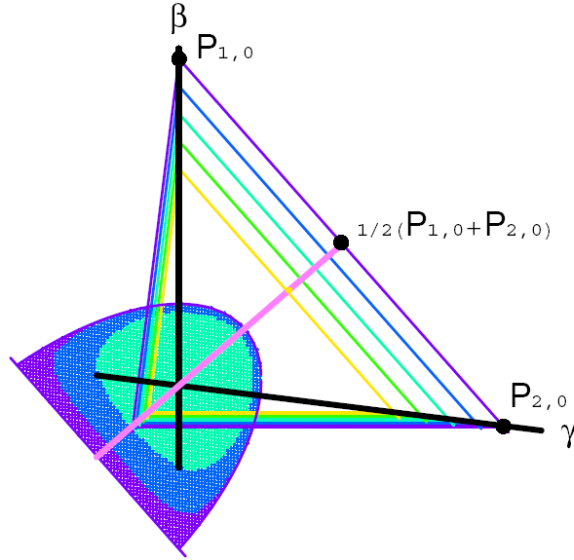

Fig. 12: States of the form (6.14) – here, without loss of generality $l = n = 0$, $k = m = p = 1$ and $o = -1$ (or, equivalently, $o = 2$) – show much more complicated structures than those of the form (6.13). The set of all states still is triangularly shaped, while the set of PPT states no more has the form of an ellipse, but a more complex one, part of which consists not of separable but of bound entangled states. The colour code is similar to Fig. 11[80].

In attempts to understand the geometry of mixtures of more states, mixtures of many states having only few different weights have been studied[81, 82], revealing that bound entanglement is not at all rare (although difficult to detect) and demonstrating that even such high mixtures still show high symmetry, since the magic simplex itself does.

7 Conclusion

Ever since the field of quantum information has been started to be taken seriously, there has been great advancement especially in characterising bipartite entangled systems (while multipartite entanglement is still widely unexplored).

While comperatively low dimensional systems, such as systems of two qubits or one qubit and one qutrit, as well as arbitrarily dimensional pure states, hardly seem to hold any secrets anymore, systems start to behave in very complex and unanticipated ways as soon as the dimensions get higher (starting with systems of two qutrits, which already are 80-dimensional). States in these systems can show completely different features from the lower dimensional ones, the most remarkable of which is probably the phenomenon of bound entanglement.

Discriminating between entangled and separable states becomes difficult, because tools like the PPT criterion are not capable of answering this question definitely anymore in these cases. Although stronger tools such as entanglement witnesses are at hand, these are much more difficult to put to use, thus still making it a hard task to determine any given state's entanglement properties.

The question of quantifying entanglement also becomes a very tricky one in higher dimensions, as it is not quite clear, which requirements a measure for entanglement should satisfy. In fact, it seems as if a single measure does not suffice at all to completely characterise and quantise the entanglement of general states. It is also completely unknown how a set of entanglement measures would need to be organised, in order to be 'complete' in the sense of containing full information about the entanglement contained in a quantum state.

Several entanglement measures are already widely established and have been thoroughly studied. Some of these indeed seem to work very well even in high dimensional systems, with the downside that most of them are (at the moment) not analytically computable (or even not computable at all). The probably most important and promising entanglement measures are the entanglement of formation and the entanglement of distillation.

The more work is put into understanding the structure of the underlying state spaces, the more it becomes appearent that geometry and symmetry

64

play very important roles and often offer a very intuitive and vivid (although maybe sometimes misleading) picture. This allows for geometrically motivated tools, such as geometric entanglement witnesses or geometric entanglement measures to be used in a very natural and sometimes surprisingly nonmathematical way.

While low-dimensional quantum information theory already finds realisation not only in laboratories but also is on the verge of commercial application, higher dimensional quantum information is still very young and only beginning to be understood. New effects and phenomenae are found frequently and there is no way of telling how many complex, contraintuitive and amazing discoveries there are yet to come in this field.

Acknowledgements

List of Figures

References

[1] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23:807, 823, 844, 1935.

[2] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[3] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

[4] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[5] Reinhold A. Bertlmann and Philipp Krammer. Bloch vectors for qudits. *J. Phys. A: Math. Theor.*, 41:235303, 2008.

[6] Barbara M. Terhal and Pawel Horodecki. Schmidt number for density matrices. *Phys. Rev. A*, 61:040301, 2000.

[7] Dagmar Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43:4237, 2002.

[8] Adriano Barenco, David Deutsch, Artur Ekert, and Richard Jozsa. Conditional quantum dynamics and logic gates. *Phys. Rev. Lett.*, 74:4083, 1995.

[9] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[10] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[11] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046, 1996.

[12] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722, 1996.

[13] R. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277, 1989.

[14] D. Deutsch. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425:73, 1989.

[15] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß. Distillability and partial transposition in bipartite systems. *Phys. Rev. A*, 61:062313, 2000.

[16] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: is there a "bound" entanglement in nature? *Phys. Rev. Lett.*, 80:5239, 1998.

[17] Rajiah Simon. NPPT bound entanglement exists. *e-Print*, pages quant–ph/0608250v1, 2006.

[18] Lukasz Pankowski, Marco Piani, Michal Horodecki, and Pawel Horodecki. Few more steps towards NPT bound entanglement. *e-Print*, pages 0711.2613 [quant–ph], 2007.

[19] Pawel Horodecki and Remigiusz Augusiak. On quantum cryptography with bipartite bound entangled states. *Quantum Information Processing: From Theory to Experiment, D.G. Angelakis et al. (eds.), NATO Science Series III*, 199:19, 2006.

[20] Remigiusz Augusiak and Pawel Horodecki. Bound entanglement maximally violating Bell inequalities: quantum entanglement is not equivalent to quantum security. *e-Print*, pages quant–ph/0405187v2, 2004.

[21] Pawel Horodecki, Michal Horodecki, and Ryszard Horodecki. Bound entanglement can be activated. *Phys. Rev. Lett.*, 82:1056, 1999.

[22] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1, 1996.

[23] Asher Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413, 1996.

[24] E. Størmer. Positive linear maps of operator algebras. *Acta Mathematica*, 110:233, 1963.

[25] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.*, 10:165, 1976.

[26] A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, 88:187904, 2002.

[27] Michal Horodecki and Pawel Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Phys. Rev. A*, 59:4206, 1999.

[28] Oliver Rudolph. A separability criterion for density operators. *J. Phys. A: Math. Gen.*, 33:3951, 2000.

[29] Oliver Rudolph. Some properties of the computable cross-norm criterion for separability. *Phys. Rev. A*, 67:032312, 2003.

[30] Oliver Rudolph. Further results on the cross norm criterion for separability. *e-Print*, pages quant–ph/0202121, 2002.

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

[32] Pawel Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232:333, 1997.

[33] Michael Reed and Barry Simon. Methods of modern mathematical physics I: Functional analysis. *Academic Press (New York and London)*, page 75, 1972.

[34] R. A. Bertlmann, H. Narnhofer, and W. Thirring. Geometric picture of entanglement and Bell inequalities. *Phys. Rev. A*, 66:032319, 2002.

[35] Reinhold A. Bertlmann and Philipp Krammer. Geometric entanglement witnesses and bound entanglement. *Phys. Rev. A*, 77:024303, 2008.

[36] Philipp Krammer. Characterizing entanglement with geometric entanglement witnesses. *J. Phys. A: Math. Theor.*, 42:065305, 2009.

[37] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3:275, 1972.

[38] K. Zyczkowski and I. Bengtsson. On duality between quantum maps and quantum states. *Open Syst. Inf. Dyn.*, 11:3, 2004.

[39] David Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. *Phys. Rev.*, 85:166, 180, 1952.

[40] N. Gisin. Bell's inequality holds for all non-product states. *Phys. Lett. A*, 154:201, 1991.

[41] Sandu Popescu and Daniel Rohrlich. Generic quantum nonlocality. *Phys. Lett. A*, 166:293, 1992.

[42] Anupam Garg and N. D. Mermin. Correlation inequalities and hidden variables. *Phys. Rev. Lett.*, 49:1220, 1982.

[43] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277, 1989.

[44] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880, 1969.

[45] R. Horodecki, P. Horodecki, and M. Horodecki. Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition. *Phys. Lett. A*, 200:340, 1995.

[46] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[47] Dagomir Kaszlikowski, L. C. Kwek, Jing-Ling Chen, Marek Zukowski, and C. H. Oh. Clauser-Horne inequality for three-state systems. *Phys. Rev. A*, 65:032118, 2002.

[48] A. Acín, T. Durt, N. Gisin, and J. I. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65:052325, 2002.

[49] Li-Bin Fu, Jing-Ling Chen, and Xian-Geng Zhao. Maximal violation of the Clauser-Horne-Shimony-Holt inequality for two qutrits. *Phys. Rev. A*, 68:022323, 2003.

[50] Willem M. de Muynck. POVMs: A small but important step beyond standard quantum mechanics. *e-Print*, pages quant–ph/0608087, 2006.

[51] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Phys. Lett. A*, 210:151, 1996.

[52] Samuel L. Braunstein, A. Mann, and M. Revzen. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett.*, 68:3259, 1992.

[53] Barbara M. Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A*, 271:319, 2000.

[54] Philipp Hyllus, Otfried Gühne, Dagmar Bruß, and Maciej Lewenstein. Relations between entanglement witnesses and Bell inequalities. *Phys. Rev. A*, 72:012321, 2005.

[55] Sandu Popescu. Bell's inequalities and density matrices: Revealing "hidden" nonlocality. *Phys. Rev. Lett.*, 74:2619, 1995.

[56] Asher Peres. Collective tests for quantum nonlocality. *Phys. Rev. A*, 54:2685, 1996.

[57] Sandu Popescu. Bell's inequalities versus teleportation: What is nonlocality? *Phys. Rev. Lett.*, 72:797, 1994.

[58] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Phys. Rev. Lett.*, 78:2275, 1997.

[59] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A*, 57:1619, 1998.

[60] Reinhold A. Berltmann, Katharina Durstberger, Beatrix C. Hiesmayr, and Philipp Krammer. Optimal entanglement witnesses for qubits and qutrits. *Phys. Rev. A*, 72:052331, 2005.

[61] Frank Verstraete, Jeroen Dehaene, and Bart De Moor. On the geometry of entangled states. *J. Mod. Opt.*, 49:1277, 2002.

[62] V. Vedral, M. B. Plenio, K. Jacobs, and P. L. Knight. Statistical inference, distinguishability of quantum states, and quantum entanglement. *Phys. Rev. A*, 56:4452, 1997.

[63] L. Henderson and V. Vedral. Information, relative entropy of entanglement, and irreversibility. *Phys. Rev. Lett.*, 84:2263, 2000.

[64] K.G. H. Vollbrecht and R. F. Werner. Entanglement measures under symmetry. *e-Print*, quant/ph/0010095, 2001.

[65] M. Kleinmann, H. Kampermann, and D. Bruß. Structural approach to unambiguous discrimination of two mixed states. *e-Print*, pages 0803:1083 [quant–ph], 2008.

[66] Christopher A. Fuchs and Carlton M. Caves. Mathematical techniques for quantum communication theory. *Open Systems and Information Dynamics*, 3:1, 1995.

[67] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824, 1996.

[68] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Limits for entanglement measures. *Phys. Rev. Lett.*, 84:2014, 2000.

[69] Patrick M. Hayden, Michal Horodecki, and Barbara M. Terhal. The asymptotic entanglement cost of preparing a quantum state. *J. Phys. A: Math. Gen.*, 34:6891, 2001.

[70] William K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245, 1998.

[71] Koenraad Audenaert, Frank Verstraete, and Bart De Moor. Variational characterizations of separability and entanglement of formation. *Phys. Rev. A*, 64:052304, 2001.

[72] Barbara M. Terhal and Karl Gerd H. Vollbrecht. Entanglement of formation for isotropic states. *Phys. Rev. Lett.*, 85:2625, 2000.

[73] Florian Minert, Marek Kus, and Andreas Buchleitner. Concurrence of mixed bipartite quantum states in arbitrary dimensions. *Phys. Rev. Lett.*, 92:167902, 2004.

[74] Guifré Vidal and Rolf Tarrach. Robustness of entanglement. *Phys. Rev. A*, 59:141, 1999.

[75] G. Vidal and R. F. Werner. Computable measure for entanglement. *Phys. Rev. A*, 65:032314, 2002.

[76] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Inseparable two spin-1/2 dinsity matrices can be distilled to a singlet form. *Phys. Rev. Lett.*, 78:574, 1997.

[77] Anna Sanpera, Dagmar Bruß, and Maciej Lewenstein. Schmidt number witnesses and bound entanglement. *Phys. Rev. A*, 63:050301, 2001.

[78] Florian Hulpke, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera. Simplifying Schmidt number witnesses via higher dimensional embeddings. *Quant. Inf. Comp.*, 4:207, 2004.

[79] Bernhard Baumgartner, Beatrix C. Hiesmayr, and Heide Narnhofer. The state space for two qutrits has a phase space structure in its core. *Phys. Rev. A*, 74:032327, 2006.

[80] B. Baumgartner, B. C. Hiesmayr, and H. Narnhofer. The geometry of bipartite qutrits including bound entanglement. *Phys. Lett. A*, 372:2190, 2008.

[81] Reinhold A. Bertlmann and Philipp Krammer. Bound entanglement in the set of Bell state mixtures of two qutrits. *Phys. Rev. A*, 78:014303, 2008.

[82] Reinhold A. Bertlmann and Philipp Krammer. Entanglement witnesses and geometry of entanglement of two-qutrit states. *e-Print*, pages 0901.4729 [quant–ph], 2009.

Lebenslauf

Andreas Gabriel
Passauerplatz 6/42
A-1010 Wien

Geboren am: 30.1.1986
Staatsbürgerschaft: Österreich
Tel.: 0699 1958 6946
E-Mail: a_gabriel@gmx.at
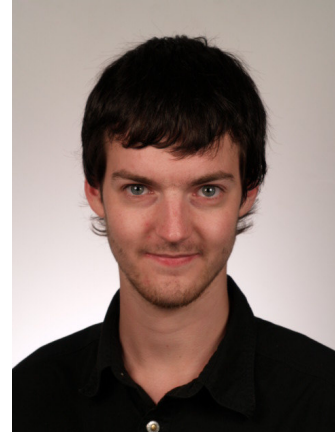
Ausbildung

10/2004 – dato	Studium der Physik, Universität Wien
09/1996 – 06/2004	Lise-Meitner-Realgymnasium, 1010 Wien Absolvierung sämtlicher Schulstufen und der Reifeprüfung mit ausgezeichnetem Erfolg
09/1992 – 06/1996	Volksschule Börsegasse, 1010 Wien

Absolvierte Vorträge

04/2006	Quantenteleportation
06/2007	Verschränkung
11/2007	Kochen-Specker-Theorem
11/2007	Beta-Spektroskopie
01/2008	Entanglement-Witnesses und Bell-Ungleichungen
05/2008	Bell-Ungleichungen für QuTrits
06/2008	Bound Entanglement
11/2008	Unambiguous State Discrimination
04/2009	Verschränkungsmaße
06/2009	Quantenkryptographie und Abhörsicherheit

Andere Leistungen

06/2004	Teilnahme am Landeswettbewerb Wien der 30. Österreichischen Chemie-Olympiade, 10. Platz
2003 – dato	Diverse Nachhilfetätigkeiten für Schüler und Studenten
2003	Vorbereitungs- und Durchführhilfe eines Vortrags von Dr. Ralf Becker

Besondere Kenntnisse

Sprachen	Deutsch (Muttersprache) Englisch fließend in Wort und Schrift Französisch Grundkenntnisse
EDV	Europäischer Computerführerschein (ECDL) Programmieren mit HTML und Basic Erfahrung mit Adobe Illustrator, LaTeX und Mathematica