Preface

Entanglement and (de-)coherence arguably define the central issues of concern in present day quantum information theory. In state-of-the-art experiments, ever larger numbers of quantum particles are entangled in a controlled way, and ever heavier particles are brought to interfere. Some sub-fields of quantum information science, in particular quantum cryptography, already find commercial applications, and communal communication networks that rely on quantum information technology are in preparation, as well as satellite-based quantum communication. Moreover, entanglement is no more considered as just an important resource for quantum information processing, but it allows for a better characterization of "complex" quantum systems, realized, e.g., in engineered, interacting many-particle systems, as well as in the solid state. Thus, there is a permanent and in many respects enhanced need for a deeper understanding of – and fresh approaches to – quantum entanglement, notably in high-dimensional quantum systems. Equally so, entanglement being a consequence of the quantum mechanical superposition principle for composite systems, we need a better understanding of the environment-induced destruction of coherent superposition states and of those interference phenomena that may survive the action of a noisy environment. Such research will allow us to identify realistic scales and possibly novel strategies for harvesting quantum interference phenomena.

The present book collects a series of advanced lectures on the theoretical foundations of this active research field and illustrates the breadth of present day theoretical efforts – from mathematics to mesoscopic transport theory. Uhlmann and Crell start out with a mathematical introduction to the geometry of state space, followed by an elementary introduction to entanglement theory by Mintert et al. Back again in the mathematical realm, Kauffman and Lomonaco discuss topological aspects of quantum computation, with some close relation to the theory of braids and knots. Ozorio de Almeida sheds new light on entanglement, in phase space, and touches some issues related to decoherence theory, which are then systematically expanded by Hornberger. Müller is subsequently concerned with dephasing and decoherence in the context of spintronics and disordered systems, thus establishing the bridge to real-life quantum transport, and the solid state.

All lecture notes start out from an elementary level and proceed along a steep learning curve, what makes the material equally suitable for student

seminars on the more fundamental theoretical aspects of quantum information, as well as to supplement advanced lectures on this topic.

The material assembled here was first taught by the authors during an international summer school on "Quantum Information" at the Max Planck Institute for the Physics of Complex Systems in Dresden, in September 2005, thus inspiring the idea to compile the present book. The editors' special thanks therefore go to the authors, as well to Markus Grassl, Martin Rötteler, Christian Roos, Hartmut Häffner, Herbert Wagner, Per Delsing, Daniel Estève, Steffen Glaser, Gilles Nogues, Mauro d'Ariano, Robin Hudson, Reinhard Werner, Maciej Lewenstein, Andzrej Kossakowski, Karol Życzkowski, Mark Fannes, Richard Gill, Rainer Blatt, Marita Schneider, Christian Caron, Gabriele Hakuba, Andreas Erdmann, Helmut Deggelmann, Torsten Goerke, Heidi Naether, Andreas Schneider, Hubert Scherrer, Andreas Wagner, Karsten Batzke, and Jan-Michael Rost, who all have their share in getting the present volume into press.

Freiburg im Breisgau and Bogotá,
August 2008

Andreas Buchleitner
Carlos Viviescas
Markus Tiersch

2 Basic Concepts of Entangled States

F. Mintert[1,3], C. Viviescas[2,3], and A. Buchleitner[3]

[1] Department of Physics, Harvard University, 17 Oxford Street, Cambridge MA, USA
[2] Departamento de Física, Universidad Nacional de Colombia, Carrera 30 No. 45-03 Edif. 404, Bogotá D. C., Colombia
[3] Max-Planck-Institut für Physik komplexer Systeme, Nöthnitzer Str. 38, 01187 Dresden, Germany

2.1 Introduction

Quantum systems display properties that are unknown for classical ones, such as the superposition of quantum states, interference, or tunneling. These are all one-particle effects that can be observed in quantum systems, which are composed of a single particle. But these are not the only distinctions between classical and quantum objects – there are further differences that manifest themselves in composite quantum systems, that is, systems that are comprised of at least two subsystems. It is the correlations between these subsystems that give rise to an additional distinction from classical systems, whereas correlations in classical systems can always be described in terms of classical probabilities; this is not always true in quantum systems. Such non-classical correlations lead to apparent paradoxes like the famous Einstein Podolsky Rosen scenario [1] that might suggest, on the first glance, that there is remote action in quantum mechanics.

States that display such non-classical correlations are referred to as *entangled states*, and it is the aim of this chapter to introduce the basic tools that allow to understand the nature of such states, to distinguish them from those that are classically correlated, and to quantify non-classical correlations.

2.2 Entangled States

Composite quantum systems are systems that naturally decompose into two or more subsystems, where each subsystem itself is a proper quantum system. Referring to a decomposition as "natural" implies that it is given in an obvious fashion due to the physical situation. Most frequently, the individual susbsystems are characterized by their mutual distance that is larger than the size of a subsystem. A typical example is a string of ions, where each ion is a subsystem, and the entire string is the composite system. Formally, the Hilbert space $\mathcal{H}$ associated with a composite, or *multipartite system*, is given by the tensor product $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ of the spaces corresponding to each of the subsystems.

Mintert, F. et al.: *Basic Concepts of Entangled States*. Lect. Notes Phys. **768**, 61–86 (2009)
DOI 10.1007/978-3-540-88169-8_2

In the following, we shall focus on finite-dimensional *bipartite* quantum systems, i.e., systems composed of two distinct subsystems, described by the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. Many of the concepts and ideas that we introduce can, nevertheless, be generalized to *multipartite systems*.

2.2.1 Pure States

We start out with a bipartite system with each subsystem prepared in a pure state $|\psi_i\rangle\,(i = 1, 2)$. The state of the composite system $|\Psi_\mathrm{s}\rangle$ is the direct product thereof:

$$|\Psi_\mathrm{s}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \ . \tag{2.1}$$

Suppose that one could perform only local measurements on the system, i.e., one had access to only one of the subsystems at a time. Then, after a measurement of any local observable $a \otimes \mathbb{1}$ on the first subsystem, where a is a hermitian operator acting on $\mathcal{H}_1$, and $\mathbb{1}$ is the identity acting on $\mathcal{H}_2$, the state of the first subsystem will be projected onto an eigenstate of a, but the state of the second subsystem remains unchanged. If later on, one performs a second local measurement, now on the second subsystem, it will yield a result that is independent of the result of the first measurement. Hence, the measurement outcomes on different subsystems are uncorrelated with each other and depend only on the states of each respective subsystem.

A general pure state in $\mathcal{H}$ can be given by a superposition of pure states of the form (2.1), for example,

$$|\Psi_\mathrm{e}\rangle = \frac{1}{\sqrt{2}} \left(|\psi_1\rangle \otimes |\psi_2\rangle + |\phi_1\rangle \otimes |\phi_2\rangle\right) \ , \tag{2.2}$$

where $|\psi_i\rangle \neq |\phi_i\rangle\,(i = 1, 2)$. We may now ask what the state $|\Psi_\mathrm{e}\rangle$ looks like if one has access to only one of the subsystems? For a local operator $a \otimes \mathbb{1}$ on the first subsystem, the expectation value observed in an experiment reads

$$\begin{aligned} \langle a \rangle &= \langle \Psi_\mathrm{e} | a \otimes \mathbb{1} | \Psi_\mathrm{e} \rangle \\ &= \mathrm{tr}(a \otimes \mathbb{1} \ |\Psi_\mathrm{e}\rangle\langle\Psi_\mathrm{e}|) \\ &= \mathrm{tr}_1(a\, \mathrm{tr}_2 |\Psi_\mathrm{e}\rangle\langle\Psi_\mathrm{e}|) \\ &= \mathrm{tr}_1(a \varrho_1) \ , \end{aligned} \tag{2.3}$$

where $\mathrm{tr}_{1,2}$ denotes the partial trace over the first/second subsystem, and $\varrho_1 = \mathrm{tr}_2 |\Psi_\mathrm{e}\rangle\langle\Psi_\mathrm{e}|$ is the reduced density matrix of the first subsystem. Since (2.3) holds for any local operator a, we need to conclude that the state of the first subsystem alone is given by ϱ_1. An analogous reasoning leads to the conclusion that also the state of the second subsystem is described by its reduced density matrix $\varrho_2 = \mathrm{tr}_1 |\Psi_\mathrm{e}\rangle\langle\Psi_\mathrm{e}|$. The state of the composite system, however, is not equal to the product of both subsystem states, $\rho = |\Psi_\mathrm{e}\rangle\langle\Psi_\mathrm{e}| \neq \rho_1 \otimes \rho_2$. Moreover, if one performs a local measurement on one subsystem, this leads

to a state reduction of the entire system state, not only of the subsystem on which the measurement had been performed. Therefore, the probabilities for an outcome of a measurement on one subsystem are influenced by prior measurements on the other subsystem. Thus, measurement results on – possibly distant and non-interacting – subsystems are correlated.

Based on these considerations, we can define that

> states that can be written as a product of pure states, as in (2.1), are called *product* or *separable states*. If on the contrary, there are no local states $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, such that the state of the system $|\Psi\rangle$ can be written as a product thereof:
>
> $$\nexists\ |\psi_1\rangle \in \mathcal{H}_1, |\psi_2\rangle \in \mathcal{H}_2 \quad \text{such that} \quad |\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle\ , \tag{2.4}$$
>
> then $|\Psi\rangle$ is an *entangled state*.

2.2.2 Mixed States

So far we considered only pure states. More generally, however, the state of a quantum system can be mixed. Mixed states are in fact the most frequently encountered states in real experiments, since hardly any quantum system can be isolated completely from its surroundings. As elaborated in more detail in Sect. 5.3.1, it is in general not possible to keep track of the many environmental degrees of freedom, and the state of the system is given by the partial trace over the environment. This reduced state is then typically mixed.

Similarly to the case of pure states, *mixed product states*,

$$\varrho = \rho^{(1)} \otimes \rho^{(2)} \tag{2.5}$$

with $\rho^{(1)}$ and $\rho^{(2)}$ for the respective subsystems, do not exhibit correlations. A convex sum of different product states,

$$\varrho = \sum_i p_i\, \rho_i^{(1)} \otimes \rho_i^{(2)}\ , \tag{2.6}$$

with $p_i > 0$ and $\sum_i p_i = 1$, however, will in general yield correlated measurement results, i.e., there are local observables a and b such that $\mathrm{tr}(\varrho(a \otimes b)) \neq \mathrm{tr}(\varrho(a \otimes \mathbb{1}))\,\mathrm{tr}(\varrho(\mathbb{1} \otimes b)) = \mathrm{tr}_1 \varrho_1 a\ \mathrm{tr}_2 \varrho_2 b$. These correlations can be described in terms of the classical probabilities p_i, and are therefore considered classical. States of the form (2.6) thus are called *separable mixed states*.

Mixed entangled states, in turn, are defined by the non-existence of a decomposition into product states [2]:

> A mixed state ϱ is entangled if there are no local states $\rho_i^{(1)}$, $\rho_i^{(2)}$, and non-negative weights p_i, such that ϱ can be expressed as a convex mixture thereof:

$$\nexists\ \varrho_i^{(1)}, \varrho_i^{(2)}, p_i\ \geq 0 \quad \text{such that} \quad \varrho = \sum_i p_i\, \rho_i^{(1)} \otimes \rho_i^{(2)}\ . \tag{2.7}$$

Entangled states imply quantum correlations of measurements on different subsystems which, in contrast to classical correlations (see above), *cannot* be described in terms of only classical probabilities.

2.3 Separability Criteria

The above definitions of separable and entangled states appear simple on a first sight. But checking separability of a given state can turn out to be much more involved than one might expect. Separability is defined via the *existence* of a decomposition of a state into product states in the case of pure states, or into a convex sum of tensor products for mixed states. That is, in order to show that a given state is separable, one has to look for such decompositions. Once a decomposition is found one knows that a state is separable. But the failure to find one can have two different reasons: either the state is entangled and there is no decomposition into product states, or the state is actually separable, but the appropriate decomposition could not be identified.

For this reason, there is a need for potentially simple criteria to distinguish separable from entangled states that do not require an explicit search. For pure states, there are criteria that discriminate separable and entangled states unambiguously, but for mixed states similar tools are available only for low-dimensional system. For higher dimensional systems, these tools can provide only partial information, as we will see later on. But, before we discuss mixed states, we will start out with the comparatively simpler case of pure states.

2.3.1 Pure States

Let us consider the exemplary case

$$|\Psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + 2|1\rangle}{\sqrt{5}}\ . \tag{2.8}$$

One can see that $|\Psi\rangle$ factorizes into local states – it is separable, though could be rewritten also as

$$|\Psi\rangle = \frac{|00\rangle + 2|01\rangle + |10\rangle + 2|11\rangle}{\sqrt{10}}\ , \tag{2.9}$$

where separability is less evident. It just turns out that separability is more easily identified if $|\Psi\rangle$ is expressed in the bases $\{(|0\rangle+|1\rangle)/\sqrt{2}, (|0\rangle-|1\rangle)/\sqrt{2}\}$ of $\mathcal{H}_1$ and $\{(|0\rangle+2|1\rangle)/\sqrt{5}, (2|0\rangle-|1\rangle)/\sqrt{5}\}$ of $\mathcal{H}_2$ than in the basis $\{|0\rangle, |1\rangle\}$. As we shall see, the observation is generic, in the sense that there is always a basis that allows to reveal the entanglement properties. The representation of a state in this basis is called the *Schmidt decomposition* [3].

Schmidt Decomposition

Given two arbitrary local bases $\{|\varphi_i\rangle\}$ and $\{|\phi_i\rangle\}$ in the spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, any pure state $|\Psi\rangle$ in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ can be expressed in terms of the corresponding product basis

$$|\Psi\rangle = \sum_{ij} d_{ij} |\varphi_i\rangle \otimes |\phi_j\rangle \ . \tag{2.10}$$

The expansion coefficients d_{ij} are given by the overlap of the state with the basis vectors, $d_{ij} = \langle\varphi_i| \otimes \langle\phi_j|\Psi\rangle$. If one now makes a change of bases $|\tilde{\varphi}_i\rangle = \mathcal{U}|\varphi_i\rangle$ and $|\tilde{\phi}_i\rangle = \mathcal{V}|\phi_i\rangle$, with $\mathcal{U}$ and $\mathcal{V}$ arbitrary, local unitary transformations on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, the d_{ij} change accordingly:

$$\begin{aligned} \tilde{d}_{ij} &= \langle\tilde{\varphi}_i| \otimes \langle\tilde{\phi}_j|\Psi\rangle \\ &= \langle\varphi_i|\mathcal{U}^\dagger \otimes \langle\phi_j|\mathcal{V}^\dagger|\Psi\rangle \\ &= \sum_{pq} \langle\varphi_i|\mathcal{U}^\dagger|\varphi_p\rangle\langle\phi_j|\mathcal{V}^\dagger|\phi_q\rangle\langle\varphi_p| \otimes \langle\phi_q|\Psi\rangle \\ &= [udv]_{ij} \ , \end{aligned} \tag{2.11}$$

where in the third line we used the resolution of the identity on each subsystem, $\sum_i |\varphi_i\rangle\langle\varphi_i| = \mathbb{1}$ and $\sum_i |\phi_i\rangle\langle\phi_i| = \mathbb{1}$, and we defined the unitary matrices $u_{ip} = \langle\varphi_i|\mathcal{U}^\dagger|\varphi_p\rangle$, $v_{qj} = \langle\phi_j|\mathcal{V}^\dagger|\phi_q\rangle$. In the new basis, the state is given by

$$|\Psi\rangle = \sum_{ij} [udv]_{ij} \, |\tilde{\varphi}_i\rangle \otimes |\tilde{\phi}_j\rangle \ . \tag{2.12}$$

In order to obtain the Schmidt decomposition of $|\Psi\rangle$, we use the fact that for every complex matrix d, there always exist unitary transformations u and v such that udv is diagonal. This provides the *singular value decomposition* of d [4], with real, non-negative diagonal entries $\mathcal{S}_i$, called *singular values*. Therefore, for each state $|\Psi\rangle$, one can always find local bases $|\varphi_i^S\rangle$ and $|\phi_i^S\rangle$ in terms of which (2.12) reduces to

$$|\Psi\rangle = \sum_i \sqrt{\lambda_i} \, |\varphi_i^S\rangle \otimes |\phi_i^S\rangle \ , \tag{2.13}$$

where the $\lambda_i = \mathcal{S}_i^2$ are known as *Schmidt coefficients*, and the sum is limited by the dimension of the smaller subsystem. Like eigenvalues of a matrix, also the singular values are uniquely defined. Hence, for any state $|\Psi\rangle$ the Schmidt coefficients are unique. Furthermore, since the *Schmidt basis* $\{|\varphi_i^S\rangle \otimes |\phi_j^S\rangle\}$ is given by separable states, all information on the entanglement of a state is encoded in the Schmidt coefficients: If there is only one non-vanishing Schmidt coefficient, then $|\Psi\rangle$ is separable. Otherwise, when at least two Schmidt coefficients are different from zero, it is not possible to express $|\Psi\rangle$ in the form (2.1). Consequently, we can conclude that a pure state $|\Psi\rangle$ is separable if and only if it has only one non-vanishing Schmidt coefficient.

Reduced Density Matrix

Since the Schmidt coefficients are so useful for the distinction of separable and entangled states, we should focus on how to evaluate them. The reduced density matrices are particularly helpful in this context. The one of the first subsystem reads

$$\begin{aligned}\varrho_1 &= \mathrm{tr}_2|\Psi\rangle\langle\Psi| \\ &= \mathrm{tr}_2 \sum_{ij} \sqrt{\lambda_i\lambda_j}\, |\varphi_i^S\rangle\langle\varphi_j^S| \otimes |\phi_i^S\rangle\langle\phi_j^S| \\ &= \sum_i \lambda_i |\varphi_i^S\rangle\langle\varphi_i^S| \,,\end{aligned} \tag{2.14}$$

in terms of the Schmidt decomposition (2.13), where we used the orthonormality of the Schmidt basis while performing the trace over the second subsystem.

We see that the Schmidt coefficients are given by the eigenvalues of the reduced density matrix ϱ_1. An equivalent reasoning holds for the reduced density matrix of the second subsystem $\varrho_2 = \mathrm{tr}_1|\Psi\rangle\langle\Psi|$; that is ϱ_1 and ϱ_2 have the same non-vanishing eigenvalues, and the basis vectors of the Schmidt basis are given by the eigenstates of ϱ_1 and ϱ_2.

We not only found a simple prescription to evaluate the Schmidt coefficients of any state $|\Psi\rangle$, but since separability requires that exactly one Schmidt coefficient is different from zero, we also have related the entanglement of a pure state $|\Psi\rangle$ to the degree of mixing of the reduced density matrices. That is, we can restate the separability criterion for pure states:

$$\begin{aligned}&\mathrm{tr}\varrho_r^2 = 1 \Rightarrow \varrho_r \text{ is pure} \quad \Rightarrow |\Psi\rangle \text{ is separable} \\ &\mathrm{tr}\varrho_r^2 < 1 \Rightarrow \varrho_r \text{ is mixed} \Rightarrow |\Psi\rangle \text{ is entangled}\end{aligned} \tag{2.15}$$

with r referring to either one of the two subsystems.

2.3.2 Mixed States

For pure states, the Schmidt decomposition provides a necessary and sufficient criterion for separability. Unfortunately, for mixed states such an elegant decomposition does not exist. In particular, if a state is mixed, the degree of mixing of its reduced density matrices is not an indicator of entanglement. Therefore, we need to find some new criteria to distinguish entangled from separable mixed states. The most prominent of such tools are *entanglement witnesses* and *positive maps*. As we shall see, both concepts are closely related.

Entanglement Witnesses

An entanglement witness W [5, 6] is a hermitian operator acting on $\mathcal{H}$ that is *not* positive definite, but that yields positive expectation values

$$\langle \Psi_{\rm s}|W|\Psi_{\rm s}\rangle \geq 0 \ , \tag{2.16}$$

for all separable pure states $|\Psi_{\rm s}\rangle$. Since any separable mixed state can be expressed as a convex sum of projectors onto pure separable states, $\varrho_{\rm s} = \sum_i p_i \, |\Psi_{\rm s}^{(i)}\rangle\langle\Psi_{\rm s}^{(i)}|$ with $p_i > 0$, and $\sum_i p_i = 1$, (2.18) implies that the expectation value of an entanglement witness with respect to any separable mixed state is also non-negative,

$$\mathrm{tr}(\varrho_{\rm s} W) = \sum_i p_i \langle \Psi_{\rm s}|W|\Psi_{\rm s}\rangle \geq 0 \ . \tag{2.17}$$

Thus, if a given density matrix ϱ leads to a negative expectation value

$$\mathrm{tr}(\varrho W) < 0 \ , \tag{2.18}$$

then ϱ is *entangled*, and one says that W *detects* ϱ.

The central benefit of witnesses is that there exists a witness for any entangled state that detects it [5]. Here we do not go into the details of the formal proof, but rather give some geometric, intuitive arguments that allow to understand why entanglement witnesses work.

Geometry of Quantum States

Let's try to understand quantum states in a geometrical setting. Density matrices can be conceived as vectors in a vector space that is referred to as Hilbert–Schmidt space [7]. For a geometric interpretation of this vector space, one needs a scalar product, and in the present context, this is defined as

$$\langle A|B\rangle = \mathrm{tr}\ A^\dagger B \ . \tag{2.19}$$

Now, separable states form a convex set. That means that, given two arbitrary separable states $\varrho_s^{(1)}$ and $\varrho_s^{(2)}$, any convex sum $\lambda\varrho_s^{(1)} + (1-\lambda)\varrho_s^{(2)}$ $(1 \geq \lambda \geq 0)$ is again separable. Geometrically, this means that the set of separable states has no trough, as illustrated in Fig. 2.1, where the shapes A, B, and C represent different convex sets, whereas D is not convex, since it has a trough on its right bottom part. Now, one can find several lines that separate the grey shaded areas from their white surrounding – the depicted lines W_i $(i = 1, \ldots, 8)$ are only exemplary ones; one may find many more.

There is one crucial difference between cases A, B, and C on the one hand, and D on the other hand: For any point outside the convex sets A, B, and C, one can find a straight line that separates this point from the gray-shaded area. For D, this is not always possible. There is no straight line that separates D from point Z.

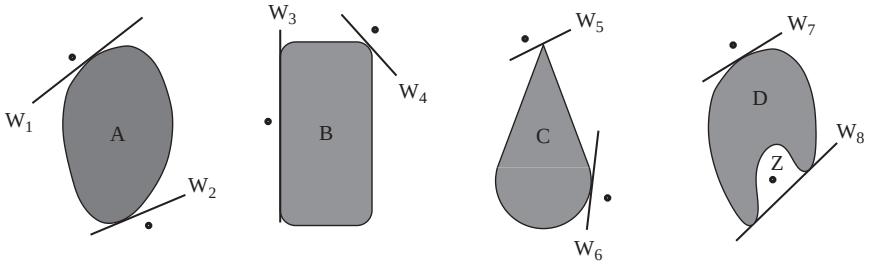

Fig. 2.1. Four different shapes, three of which (A, B, C) are convex, whereas shape D is not. To any point outside the convex shapes, there exists a line (like W_i, $i = 1, \ldots, 6$) that separates this point from the corresponding convex shape. For the non-convex shape D, the situation is different: for the point Z, there is no such line. The situation of entanglement witnesses is analogous: the set of separable states is convex; there exists a witness (the analogue of a line W_i) to any entangled state (the analogue of a point outside the grey shapes) that separates it from the set of separable states (the analogue of one of the convex shapes)

Although, the set of separable states is high dimensional and more complicated than the shapes in Fig. 2.1, the basic geometric picture of Fig. 2.1 still allows to understand the basic mechanism of entanglement witnesses.

Geometric Interpretation of Entanglement Witnesses

A separable state is characterized by the condition tr $\varrho W \geq 0$. The condition that trσW vanishes, requires σ to be a linear combination of operators $\mathcal{O}_i$ that are orthogonal to W:

$$\sigma = \sum_i \alpha_i \mathcal{O}_i \ , \qquad \text{with} \qquad \mathrm{tr}(\mathcal{O}_i W) = 0 \ . \tag{2.20}$$

That is, the condition tr$\sigma W = 0$ defines a hyperplane in the space of operators – analogous to the lines W_i in Fig 2.1. The sign of tr ϱW then indicates on which side of the hyperplane ϱ is situated, and all separable states are situated on one side of this hyperplane (tr $\varrho W \geq 0$). Since the separable states form a convex set, there is a witness to any entangled state that detects it, just like there is a line to any point outside A, B, or C that separates it from the respective grey shaded areas.

Due to the complicated structure of the set of separable states that has curved borders, one needs infinitely many witnesses to characterize it completely. Given some specific entangled state ϱ, it can be rather complicated to find a witness that detects it, and the failure to find a suitable witness for a state ϱ does not necessarily allow to conclude that ϱ is separable. Therefore, a witness provides a *necessary separability criterion*: if a state is separable, it will yield a non-negative expectation value for any witness; but separability of a state *cannot* deduced from such a non-negative expectation value.

Positive Maps

An alternative tool to check on separability is the so-called positive linear maps Λ that map the set of operators $\mathcal{B}(\mathcal{H})$ acting on a Hilbert space $\mathcal{H}$ on the set $\mathcal{B}(\tilde{\mathcal{H}})$, where $\tilde{\mathcal{H}}$ can – though not necessarily needs to – be a different Hilbert space than $\mathcal{H}$. Such a map Λ is considered positive if $\tilde{\varrho} = \Lambda(\varrho)$ is a positive operator, for any positive operator ϱ. Now, let us consider the case of a bipartite system. One can extend this map to the product space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, such that the extended map Λ_E acts on $\mathcal{B}(\mathcal{H}_1)$ like Λ, and Λ_E acts trivially on $\mathcal{B}(\mathcal{H}_2)$, i.e.,

$$\Lambda_E = \Lambda \otimes \mathbb{1} \ . \tag{2.21}$$

A very counterintuitive property of these positive maps is that the extended map Λ_E is *not* necessarily positive. That is, for some maps Λ, there are states ϱ on $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, such that $\Lambda_E(\varrho)$ is not a positive operator.

Now, let us take a separable state ϱ_s, i.e., one that has a convex decomposition into product states, and apply a positive linear map to it,

$$\Lambda_E(\varrho_s) = \sum_i p_i \Lambda(\rho_i^{(1)}) \otimes \rho_i^{(2)} \ . \tag{2.22}$$

Since Λ is positive, $\Lambda(\rho_i^{(1)})$ is a positive operator; and since also p_i and $\rho_i^{(2)}$ are positive, any expectation value of $\Lambda_E(\varrho_s)$ is positive, and therefore $\Lambda_E(\varrho_s)$ remains a positive operator. Thus, for any separable state, there is *no* positive map Λ, such that $\Lambda_E(\varrho_s)$ is *not* a positive operator. That is, if one can find a positive map Λ such that $\Lambda_E(\varrho)$ has at least one negative eigenvalue for a given state ϱ, then one knows for sure that ϱ is entangled.

The inverse statement is more involved. If one wants to prove separability of a state ϱ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, then it is necessary to consider maps Λ that map $\mathcal{B}(\mathcal{H}_2)$ on $\mathcal{B}(\mathcal{H}_1)$ – that is $(\mathbb{1} \otimes \Lambda)(\varrho)$ is an operator acting on $\mathcal{H}_1 \otimes \mathcal{H}_1$. Now, a state is separable if and only if $(\mathbb{1} \otimes \Lambda)(\varrho)$ is positive for all positive linear maps of $\mathcal{B}(\mathcal{H}_2)$ on $\mathcal{B}(\mathcal{H}_1)$. But, since the characterization of positive maps is an open problem, such maps only provide a necessary separability criterion like above in the case of witnesses: if one has found a map Λ, such that $(\mathbb{1} \otimes \Lambda)(\varrho)$ is *not* a positive operator, then the state ϱ is entangled. But if one fails to find such a map, then one does not necessarily know whether this is due to separability of ϱ, or just due to the lack of success to find a suitable map.

Only in systems of small dimension the concept of positive maps allows to formulate a constructive criterion that is both necessary and sufficient: for a system of two qubits or a system of one qubit and one qutrit (three-level system), one can check separability by considering only a single positive map, and that is the transposition $T(\varrho) = \varrho^T$, i.e., the reflection of a matrix ϱ along the diagonal [5, 8]. The underlying reason for this is that *any* positive map

from $\mathcal{B}(\mathbb{C}^2)$ on $\mathcal{B}(\mathbb{C}^2)$, or on $\mathcal{B}(\mathbb{C}^3)$, i.e., maps that take a qubit-operator to a qubit- or to a qutrit-operator can be written as

$$\Lambda = \Lambda^1_{CP} + \Lambda^2_{CP} \circ T \;, \tag{2.23}$$

where Λ^i_{CP} $(i = 1, 2)$ are completely positive maps, and T is the transposition [9, 10]. Therefore, the condition that $(\mathbb{1} \otimes \Lambda)(\varrho)$ be positive for any positive map Λ reduces to

$$\begin{aligned}(\mathbb{1} \otimes \Lambda)(\varrho) &= (\mathbb{1} \otimes \Lambda^{(1)}_{CP})(\varrho) + (\mathbb{1} \otimes \Lambda^{(2)}_{CP})(\mathbb{1} \otimes T)(\varrho) \\ &= (\mathbb{1} \otimes \Lambda^{(1)}_{CP})(\varrho) + (\mathbb{1} \otimes \Lambda^{(2)}_{CP})(\varrho^{\mathrm{pt}}) \geq 0 \;,\end{aligned} \tag{2.24}$$

where $\varrho^{\mathrm{pt}} = (\mathbb{1} \otimes T)(\varrho)$ is called the *partial transpose* of ϱ. Since the $\Lambda^{(i)}_{CP}$ are completely positive, the extended maps $\mathbb{1} \otimes \Lambda^{(i)}_{CP}$ are positive maps. Therefore, $(\mathbb{1} \otimes \Lambda^{(1)}_{CP})(\varrho)$ is non-negative, i.e., it has no negative eigenvalue. The partial transpose ϱ^{pt}, however, is not necessarily a positive operator, since $\mathbb{1} \otimes T$ is *not* a positive map. But, if ϱ is such that its partial transpose is non-negative, then also $(\mathbb{1} \otimes \Lambda^{(2)}_{CP})(\varrho^{\mathrm{pt}})$ is non-negative. In that case, we can conclude that $(\mathbb{1} \otimes \Lambda)(\varrho)$ is non-negative for arbitrary positive maps Λ, and this implies that ϱ is separable. On the other hand, we already know that ϱ is entangled if its partial transpose has at least one negative eigenvalue. Therefore, the spectrum of ϱ^{pt} allows to unambiguously distinguish separable from entangled states in 2×2-dimensional and 2×3-dimensional systems.

In higher dimensional systems, however, (2.23) does not characterize all positive maps anymore, and there are entangled states with positive partial transpose (*ppt*). But also in high-dimensional systems, the so-called *ppt-criterion* is a frequently used separability criterion: despite being only a necessary separability criterion it still detects many entangled states, and it is rather straightforward to implement: a general state of a bipartite system can be expanded in some arbitrary product basis $\varrho = \sum_{ij,kl} \varrho_{ij,kl} \, |\varphi_i\rangle\langle\varphi_j| \otimes |\phi_k\rangle\langle\phi_l|$, and its partial transpose is obtained by a simple rearrangement of matrix elements. $\varrho^{\mathrm{pt}} = (\mathbb{1} \otimes T)(\varrho) = \sum_{ij,kl} \varrho_{ij,lk} \, |\varphi_i\rangle\langle\varphi_j| \otimes |\phi_k\rangle\langle\phi_l|$. One may check that ϱ^{pt} actually depends on the basis with the help of which it is constructed. However, it is only the spectrum of ϱ^{pt} that enters the present separability criterion, and the spectrum does *not* depend on this choice of basis.

Witnesses and Positive Maps

So far, we presented entanglement witnesses and positive maps as independent concepts. And indeed, they do not seem to have too much in common. Entanglement witnesses could be understood in a geometric setting, and positive maps have rather counterintuitive properties. However, these two concepts are more closely related than they seem to be on the first glance.

Let us consider a positive map Λ such that the extended map $\mathbb{1}\otimes\Lambda$ applied to some state ϱ yields a non-positive operator, i.e., Λ is not a completely positive map. Then $(\mathbb{1}\otimes\Lambda)(\varrho)$ has an eigenvector $|\chi\rangle$ with a negative eigenvalue λ,

$$(\mathbb{1}\otimes\Lambda)(\varrho)|\chi\rangle = \lambda|\chi\rangle \ . \tag{2.25}$$

We can now show that the observable $W = (\mathbb{1}\otimes\Lambda^\dagger)(|\chi\rangle\langle\chi|)$ is an entanglement witness. For an arbitrary separable state $|\Phi_s\rangle$, we have

$$\begin{aligned}\langle\Phi_s|W|\Phi_s\rangle &= \mathrm{tr}\Big[\big((\mathbb{1}\otimes\Lambda^\dagger)(|\chi\rangle\langle\chi|)\big)\ |\Phi_s\rangle\langle\Phi_s|\Big] \\ &= \mathrm{tr}\Big[|\chi\rangle\langle\chi|\ \ ((\mathbb{1}\otimes\Lambda)(|\Phi_s\rangle\langle\Phi_s|))\Big] \geq 0 \ ,\end{aligned} \tag{2.26}$$

where the inequality is due to the positivity of Λ, such that $(\mathbb{1}\otimes\Lambda)(|\Phi_s\rangle\langle\Phi_s|)$ is a positive operator. And, indeed, this witness detects ϱ to be entangled:

$$\begin{aligned}\mathrm{tr}(\varrho W) &= \mathrm{tr}\Big[\varrho\ \ \big((\mathbb{1}\otimes\Lambda^\dagger)(|\chi\rangle\langle\chi|)\big)\Big] \\ &= \mathrm{tr}\Big[\big((\mathbb{1}\otimes\Lambda)(\varrho)\big)\ |\chi\rangle\langle\chi|\Big] \\ &= \langle\chi|(\mathbb{1}\otimes\Lambda)(\varrho)|\chi\rangle = \lambda < 0\end{aligned} \tag{2.27}$$

because of the above eigenvector relation.

2.4 Entanglement Monotones and Measures

So far we contented ourselves with a qualitative distinction between separable and entangled states. This, however, does not allow to compare the amount of entanglement of two different states. For such purposes, one would need a quantitative description of entanglement. But the prior definition of entanglement in terms of the nonexistence of a decomposition of a state into product states (cf. (2.4),(2.7)) will not be helpful for finding such a quantification. Therefore, before we can introduce entanglement measures, we need to refine our concept of entanglement.

2.4.1 General Considerations

Let us forget for a while about the prior formal definition and focus more on the interpretation that entanglement is tantamount to correlations that cannot be described in terms of classical probabilities. This allows to arrive at a new concept that allows for a quantitative description of entangled states, and it will still be in agreement with the previous definitions of entanglement and separability.

The idea is to classify all operations that one could apply to a composite quantum system, and that can increase only classical correlations, that is

those that are captured by probabilities p_i as in (2.6). Once this is done, one can make the decrease of correlations under all such operations a defining property of entanglement. Thus, before we can come to the promised quantification of entanglement, we first have to make a significant detour to end up with what is referred to as *local operations and classical communication*.

Quantum Operations

To do so, let us start out with the most general operations. The basic ones that are allowed by the laws of quantum mechanics comprise unitary evolutions

$$\varrho \;\mapsto\; \mathcal{U}\varrho\mathcal{U}^\dagger \;,\; \text{with}\; \mathcal{U}\mathcal{U}^\dagger = \mathcal{U}^\dagger\mathcal{U} = \mathbb{1} \;, \tag{2.28}$$

and v. Neumann measurements in which a quantum state ϱ is projected onto an eigenstate of the associated observable (see Sect. 5.1.3). Let us denote such a complete set of eigenstates $\{|\varphi_i\rangle\}$. Then, the corresponding measurement results in the collapse of ϱ on the state $|\varphi_i\rangle\langle\varphi_i|$, with probability $p_i = \langle\varphi_i|\varrho|\varphi_i\rangle$. That is, on average the state evolves as

$$\varrho \;\mapsto\; \sum_i p_i|\varphi_i\rangle\langle\varphi_i| = \sum_i |\varphi_i\rangle\langle\varphi_i|\varrho|\varphi_i\rangle\langle\varphi_i| \;. \tag{2.29}$$

Thus, a v. Neumann measurement takes a state to a purely probabilistic mixture of the states $|\varphi_i\rangle$, and it destroys all coherences between them completely. Though, one might wonder if one could come up with a slightly less 'invasive' measurement with less dramatic effects. And, indeed, one can do so, if one uses an additional quantum system – often referred to as *ancilla* – lets this ancilla interact with the original system, and finally performs the measurement on the ancilla only. The original state ρ of the combined systems including the ancilla reads

$$\rho = \varrho \otimes |\Psi_a\rangle\langle\Psi_a| \;, \tag{2.30}$$

where $|\Psi_a\rangle$ is an ancilla state. An interaction between the original system and the ancilla results in a global unitary evolution

$$U\big(\varrho \otimes |\Psi_a\rangle\langle\Psi_a|\big)U^\dagger \;, \tag{2.31}$$

and a subsequent measurement in the basis $\{|\Psi_a^{(i)}\rangle\}$ of ancilla states projects this state on

$$\langle\Psi_a^{(i)}|U|\Psi_a\rangle\,\varrho\,\langle\Psi_a|U^\dagger|\Psi_a^{(i)}\rangle = A_i\varrho A_i^\dagger \;, \tag{2.32}$$

with the operators $A_i = \langle\Psi_a^{(i)}|U|\Psi_a\rangle$ that act only on the original system. On average, the state evolves as

$$\varrho \;\mapsto\; \sum_i A_i\varrho A_i^\dagger \;. \tag{2.33}$$

If one utilizes the completeness of the ancilla states $\sum_i |\Psi_a^{(i)}\rangle\langle\Psi_a^{(i)}| = \mathbb{1}$, and subsequently $U^\dagger U = \mathbb{1}$, one can convince oneself that the operators A_i satisfy the resolution of the identity

$$\sum_i A_i^\dagger A_i = \sum_i \langle\Psi_a|U^\dagger|\Psi_a^{(i)}\rangle\langle\Psi_a^{(i)}|U|\Psi_a\rangle = \mathbb{1} \ . \tag{2.34}$$

This property is crucial, since it guarantees the conservation of the trace

$$\mathrm{tr}\sum_i A_i \varrho A_i^\dagger = \mathrm{tr}\sum_i A_i^\dagger A_i \varrho = \mathrm{tr}\varrho \ , \tag{2.35}$$

and, therefore, of probability.

In Sect. 2.3.2, we were discussing positive maps and saw that a trivial extension of a map is not necessarily a positive map again. However, for any map that describes the evolution of a real quantum system, any such extension needs to be positive: if a map acts only on a subcomponent of a system, obviously the positivity of the state of the entire system has to be ensured; this is the case exactly if the extension of the map is positive, i.e., if the map is *completely positive*. Since any trace preserving, completely positive map can always be expressed in the form of (2.33), and, since any map of the form (2.33) is trace preserving and completely positive (see Sect. 5.3.1) [11–13], (2.33) is indeed the most general evolution a quantum state can undergo.

Some Examples

Let us look at a few exemplary cases of operations of the form (2.33) to see how they can affect entanglement properties. First, consider the specific unitary map

$$\mathcal{U} = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)\langle 00| + \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10| \ . \tag{2.36}$$

This is an example of a *global* operation, that is, it cannot be written as $\mathcal{U} = \mathcal{U}_1 \otimes \mathcal{U}_2$, and its implementation requires an interaction between the two individual subsystems. Applying the map to $|00\rangle$ takes this separable state to the entangled state $\mathcal{U}|00\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Thus, such a global operation can indeed create entanglement.

A second example is given by a measurement in the Bell-basis

$$|\varphi_1\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \ , \qquad |\varphi_2\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \ , \tag{2.37}$$

$$|\varphi_3\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \ , \qquad |\varphi_4\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \ , \tag{2.38}$$

followed by a local unitary transformation that is conditioned on the measurement outcome. Let us start again with the separable state $|00\rangle$. Repeated measurements yield the two different outcomes $(|00\rangle + |11\rangle)/\sqrt{2}$, and

$(|00\rangle - |11\rangle)/\sqrt{2}$, with equal probability. A conditioned local unitary operation that is comprised of the identity operation in case of the first outcome, and of $u = |0\rangle\langle 0| - |1\rangle\langle 1|$ on the second subsystem in case of the second, yields the final state $(|00\rangle + |11\rangle)/\sqrt{2}$, which, once again, is entangled. This provides a second example of a global operation that can create entanglement.

We will see later, however, that the situation is different if we restrict ourselves to local operations, or, to *local operations and classical communication* that we introduce now.

Local Operations and Classical Communication

The most general local operation that acts non-trivially only on the first subsystem reads

$$\varrho \to \sum_i (a_i \otimes \mathbb{1})\varrho(a_i^\dagger \otimes \mathbb{1}) \ , \qquad \sum_i a_i^\dagger a_i = \mathbb{1} \ , \tag{2.39}$$

and analogously for operations on the second subsystem alone. Such operations do not induce any correlations: They map product states on product states,

$$\varrho = \rho^{(1)} \otimes \rho^{(2)} \ \mapsto \ \left(\sum_i a_i \rho^{(1)} a_i^\dagger \right) \otimes \rho^{(2)} \ , \tag{2.40}$$

and separable states on separable states

$$\varrho = \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)} \ \mapsto \ \sum_i p_i \Big(\sum_j a_j \rho_i^{(1)} a_j^\dagger \Big) \otimes \rho_i^{(2)} \ . \tag{2.41}$$

The situation changes if one allows for a correlated application of such local operations, where the operation that is applied at a certain instance depends on the outcomes of previous operations:

$$\varrho \mapsto \sum_i (a_i \otimes \mathbb{1})\varrho(a_i^\dagger \otimes \mathbb{1}) \tag{2.42a}$$

$$\mapsto \sum_{ij} (\mathbb{1} \otimes b_{ij})(a_i \otimes \mathbb{1})\varrho(a_i^\dagger \otimes \mathbb{1})(\mathbb{1} \otimes b_{ij}^\dagger) \tag{2.42b}$$

$$\mapsto \sum_{ijp} (c_{ijp} \otimes \mathbb{1})(\mathbb{1} \otimes b_{ij})(a_i \otimes \mathbb{1})\varrho(a_i^\dagger \otimes \mathbb{1})(\mathbb{1} \otimes b_{ij}^\dagger)(c_{ijp}^\dagger \otimes \mathbb{1}) \tag{2.42c}$$

$$\mapsto \sum_{ijp\ldots q} (\mathbb{1} \otimes g_{ijp\ldots q}) \ldots (a_i \otimes \mathbb{1})\varrho(a_i^\dagger \otimes \mathbb{1}) \ldots (\mathbb{1} \otimes g_{ijp\ldots q}^\dagger) \ . \tag{2.42d}$$

In the first step, a local operation has been applied to the first subsystem. This can be understood as an interaction with an ancillary system and a subsequent measurement thereon, as discussed before (2.33). Conditioned on the measurement result that is associated with the collapse on the states $(a_i \otimes \mathbb{1})\varrho(a_i^\dagger \otimes \mathbb{1})$, the local operation associated with the operators b_{ij} is

applied to the second subsystem in a consecutive step. And, conditioned on the outcome of this operation, another local operation is applied to the first subsystem, and so on.

Such operations are called *local operations and classical communication* (LOCC). The idea behind that terminology is that one could imagine two parties that have access to the individual subsystems, and those parties could apply their individual operations to their part of the composite system. But in order to arrive at the above operation, they would need to communicate with each other, i.e., tell the other party their measurement results. This communication, however, can be performed via a classical channel, does not require any quantum nature, and, therefore is referred to as 'classical'.

LOCC operations can take product states to states no more necessarily of product form. Thus, it is possible to create correlations with LOCC operations. Yet, since these correlations are based on the classical exchange of information, they remain correlations of classical nature. Therefore, we can refine our concept of entangled states by requiring [14, 15] that

> an *entanglement monotone* is a quantity that does not increase under *local operations and classical communication*.

Note that this requirement is perfectly compatible with the previous definition of separable and entangled states, since an entangled state cannot be created from a separable one by LOCC alone, but LOCC suffice to transform arbitrary separable states into each other.

Invariance of Entanglement Under Local Unitaries

Monotonicity under LOCC as the defining property of an entanglement monotone is in general difficult to verify. We can, however, formulate a simpler, necessary criterion thereof: among all LOCC operations, the local unitary transformations $\varrho \to \mathcal{U}_1 \otimes \mathcal{U}_2 \varrho \mathcal{U}_1^\dagger \otimes \mathcal{U}_2^\dagger$ are special since they have an inverse that is again LOCC. If one applies some arbitrary local unitary in a first step, and its inverse in a second step, then a monotone $\mathcal{M}$ cannot increase after either step

$$\mathcal{M}(\varrho) \geq \mathcal{M}(\mathcal{U}_1 \otimes \mathcal{U}_2 \ \varrho \ \mathcal{U}_1^\dagger \otimes \mathcal{U}_2^\dagger) \geq \mathcal{M}(\varrho) \ . \tag{2.43}$$

However, because initial and final states are equal, so is their entanglement, and one necessarily concludes that any entanglement monotone is invariant under local unitaries

$$\mathcal{M}(\varrho) = \mathcal{M}(\mathcal{U}_1 \otimes \mathcal{U}_2 \ \varrho \ \mathcal{U}_1^\dagger \otimes \mathcal{U}_2^\dagger) \ . \tag{2.44}$$

This invariance is significantly easier to check than monotonicity under LOCC. However, as mentioned above, it provides only a necessary, but not a sufficient condition.

Schmidt Coefficients and Majorization

Invariance under local unitary transformations is not only a simple test to rule out potential candidates for entanglement monotones as non-monotonous under LOCC, but indeed it has much deeper implications. It implies that any entanglement monotone can be expressed as a function only of invariants under local unitaries. Consequently, if one can identify these invariants, one proceeds a big step forward, toward the systematic construction of entanglement monotones. Although the exhaustive search for such invariants turns out to be a very intricate task for a general state, it has a surprisingly simple answer in the case of pure states of bipartite systems. There, the Schmidt coefficients introduced earlier in Sect. 2.3.2 provide a complete set of invariants, and all entanglement properties can be expressed in terms of only those quantities.

Majorization

One very useful application of the characterization of entanglement in terms of Schmidt coefficients is a simple test that allows to check whether one state $|\Phi\rangle$ can be prepared by LOCC starting from another state $|\Psi\rangle$. This is possible [16, 17] if and only if their Schmidt coefficients, ordered decreasingly (i.e., $\lambda_1 \geq \lambda_2 \geq \ldots$), satisfy the set of inequalities

$$\begin{aligned} \lambda_1^{(\Phi)} &\geq \lambda_1^{(\Psi)} \\ \sum_{i=1}^{2} \lambda_i^{(\Phi)} &\geq \sum_{i=1}^{2} \lambda_i^{(\Psi)} \\ \sum_{i=1}^{3} \lambda_i^{(\Phi)} &\geq \sum_{i=1}^{3} \lambda_i^{(\Psi)} \\ &\vdots \quad \vdots \end{aligned} \tag{2.45}$$

This set of conditions is often expressed in short-hand notation $\boldsymbol{\lambda}^{(\Phi)} \succ \boldsymbol{\lambda}^{(\Psi)}$ in terms of the *Schmidt vectors* $\boldsymbol{\lambda}^{(\Phi)} = [\lambda_1^{(\Phi)}, \lambda_2^{(\Phi)}, \ldots]$ and similarly for $\boldsymbol{\lambda}^{(\Psi)}$, and reads '$\boldsymbol{\lambda}^{(\Phi)}$ majorizes $\boldsymbol{\lambda}^{(\Psi)}$', or, also '$\boldsymbol{\lambda}^{(\Psi)}$ is majorized by $\boldsymbol{\lambda}^{(\Phi)}$'.

An Example

In order to get a bit better idea of how such an LOCC transformation works, let us look at the exemplary case to start out with the state $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and aim at the preparation of the state $|\Phi\rangle = \sqrt{\lambda_1}|00\rangle + \sqrt{\lambda_2}|11\rangle$ using only LOCC operations. This is possible since $\boldsymbol{\lambda}^{(\Phi)}$ actually majorizes $\boldsymbol{\lambda}^{(\Psi)}$. However, this majorization criterion does not give a prescription on how such a transformation can be achieved. Therefore, we will content ourselves with verifying that the LOCC operation that is comprised of the operators

$$\begin{aligned} a_1 &= \sqrt{\lambda_1}|0\rangle\langle 0| + \sqrt{\lambda_2}|1\rangle\langle 1| \,, & b_{11} &= |0\rangle\langle 0| + |1\rangle\langle 1| \,, \\ a_2 &= \sqrt{\lambda_1}|0\rangle\langle 1| + \sqrt{\lambda_2}|1\rangle\langle 0| \,, & b_{21} &= |0\rangle\langle 1| + |1\rangle\langle 0| \,, \end{aligned} \tag{2.46}$$

indeed transforms $|\Psi\rangle$ to $|\Phi\rangle$. First, however, one should verify that the resolutions to identity $\sum_i a_i^\dagger a_i = \mathbb{1}$ and $b_{11}^\dagger b_{11} = b_{21}^\dagger b_{21} = \mathbb{1}$ are given. Then, consider the action of these operators onto the state $|\Psi\rangle$. First the a_i:

$$a_1|\Psi\rangle = \sqrt{\frac{\lambda_1}{2}}|00\rangle + \sqrt{\frac{\lambda_2}{2}}|11\rangle = \frac{1}{\sqrt{2}}|\Phi\rangle, \tag{2.47}$$

$$a_2|\Psi\rangle = \sqrt{\frac{\lambda_1}{2}}|01\rangle + \sqrt{\frac{\lambda_2}{2}}|10\rangle \,. \tag{2.48}$$

The first term is already proportional to $|\Phi\rangle$, so that in the next step the identity operation b_{11} is applied. But, the second term does not have the correct form yet. Here, one needs to transform $|0\rangle$ of the second subsystem into $|1\rangle$ and vice versa, what is exactly what b_{21} does. Thus, one obtains $b_{11}a_1|\Psi\rangle = b_{21}a_2|\Psi\rangle = 1/\sqrt{2}|\Phi\rangle$. So all together, the final state reads

$$\sum_{ij} a_i \otimes b_{ij}|\Psi\rangle\langle\Psi|a_i^\dagger \otimes b_{ij}^\dagger = |\Phi\rangle\langle\Phi| \,. \tag{2.49}$$

And, this is exactly what we were aiming at.

Inequivalent Entanglement Properties

So far, we found a criterion that excludes some quantities from the list of potential quantifiers of entanglement, but does not yet define one *unique* entanglement measure. Whether such a *unique* measure exists is still a subject of debate, and beyond the scope of the present introduction. Let us however briefly illustrate why the characterization of entanglement by a simple scalar quantity might reveal problematic.

The entanglement of a pure state of two qubits is characterized by a single independent Schmidt coefficient due to the normalization of the reduced density matrix. Therefore, the set of majorization conditions (2.45) reduces to its first line. For two arbitrary pure states $|\Psi_1\rangle$ and $|\Psi_2\rangle$ either both Schmidt vectors coincide, i.e., $\boldsymbol{\lambda}_1^{(\Psi_1)} = \boldsymbol{\lambda}_1^{(\Psi_2)}$, or one majorizes the other. That is, there is an unambiguous order of pure states with respect to their degree of entanglement, and any entanglement monotone will respect this order. The situation is different in higher dimensional systems as one can see in the exemplary case of the following two states

$$\begin{aligned} |\Psi_1\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \,, \\ |\Psi_2\rangle &= \sqrt{\frac{3}{5}}|00\rangle + \sqrt{\frac{1}{5}}|11\rangle + \sqrt{\frac{1}{5}}|22\rangle \,. \end{aligned} \tag{2.50}$$

The Schmidt vectors are $\boldsymbol{\lambda}^{(\Psi_1)} = [1/2, 1/2, 0]$ and $\boldsymbol{\lambda}^{(\Psi_2)} = [3/5, 1/5, 1/5]$, respectively, and neither does $\boldsymbol{\lambda}^{(\Psi_1)}$ majorize $\boldsymbol{\lambda}^{(\Psi_2)}$, nor vice versa

$$\begin{aligned} \lambda_1^{(\Psi_1)} &= \tfrac{1}{2} < \tfrac{3}{5} = \lambda_1^{(\Psi_2)} \\ \textstyle\sum_{i=1}^{2} \lambda_i^{(\Psi_1)} &= 1 > \tfrac{4}{5} = \textstyle\sum_{i=1}^{2} \lambda_i^{(\Psi)} \\ \textstyle\sum_{i=1}^{3} \lambda_i^{(\Psi_1)} &= 1 = 1 = \textstyle\sum_{i=1}^{3} \lambda_i^{(\Psi)} \,. \end{aligned}$$

Thus neither can $|\Psi_1\rangle$ be prepared by LOCC from $|\Psi_2\rangle$, nor is there an LOCC operation that takes $|\Psi_2\rangle$ to $|\Psi_1\rangle$. This implies that the two states have non-equivalent entanglement properties, and it is not obvious that either one can be considered more entangled than the other. In particular, the use of different entanglement monotones may lead to contradictory conclusions on the relative entanglement content of both states.

Entanglement Measures

So far, we required only monotonicity under LOCC for a potential entanglement quantifier. There are additional axioms that qualify a monotone as an *entanglement measure*. While there is no general agreement on the complete list of axioms, we list some important ones:

- Mixing two states ϱ and σ probabilistically can increase only classical correlations. Therefore, one expects that a probabilistic mixture $p\varrho + (1-p)\sigma$, $(0 \leq p \leq 1)$, should be no more entangled than the two individual states on average. This implies *convexity* of an entanglement measure, i.e., $\mathcal{M}(p\varrho + (1-p)\sigma) \leq p\mathcal{M}(\varrho) + (1-p)\mathcal{M}(\sigma)$.
- Assume one is given n copies of a state ϱ on $\mathcal{H}_1 \otimes \mathcal{H}_2$. This is equivalent to a single n-fold state $\varrho^{\otimes n} = \varrho \otimes \ldots \otimes \varrho$, and one wants to quantify the entanglement between the subsystems associated with the larger Hilbert spaces $\mathcal{H}_1^{\otimes n}$ and $\mathcal{H}_2^{\otimes n}$. An entanglement monotone that fulfills $\mathcal{M}(\varrho^{\otimes n}) = n\mathcal{M}(\varrho)$ is called *additive*.
- Similarly, one can consider two different states ϱ and σ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ and evaluate the entanglement of the joint state $\varrho \otimes \sigma$ on $\mathcal{H}_1^{\otimes 2} \otimes \mathcal{H}_2^{\otimes 2}$. A monotone $\mathcal{M}$ that satisfies the inequality $\mathcal{M}(\varrho \otimes \sigma) \leq \mathcal{M}(\varrho) + \mathcal{M}(\sigma)$ is called *subadditive*.

2.4.2 Some Specific Monotones and Measures

In the above, we discussed very general properties of entanglement quantifiers. Now we will discuss some more specific entanglement monotones and measures that are frequently used in the literature.

Pure States

We saw earlier that any entanglement monotone or measure can be expressed in terms of invariants under local unitary transformations, and that, in the

case of bipartite pure states, the Schmidt coefficients provide a complete set thereof. Therefore, we can restrict our discussion to functions $\mathcal{F}(\boldsymbol{\lambda})$ of the Schmidt coefficients only. But not every such function is also an entanglement monotone, i.e., non-increasing under LOCC. The following criterion allows to verify this property: A function $\mathcal{F}(\boldsymbol{\lambda})$ is monotonously decreasing under LOCC if $\mathcal{F}$ is invariant under any permutation of the Schmidt coefficients λ_i, and if $\mathcal{F}$ is Schur concave, i.e., [18]

$$(\lambda_1 - \lambda_2)\left(\frac{\partial \mathcal{F}}{\partial \lambda_1} - \frac{\partial \mathcal{F}}{\partial \lambda_2}\right) \leq 0 \tag{2.51}$$

It suffices to express the condition for Schur concavity in terms of only the first two Schmidt coefficients because of the required permutation invariance. We now evaluate this criterion for a few specific monotones and measures.

Entanglement Entropy

The *entanglement entropy*, which is the von Neumann entropy of the reduced density matrix,

$$E(\Psi) = S(\varrho_r) = -\mathrm{tr}\varrho_r \ln \varrho_r = -\sum_i \lambda_i \ln \lambda_i \ , \tag{2.52}$$

is indeed invariant under permutation of the λ_i, satisfies

$$(\lambda_1 - \lambda_2)\left(\frac{\partial S(\rho_r)}{\partial \lambda_1} - \frac{\partial S(\rho_r)}{\partial \lambda_2}\right) = (\lambda_1 - \lambda_2)\ln\frac{\lambda_2}{\lambda_1} \leq 0 \ , \tag{2.53}$$

and thus is a valid entanglement monotone.

Concurrence

Another frequently used monotone is *concurrence* c. For bipartite systems, c is often defined in terms of the local Pauli matrices

$$\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{2.54}$$

represented in a given orthonormal basis $\{|0\rangle,\ |1\rangle\}$ of the factor spaces $\mathcal{H}_1$, and $\mathcal{H}_2$ of $\mathcal{H}$ [19],

$$c(\Psi) = |\langle\Psi^*|\sigma_y \otimes \sigma_y|\Psi\rangle| \ . \tag{2.55}$$

$\langle\Psi^*|$ denotes the complex conjugate of $\langle\Psi|$, with the conjugation performed in the same basis. That is, if $\langle\Psi|$ reads $\langle\Psi| = \sum_{ij}\beta_{ij}\langle ij|$, then $\langle\Psi^*|$ reads $\langle\Psi^*| = \sum_{ij}\beta_{ij}^*\langle ij|$. Equivalently, $\langle\Psi^*|$ is the transpose of $|\Psi\rangle$, whereas $\langle\Psi|$ is the adjoint of $|\Psi\rangle$.

A possible generalization of the above definition for higher dimensional systems (see e.g., [20]) reads [21]

$$c(\Psi) = \sqrt{2(1 - \mathrm{tr}\varrho_r^2)} \,, \tag{2.56}$$

and is equivalent to (2.55), for two-level systems. In terms of the Schmidt coefficients, concurrence reads

$$c(\Psi) = \sqrt{2 \sum_{i \neq j} \lambda_i \lambda_j} \,. \tag{2.57}$$

This is invariant under permutations of the λ_i, and since

$$(\lambda_1 - \lambda_2) \left(\frac{\partial c}{\partial \lambda_1} - \frac{\partial c}{\partial \lambda_2} \right) = \frac{(\lambda_1 - \lambda_2)}{2c} \left(\sum_{i \neq 1} \lambda_i - \sum_{i \neq 2} \lambda_i \right) = - \frac{(\lambda_1 - \lambda_2)^2}{2c} \leq 0 \,, \tag{2.58}$$

concurrence is a valid monotone.

Mixed States

For pure states, we were able to give constructive definitions for some entanglement measures. In the case of mixed states, however, it turns out to be much more involved to find a quantity that is monotonously decreasing under LOCC. The basic difference between mixed and pure states in this specific context is that pure states bear no classical correlations. These need to be distinguished from genuine quantum correlations by a mixed state entanglement monotone.

Negativity

So far, only very few constructively defined quantities were proved to be non-increasing under LOCC. The most prominent example is *negativity* [22]. Earlier, in Sect. 2.3.2, we saw that the partial transpose ϱ^{pt} of a mixed state ϱ can be very helpful to decide on the separability of ϱ: if one of the eigenvalues λ_i of ϱ^{pt} is negative, then ϱ is entangled. This inspired the definition of negativity as

$$\mathcal{N}(\varrho) = \frac{(\sum_i |\lambda_i|) - 1}{2} \,, \tag{2.59}$$

what was proved to be monotonously decreasing under LOCC [22]. If ϱ^{pt} is positive semi-definite, $\mathcal{N}$ vanishes, but takes positive values if ϱ^{pt} has one, or more negative eigenvalues. In comparison to virtually all other mixed state entanglement monotoness, $\mathcal{N}$ can be evaluated easily, since it is an algebraic function of the spectrum of ϱ^{pt}. This advantage, however, comes at the price that negativity assigns non-vanishing entanglement only to those states that are detected via their negative partial transpose. Therefore, much as for the ppt-criterion itself, negativity is fully reliable only for 2×2 or 2×3 system.

Convex Roofs

The failure to detect all entangled states finds its remedy with the so-called convex roof measures. However, the solution to this issue comes at the expense of an additional optimization problem that prevents the explicit algebraic evaluation in most cases. Since any mixed state can be decomposed into a probabilistic mixture of pure states

$$\varrho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i| \ , \tag{2.60}$$

with positive prefactors p_i, one can characterize the entanglement properties of ϱ in terms of those of its pure state components. A very suggestive generalization of a pure state monotone for mixed states is the *average* value $\sum_i p_i \mathcal{M}(\Psi_i)$ of the monotone $\mathcal{M}$. However, a mixed state does not have a unique pure state decomposition, and different decompositions typically yield different average values. A valid mixed state generalization that is monotonously decreasing under LOCC is the infimum over all pure state decompositions, i.e., the minimal average value

$$\mathcal{M}(\varrho) = \inf_{\{p_i, |\Psi_i\rangle\}} \sum_i p_i \mathcal{M}(\Psi_i) \ , \tag{2.61}$$

what is called the *convex roof*. To solve the optimization problem implicit in the convex roof definition (2.61), one needs a systematic way to explore all pure state decompositions of ϱ. Given the eigenstates $|\Phi_j\rangle$ of ϱ, together with the associated eigenvalues μ_i, any linear combination of the eigenstates

$$\sqrt{p_i}|\Psi_i\rangle = \sum_j V_{ij}\sqrt{\mu_j}|\Phi_j\rangle \ , \tag{2.62}$$

defines another valid decomposition [23], provided $\sum_k V_{ik}^\dagger V_{kj} = \delta_{jk}$, i.e., for a left-unitary coefficient matrix V (with adjoint $V^\dagger$):

$$\begin{aligned} \sum_i p_i |\Psi_i\rangle\langle\Psi_i| &= \sum_{ijk} V_{ij}\sqrt{\mu_j}|\Phi_j\rangle\langle\Phi_k|\sqrt{\mu_k}V_{ik}^* \\ &= \sum_{ijk} V_{ki}^\dagger V_{ij}\sqrt{\mu_j\mu_k}|\Phi_j\rangle\langle\Phi_k| \\ &= \sum_{jk} \delta_{jk}\sqrt{\mu_j\mu_k}|\Phi_j\rangle\langle\Phi_k| \\ &= \sum_j \mu_j |\Phi_j\rangle\langle\Phi_j| = \varrho \ ; \end{aligned} \tag{2.63}$$

and *any* pure state decomposition of ϱ can be obtained in this fashion [23].

Concurrence of Mixed States

With this characterization of pure state decompositions at hand, we can now focus on the evaluation of concurrence for mixed states. So far, concurrence is virtually the only quantity for which the convex roof can be evaluated algebraically. Later in Sect. 2.4.2, we will see that also the convex roof of the entanglement entropy has an algebraic solution. This solution, however follows from the known solution for concurrence.

A crucial property of concurrence in contrast to other monotones is the homogeneity,

$$c(\eta|\Psi\rangle\langle\Psi|) = \eta\, c(|\Psi\rangle) \ , \text{ for } \eta \geq 0, \tag{2.64}$$

which allows to rewrite the convex roof expression above as

$$c(\varrho) = \inf_{\{|\psi_i\rangle\}} \sum_i c(\psi_i) \ , \tag{2.65}$$

where everything is expressed in terms of *subnormalized* states $|\psi_i\rangle = \sqrt{p_i}|\Psi_i\rangle$, and the probabilities p_i do not enter explicitly any more.

This allows to reformulate (2.61) in the following closed form

$$\begin{aligned} c(\varrho) &= \inf_{\{|\psi_i\rangle\}} \sum_i c(\psi_i) \\ &= \inf_{\{|\psi_i\rangle\}} \sum_i |\langle\psi_i^*|\sigma_y \otimes \sigma_y|\psi_i\rangle| \\ &= \inf_V \sum_i \Big| \sum_{jk} V_{ij} \langle\phi_j^*|\sigma_y \otimes \sigma_y|\phi_k\rangle V_{ki}^T \Big| \\ &= \inf_V \sum_i \Big| [V\tau V^T]_{ii} \Big| \ , \end{aligned} \tag{2.66}$$

where we used (2.55) and (2.62). In the last line, we introduced a short-hand notation, where τ is a complex symmetric matrix, $\tau = \tau^T$, with elements

$$\tau_{ij} = \langle\phi_i^*|\sigma_y \otimes \sigma_y|\phi_j\rangle \ . \tag{2.67}$$

Equation (2.66) resembles the diagonalization of a hermitean matrix H through a unitary transformation $\mathcal{U}H\mathcal{U}^\dagger$, where $\mathcal{U}$ is unitary. The difference resides, however, in the fact that τ is symmetric and not hermitean, and that the transpose of a unitary, respectively left unitarys, enters instead of its adjoint. But also a symmetric matrix can be diagonalized in a similar fashion. Already earlier, in (2.13) we have been invoking the singular value decomposition of a matrix. It stated that any matrix A could be diagonalized with two unitary transformations u_1 and u_2 as $u_1 A u_2$. This, of course, also holds for the particular case of a symmetric matrix that we are facing here. However, in this specific case, u_2 is equal to u_1^T. Therefore, we can rephrase the infimum to be evaluated as

$$c(\varrho) = \inf_V \sum_i \left| [VU^\dagger U \tau U^T U^* V^T]_{ii} \right| = \inf_{\tilde{V}} \sum_i \left| [\tilde{V} \tau_d \tilde{V}^T]_{ii} \right| , \tag{2.68}$$

where $\tilde{V} = VU^\dagger$, and $\tau_d = \mathcal{U}\tau\mathcal{U}^T = \mathrm{diag}[\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{S}_4]$ is the diagonal form of τ. The order of the diagonal elements is not determined and can be chosen arbitrarily. But in the following, we will use the convention that $\mathcal{S}_1$ is the largest of all diagonal entries.

With the diagonal form τ_d of τ, we have simplified the problem a lot: instead of 20 real parameter that characterize a general complex symmetric matrix, we are left with only four real parameters. But it is still not straightforward to derive an optimal matrix $\tilde{V}$ that achieves the infimum. Instead of a systematic derivation, we are going to take an Ansatz that eventually will turn out to do the job. Let us take $\tilde{V}$ equal to $\mathcal{V}$ with

$$\mathcal{V} = \frac{1}{2} \begin{bmatrix} 1 & e^{i\varphi_2} & e^{i\varphi_3} & e^{i\varphi_4} \\ 1 & e^{i\varphi_2} & -e^{i\varphi_3} & -e^{i\varphi_4} \\ 1 & -e^{i\varphi_2} & e^{i\varphi_3} & -e^{i\varphi_4} \\ 1 & -e^{i\varphi_2} & -e^{i\varphi_3} & e^{i\varphi_4} \end{bmatrix} , \tag{2.69}$$

where we still have the free phases φ_2, φ_3, and φ_4 that we can adjust. With this choice, we obtain

$$\sum_i \left| \mathcal{V} \tau_d \mathcal{V}^T \right| = \left| \mathcal{S}_1 + \sum_{i>1} e^{2i\varphi_i} \mathcal{S}_i \right| . \tag{2.70}$$

Now, we can minimize this expression by proper choices of the free phases, what is most conveniently done by distinguishing two cases. In the former case, where $\mathcal{S}_1 \geq \sum_{i>1} \mathcal{S}_i$, it is optimal to take $\varphi_2 = \varphi_3 = \varphi_4 = \pi/2$, what leads to $\sum_i |\mathcal{V}\tau_d\mathcal{V}^T| = \mathcal{S}_1 - \sum_{i>1} \mathcal{S}_i$. In the latter case, $\mathcal{S}_1 < \sum_{i>1} \mathcal{S}_i$, one can always find a choice of phases such that $\sum_i |\mathcal{V}\tau_d\mathcal{V}^T| = 0$, as depicted in Fig. 2.2. That is, we found a pure state decomposition in which the average

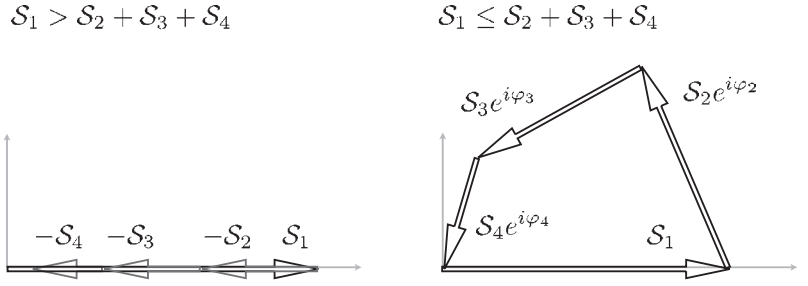

Fig. 2.2. Schematic drawing of the singular values $\mathcal{S}_i$ added up with adjustable phases $e^{2i\varphi_i}$ in the complex plane. If $\mathcal{S}_1 > \sum_{i>1} \mathcal{S}_i$, as depicted on the left, the optimal choice to minimize $|\mathcal{S}_1 + \sum_{i>1} \mathcal{S}_i e^{2i\varphi_i}|$ of the phases is $\varphi_i = \pi/2$. If, on the other hand, $\mathcal{S}_1 < \sum_{i>1} \mathcal{S}_i$ as depicted on the right, then one can always find phases φ_i such that $|\mathcal{S}_1 + \sum_{i>1} \mathcal{S}_i e^{2i\varphi_i}|$ vanishes

concurrence reads $\max(\mathcal{S}_1 - \sum_{i>1} \mathcal{S}_i,\ 0)$. However, we still do not know, if this is optimal, or if there are decompositions that yield a smaller value.

For answering this question, we can restrict ourselves to the case $\mathcal{S}_1 \geq \sum_{i>1} \mathcal{S}_i$. In the other case, we found a vanishing value for concurrence, which obviously is the infimum, since concurrence cannot be negative. Now, let us start out not with $\tilde{\tau} = \mathcal{V}\tau_d\mathcal{V}^T$ with the choice $\varphi_2 = \varphi_3 = \varphi_4 = \pi/2$ that we found optimal above. We now show that there is no left-unitary W that could yield a smaller value than what we have found so far.

$$\begin{aligned}
\sum_i \Big| [W\tau_d W^T]_{ii} \Big| &= \sum_i \Big| \sum_j W_{ij}^2 \mathcal{S}_j \Big| \\
&= \sum_i \Big| W_{i1}^2 \mathcal{S}_1 + \sum_{j>1} W_{ij}^2 \mathcal{S}_j \Big| \\
&\geq \sum_i \Big(\Big| W_{i1}^2 \Big| \mathcal{S}_1 - \Big| \sum_{j>1} W_{ij}^2 \mathcal{S}_j \Big| \Big) \\
&= \mathcal{S}_1 - \sum_i \Big| \sum_{j>1} W_{ij}^2 \mathcal{S}_j \Big| \\
&\geq \mathcal{S}_1 - \sum_i \sum_{j>1} \Big| W_{ij} \Big|^2 \mathcal{S}_j \\
&= \mathcal{S}_1 - \sum_{j>1} \mathcal{S}_j \ ,
\end{aligned} \tag{2.71}$$

where going from the second to the third line we used $|a+b| \geq |a| - |b|$ with $a = W_{i1}^2 \mathcal{S}_1$, and $b = \sum_{j>1} W_{ij}^2 \mathcal{S}_j$, and in the fourth line, we used the left-unitarity condition of W, i.e., $\sum_i |W_{ij}|^2 = 1$. We obtained the fifth line using $-|\sum a_j| \geq -\sum |a_j|$, with $a_j = W_{ij}^2 \mathcal{S}_j$, and the last line followed again from the left-unitarirty of W. Thus, we found the algebraic solution

$$c(\varrho) = \max(\mathcal{S}_1 - \sum_{i>1} \mathcal{S}_i, 0) \tag{2.72}$$

for the concurrence of an arbitrary mixed state of a bipartite two-level system.

Entanglement of Formation of Mixed States

With this solution for concurrence, we can now proceed and consider entanglement of formation, which is the convex roof extension of the entanglement entropy. Here we will make use of the fact that for *pure* states in bipartite two-level systems, there is only one independent Schmidt coefficient, since they sum up to unity. Therefore, one can determine both Schmidt coefficients in terms of the concurrence:

$$\lambda_\pm = \frac{1 \pm \sqrt{1 - c^2}}{2} \ . \tag{2.73}$$

And, since the entanglement entropy is a function of $\boldsymbol{\lambda}$, it can also be expressed in terms of concurrence via

$$\begin{aligned} E(\Psi) &= -\frac{1+\sqrt{1-c^2}}{2}\ln\frac{1+\sqrt{1-c^2}}{2} - \frac{1-\sqrt{1-c^2}}{2}\ln\frac{1-\sqrt{1-c^2}}{2} \\ &\equiv \mathcal{E}(c)\ , \end{aligned} \tag{2.74}$$

where we introduced the function $\mathcal{E}(c)$. One easily convinces oneself that $\mathcal{E}(c)$ is monotonously increasing $\partial\mathcal{E}(c)/\partial c \geq 0$, and convex $\partial^2\mathcal{E}(c)/\partial c^2 \geq 0$, for $c \geq 0$. Convexity can equivalently be expressed as $\sum_i p_i\mathcal{E}(q_i) \geq \mathcal{E}(\sum_i p_i q_i)$. With the help of these properties, we arrive at the following reasoning:

$$\begin{aligned} E(\varrho) &= \inf \sum_i p_i E(\Psi_i) \\ &= \inf \sum_i p_i \mathcal{E}(c(\Psi_i)) \\ &\geq \inf \mathcal{E}(\sum_i p_i c(\Psi_i)) \\ &= \mathcal{E}(\inf \sum_i p_i c(\Psi_i)) \\ &= \mathcal{E}(c(\varrho))\ . \end{aligned} \tag{2.75}$$

Here, in going from the second to the third line, we used the convexity of $\mathcal{E}$, and from the third to the fourth its monotonicity. Thus, we found that entanglement of formation is bounded from below by $\mathcal{E}(c(\varrho))$. But, we are close to seeing that this is indeed not only a bound but rather the exact result. The crucial feature here is the fact that there is not a single optimal decomposition of a mixed state ϱ into pure states that yields the actual value of concurrence, but there is actually a continuum of optimal decompositions. And, in particular, there is one, $\varrho = \sum_i \tilde{p}_i |\tilde{\Psi}_i\rangle\langle\tilde{\Psi}_i|$ in which all pure states do have the same value of concurrence, i.e., $c(\tilde{\Psi}_i) = c(\varrho)$ [19]. With the help of this particular decomposition, we can now show that $\mathcal{E}(c(\varrho))$ is not only a lower bound on entanglement of formation, but actually its exact value: due to its definition as convex roof, $E(\varrho)$ is bounded from above by its average value evaluated in any decomposition – in particular $\{\tilde{p}_i, |\Psi_i\rangle\}$, i.e., $E(\varrho) \leq \sum_i \tilde{p}_i \mathcal{E}(c(\tilde{\Psi}_i))$. Now, we can replace $c(\tilde{\Psi}_i)$ by $c(\varrho)$, so that we end up with $E(\varrho) \leq \sum_i \tilde{p}_i \mathcal{E}(c(\varrho))$. And, finally, since the probabilities add up to 1, we arrive at the conclusion that entanglement of formation is bounded from above by $\mathcal{E}(c(\varrho))$. Since we found above in (2.75) that it is also bounded from below by the same quantity, we necessarily need to conclude that these two quantities coincide:

$$E(\varrho) = \mathcal{E}(c(\varrho))\ . \tag{2.76}$$

Therefore, once one has evaluated concurrence for a mixed state – what can be done algebraically (2.72) – one can easily also obtain entanglement of formation.

References

1. A. Einstein, B. Podolsky, and N. Rosen: *Can quantum-mechanical description of physical reality be considered complete?*. Phys. Rev. **47**, 777 (1935)
2. R. F. Werner: *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*. Phys. Rev. A **40**, 4277 (1989)
3. E. Schmidt: *Zur Theorie der linearen und nichtlinearen Integralgleichungen*. Math. Ann. **63**, 433 (1907)
4. P. A. Horn and C. R. Johnson: *Matrix Analysis* (Cambridge University Press, New York 1985)
5. M. Horodecki, P. Horodecki, and R. Horodecki: *Separability of mixed states: necessary and sufficient conditions*. Phys. Lett. A **223**, 1 (1996)
6. B. M. Terhal: *Bell inequalities and the separability criterion*. Phys. Lett. A **271**, 319 (2001)
7. M. Reed and B. Simon: *Analysis of Operators*. (Elsevier, Amsterdam 1978)
8. A. Peres: *Separability criterion for density matrices*. Phys. Rev. Lett. **77**, 1413 (1996)
9. E. Størmer: *Positive linear maps of operator algebras*. Acta. Math. **110**, 233 (1963)
10. S. L. Woronowicz: *Positive maps of low dimensional matrix algebras*. Rep. Math. Phys. **10**, 165 (1976)
11. K. Kraus: *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, New York 1983)
12. W. F. Stinespring: *Positive functions on c*-algebras*. Proc. Am. Math. Soc. **6**, 211 (1955)
13. Man-Duen Choi: *Completely positive linear maps on complex matrices*. Linear Algebra Appl. **10**, 285 (1975)
14. V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight: *Quantifying entanglement*. Phys. Rev. Lett. **78**, 2275 (1997)
15. G. Vidal. *Entanglement monotones*. J. Mod. Opt. **47**, 355 (2000)
16. M. A. Nielsen: *Conditions for a class of entanglement transformations*. Phys. Rev. Lett. **83**, 436 (1999)
17. M. A. Nielsen and G. Vidal: *Majorization and the interconversion of bipartite states*. Quant. Inf. Comp. **1**, 76 (2001)
18. T. Ando: *Majorization, doubly stochastic matrices, and comparison of eigenvalues*. Lin. Alg. Appl. **118**, 163 (1989)
19. W. K. Wootters: *Entanglement of formation of an arbitrary state of two qubits*. Phys. Rev. Lett. **80**, 2245 (1998)
20. A. Uhlmann: *Fidelity and concurrence of conjugated states*. Phys. Rev. A **62**, 032307 (2000)
21. P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn: *Universal state inversion and concurrence in arbitrary dimensions*. Phys. Rev. A **64**, 042315 (2001)
22. G. Vidal and R. F. Werner: *Computable measure of entanglement*. Phys. Rev. A **65**, 032314 (2002)
23. E. Schrödinger. *Probability relations between separated systems*. Proc. Cambridge Philos. Soc. **32**, 446 (1936)