Quantum Information and Computation, Vol. 7, No. 1 (2007) 001–051

AN INTRODUCTION TO ENTANGLEMENT MEASURES

MARTIN B. PLENIO and SHASHANK VIRMANI
Blackett Laboratory, Imperial College London
Prince Consort Rd, London SW7 2BW, UK
and
Institute for Mathematical Sciences, Imperial College London
53 Prince's Gate, Exhibition Rd, London, SW7 2PG, UK

Received February 17, 2006
Revised May 31, 2006

We review the theory of entanglement measures, concentrating mostly on the finite dimensional two-party case. Topics covered include: single-copy and asymptotic entanglement manipulation; the entanglement of formation; the entanglement cost; the distillable entanglement; the relative entropic measures; the squashed entanglement; log-negativity; the robustness monotones; the greatest cross-norm; uniqueness and extremality theorems. Infinite dimensional systems and multi-party settings will be discussed and an extensive list of open research questions will be presented.

Keywords:

Communicated by: I Cirac & M Mosca

1 Introduction

The concept of *entanglement* has played a crucial role in the development of quantum physics. In the early days entanglement was mainly perceived as the qualitative feature of quantum theory that most strikingly distinguishes it from our classical intuition. The subsequent development of Bell's inequalities has made this distinction quantitative, and therefore rendered the non-local features of quantum theory accessible to experimental verification [1, 2, 3]. Bell's inequalities may indeed be viewed as an early attempt to quantify the quantum correlations that are responsible for the counterintuitive features of quantum mechanically entangled states. At the time it was almost unimaginable that such quantum correlations could be created in well controlled environments between distinct quantum systems. However, the technological progress of the last few decades means that we are now able to coherently prepare, manipulate, and measure individual quantum systems, as well as create controllable quantum correlations. In parallel with these developments, quantum correlations have come to be recognized as a novel resource that may be used to perform tasks that are either impossible or very inefficient in the classical realm. These developments have provided the seed for the development of modern quantum information science.

Given the new found status of entanglement as a resource it is quite natural and important to discover the mathematical structures underlying its theoretical description. We will see that such a description aims to provide answers to three questions about entanglement, namely

(1) its characterisation, (2) its manipulation and, (3) its quantification.

In the following we aim to provide a tutorial overview summarizing results that have been obtained in connection with these three questions. We will place particular emphasis on developments concerning the *quantification* of entanglement, which is essentially the theory of *entanglement measures*. We will discuss the motivation for studying entanglement measures, and present their implications for the study of quantum information science. We present the basic principles underlying the theory and main results including many useful entanglement monotones and measures as well as explicit useful formulae. We do not, however, present detailed technical derivations. The majority of our review will be concerned with entanglement in bipartite systems with finite and infinite dimensional constituents, for which the most complete understanding has been obtained so far. The multi-party setting will be discussed in less detail as our understanding of this area is still far from satisfactory.

It is our hope that this work will give the reader a good first impression of the subject, and will enable them to tackle the extensive literature on this topic. We have endeavoured to be as comprehensive as possible in both covering known results and also in providing extensive references. Of course, as in any such work, it is inevitable that we will have made several oversights in this process, and so we encourage the interested reader to study various other interesting review articles (e.g. [4, 5, 6, 7, 8, 9]) and of course the original literature.

2 Foundations

What is entanglement? – Any study of entanglement measures must begin with a discussion of what entanglement *is*, and how we actually *use* it. In the following we will adopt a highly operational point of view. Then the usefulness of entanglement emerges because it allows us to overcome a particular constraint that we will call the *LOCC constraint* - a term that we will shortly explain. This restriction has both technological and fundamental motivations, and arises naturally in many explicit physical settings involving quantum communication across a distance.

We will consider these motivations in some detail, starting with the technological ones. In any quantum communication experiment we would like to be able to distribute quantum particles across distantly separated laboratories. Perfect quantum communication is essentially equivalent to perfect entanglement distribution. If we can transport a qubit without any decoherence, then any entanglement shared by that qubit will also be distributed perfectly. Conversely, if we can distribute entangled states perfectly then with a small amount of classical communication we may use teleportation [10] to perfectly transmit quantum states. However, in any forseeable experiment involving these processes, the effects of noise will inevitably impair our ability to send quantum states over long distances.

One way of trying to overcome this problem is to distribute quantum states by using the noisy quantum channels that are available, but then to try and combat the effects of this noise using higher quality local quantum processes in the distantly separated labs. Such local quantum operations ('LO') will be much closer to ideal, as they can be performed in well-controlled environments without the decoherence induced by communication over long-distances. However, there is no reason to make the operations of separated labs totally independent. Classical communication ('CC') can essentially be performed perfectly using standard telecom technologies, and so we may also use such communication to coordinate the quantum actions of the different labs (see fig. 1). It turns out that the ability to perform classical communication is vital for many quantum information protocols - a prominent example being teleportation. These considerations are the technological reasons for the key status of the *Local Operations and Classical Communication* 'LOCC' paradigm, and are a major motivation for their study. However, for the purposes of this article, the fundamental motivations

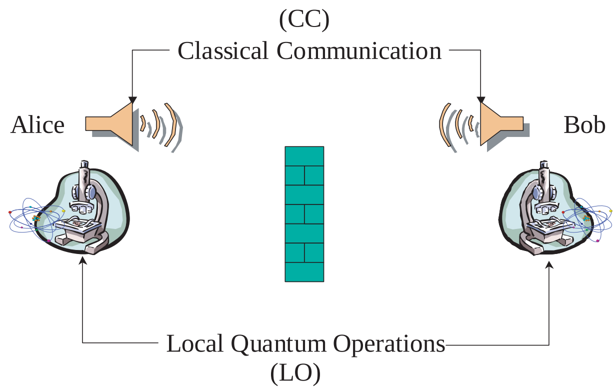

Fig. 1. In a standard quantum communication setting two parties Alice and Bob may perform any generalized measurement that is localized to their laboratory and communicate classically. The brick wall indicates that no quantum particles may be exchanged coherently between Alice and Bob. This set of operations is generally referred to as LOCC.

of the LOCC paradigm are perhaps more important than these technological considerations. We have loosely described entanglement as the *quantum correlations* that can occur in many-party quantum states. This leads to the question - how do we define quantum correlations, and what differentiates them from *classical correlations*? The distinction between 'quantum' effects and 'classical' effects is frequently a cause of heated debate. However, in the context of quantum information a precise way to define classical correlations is via LOCC operations. Classical correlations can be defined as those that can be generated by LOCC operations. If we observe a quantum system and find correlations that cannot be simulated classically, then we usually attribute them to quantum effects, and hence label them *quantum correlations* [11]. So suppose that we have a noisy quantum state, and we process it using LOCC operations. If in this process we obtain a state that can be used for some task that cannot be simulated by classical correlations, such as violating a Bell inequality, then we must not attribute these effects to the LOCC processing that we have performed, but to quantum correlations that were *already present* in the initial state, even if the initial state was quite noisy. This is an extremely important point that is at the heart of the study of entanglement.

It is the constraint to LOCC-operations that elevates entanglement to the status of a resource. Using LOCC-operations as the only other tool, the inherent quantum correlations of entanglement are required to implement general, and therefore nonlocal, quantum operations on two or more parties [13, 14]. As LOCC-operations alone are insufficient to achieve these transformations, we conclude that entanglement may be defined as the sort of correlations that may not be created by LOCC alone.

Allowing classical communication in the set of LOCC operations means that they are not completely local, and can actually have quite a complicated structure. In order to understand this structure more fully, we must first take a closer look at the notion of general quantum operations and their formal description.

Quantum Operations – In quantum information science much use is made of so-called 'generalised measurements' (see [10] for a more detailed account of the following basic principles). It should be emphasized that such generalised measurements do not go beyond standard quantum mechanics. In the usual approach to quantum evolution, a system is evolved according to unitary operators, or through collapse caused by projective measurements. However, one may consider a more general setting where a system evolves through interactions with other quantum particles in a sequence of three steps: (1) first we first add ancilla particles, (2) then we perform joint unitaries and measurements on both the system and ancillae, and finally (3) we discard some particles on the basis of the measurement outcomes. If the ancillae used in this process are originally uncorrelated with the system, then the evolution can be described by so-called *Kraus operators*. If one retains total knowledge of the outcomes obtained during any measurements, then the state corresponding to measurement outcomes i occurs with probability $p_i = tr\{A_i\rho_{in}A_i{}^\dagger\}$ and is given by

$$\rho_i = \frac{A_i\rho_{in}A_i{}^\dagger}{tr\{A_i\rho_{in}A_i{}^\dagger\}} \tag{1}$$

where ρ_{in} is the initial state and the A_i are matrices known as *Kraus* operators (see part (a) of Fig. 2 for illustration). The normalisation of probabilities implies that Kraus operators must satisfy $\sum_i A_i{}^\dagger A_i = \mathbb{1}$. In some situations, for example when a system is interacting with an environment, all or part of the measurement outcomes might not be accessible. In the most extreme case this corresponds to the situation where the ancilla particles are being traced out. Then the map is given by

$$\sigma = \sum_i A_i\rho_{in}A_i^\dagger \tag{2}$$

which is illustrated in part (b) of Fig. (1). Such a map is often referred to as a *trace preserving*

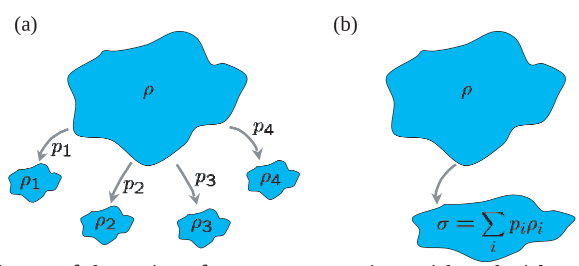

Fig. 2. Schematic picture of the action of quantum operations with and without sub-selection (eqs. (1) and (2) respectively) shown in part (a) and part (b) respectively.

quantum operation, whereas operations in which measurement outcomes are retained are sometimes referred to as *measuring* quantum operations (or sometimes also *selective* quantum operations, or *stochastic* quantum operations, depending upon the context). Conversely, it can be shown (see e.g. [10]) that for *any* set of linear operators A_i satisfying $\sum_i A_i^\dagger A_i = \mathbb{1}$ we can find a process, composed of the addition of ancillae, joint unitary evolution, and von-Neumann measurements, that leads to eq. (1). In trace preserving operations the A_i should strictly all be matrices of the same dimensions, however, if knowledge of outcomes is retained, then different A_i may have different dimensions. Having summarized the basic ingredients of generalised quantum operations, we are in a position to consider approaches that may be taken to determine which operations are implementable by LOCC. The LOCC constraint is illustrated in figure 1. In general this set of operations is quite complicated. Alice and Bob may communicate classically before or after any given round of local actions, and hence in any given round their actions may depend upon the outcomes of previous measuring operations. As a consequence of this complexity, there is no known simple characterisation of the LOCC operations. This has motivated the development of larger classes of operations that can be more easily characterised, while still retaining a considerable element of LOCC-ality. One of the most important such classes is the set of *separable operations*. These are the operations that can be written in terms of Kraus operators with a *product* decomposition:

$$\rho_k = \frac{A_k \otimes B_k \rho_{in} A_k^\dagger \otimes B_k^\dagger}{tr A_k \otimes B_k \rho_{in} A_k^\dagger \otimes B_k^\dagger} \tag{3}$$

such that $\sum_k A_k^\dagger A_k \otimes B_k^\dagger B_k = \mathbb{1} \otimes \mathbb{1}$. Clearly, any LOCC operation can be cast in the form of separable operation, as the local Kraus operators corresponding to the individual actions of Alice and Bob can be joined into product Kraus operators. However, it is remarkable that the converse is *not* true. This was first demonstrated in [16], where an example task of a separable operation is presented that cannot be implemented using LOCC actions - the example presented there requires a finite amount of quantum communication to implement it, even though the operation is itself separable.

It is nevertheless convenient from a mathematical point of view to work with separable operations, as optimising a given task using separable operations provides strong bounds on what may be achieved using LOCC. Sometimes this process can even lead to tight results - one may try to show whether the optimal separable operation may in fact be also implemented using LOCC, and this can often, but not always, be guaranteed in the presence of symmetries (see e.g. [17, 15] and refs. therein). Even more general classes of operations such as positive partial transpose preserving operations (PPT) [a] may also be used in the study of entanglement as they have the advantage of a very compact mathematical characterization [17, 18, 19].

After this initial discussion of quantum operations and the LOCC constraint we are now in a position to consider in more detail the basic properties of entanglement.

Basic properties of entanglement – Following our discussion of quantum operations and their natural constraint to local operations and classical communication, we are now in a position to establish some basic facts and definitions regarding entangled states. Given the wide range of tasks that exploit entanglement one might try to define entanglement as 'that

[a] The class of PPT operations was proposed by Rains [40, 17], and is defined as the set of completely positive operations Φ such that $\Gamma_B \circ \Phi \circ \Gamma_B$ is also completely positive, where Γ_B corresponds to transposition of *all* of Bob's particles, including ancillas. One can also consider transposition only of those particles belonging to Bob that undergo the operation Φ. However, we believe that this does not affect the definition. It is also irrelevant whether the transposition is taken over Alice or Bob, and so one may simply assert that $\Gamma \circ \Phi \circ \Gamma$ must be completely positive, where Γ is the transposition of one party. It can be shown that the PPT operations are precisely those operations that preserve the set of PPT states. Hence the set of non-PPT operations includes any operation that creates a free (non-bound) entangled state out of one that is PPT. Hence PPT operations correspond to some notion of locality, and in contrast to separable operations it is relatively easy to check whether a quantum operation is PPT [17].

property which is exploited in such protocols'. However, there is a whole range of such tasks, with a whole range of possible measures of success. This means that situations will almost certainly arise where a state ρ_1 is better than another state ρ_2 for achieving one task, but for achieving a different task ρ_2 is better than ρ_1. Consequently using a task-based approach to quantifying entanglement will certainly not lead to a single unified perspective. However, despite this problem, it is possible to assert some general statements which are valid regardless of what your favourite use of entanglement is, as long as the key set of 'allowed' operations is the LOCC class. This will serve us a guide as to how to approach the quantification of entanglement, and so we will discuss some of these statements in detail:

• *Separable states contain no entanglement.*

A state $\rho_{ABC...}$ of many parties $A, B, C, ...$ is said to be *separable* [20], if it can be written in the form

$$\rho_{ABC...} = \sum_i p_i \; \rho_A^i \otimes \rho_B^i \otimes \rho_C^i \otimes ... \tag{4}$$

where p_i is a probability distribution. These states can trivially be created by LOCC - Alice samples from the distribution p_i, informs all other parties of the outcome i, and then each party X locally creates ρ_X^i and discards the information about the outcome i. As these states can be created from scratch by LOCC they trivially satisfy a local hidden variables model and all their correlations can be described classically. Hence, it is quite reasonable to state that separable states contain no entanglement.

• *All non-separable states allow some tasks to be achieved better than by LOCC alone, hence all non-separable states are entangled.*

For a long time the quantum information community has used a 'negative' characterization of the term entanglement essentially defining entangled states as those that cannot be created by LOCC alone. On the other hand, it can be shown that a quantum state ρ may be generated perfectly using LOCC if and only if it is separable. Of course this is a task that becomes trivially possible by LOCC when the state ρ has been provided as a non-local resource in the first place. More interestingly, it has been shown recently that for any non-separable state ρ, one can find another state σ whose teleportation fidelity may be enhanced if ρ is also present [21, 23, 22]. This is interesting as it allows us to positively characterize non-separable states as those possessing a useful resource that is not present in separable states. This hence justifies the synonymous use of the terms *non-separable* and *entangled.*

• *The entanglement of states does not increase under LOCC transformations.*

Given that by LOCC we can only create separable, ie non-entangled states, this immediately implies the statement that LOCC cannot create entanglement from an unentangled state. Indeed, we even have the following stronger fact. Suppose that we know that a quantum state ρ can be transformed with certainty to another quantum state σ using LOCC operations. Then anything that we can do with σ and LOCC operations we can also achieve with ρ and LOCC operations. Hence the utility of quantum states cannot increase under LOCC operations [24, 25, 26, 4], and one can rightfully state that ρ is at least as entangled as σ.

• *Entanglement does not change under Local Unitary operations.*

This property follows from the previous one because local unitaries can be inverted by local unitaries. Hence, by the non-increase of entanglement under LOCC, two states related by local unitaries have an equal amount of entanglement.

• *There are maximally entangled states.*

Now we have a notion of which states are entangled and are also able, in some cases, to assert that one state is more entangled than another. This naturally raises the question whether there is a *maximally entangled state*, i.e. one that is more entangled than all others. Indeed, at least in two-party systems consisting of two fixed d-dimensional sub-systems (sometimes called qudits), such states exist. It turns out that any pure state that is local unitarily equivalent to

$$|\psi_d^+\rangle = \frac{|0,0\rangle + |1,1\rangle + .. + |d-1,d-1\rangle}{\sqrt{d}}$$

is maximally entangled. This is well justified, because as we shall see in the next subsection, any pure or mixed state of two d-dimensional systems can be prepared from such states with certainty using only LOCC operations. We shall later also see that the non-existence of an equivalent statement in multi-particle systems is one of the reasons for the difficulty in establishing a theory of multi-particle entanglement.

The above considerations have given us the extremes of entanglement - as long as we consider LOCC as our set of available operations, separable states contain zero entanglement, and we can identify certain states that have maximal entanglement. They also suggest that we can impose some form of ordering - we may say that state ρ is more entangled than a state σ if we can perform the transformation $\rho \rightarrow \sigma$ using LOCC operations. A key question is whether this method of ordering gives a partial or total order? To answer this question we must try and find out when one quantum state may be transformed to another using LOCC operations. Before we move on to the discussion of entanglement measures we will consider this question in more detail in the next part.

Note that the notion that '*entanglement does not increase under LOCC*' is implicitly related to our restriction of quantum operations to LOCC operations - if other restrictions apply, weaker or stronger, then our notion of 'more entangled' is likely to also change.

3 Local Manipulation of Quantum States

Manipulation of single bi-partite states – In the previous section we indicated that for bi-partite systems there is a notion of maximally entangled states that is independent of the specific quantification of entanglement. This is so because there are so-called *maximally entangled states* from which all others can be created by LOCC only (at least for bipartite systems of fixed maximal dimension). We we will show this explicitly here for the case of two qubits and leave the generalization as an exercise to the reader. In the case of two qubits, we will see that the maximally entangled states are those that are local-unitarily equivalent to the state

$$|\psi_2^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,. \tag{5}$$

Our aim is now to justify this statement by showing that for any bipartite pure state written in a Schmidt decomposed form (see discussion around equation (10) for an explanation of the Schmidt Decomposition):

$$|\phi\rangle = \alpha|00\rangle + \beta|11\rangle \tag{6}$$

we can find a LOCC map that takes $|\psi_2^+\rangle$ to $|\phi\rangle$ with certainty. To this end we simply need to write down the Kraus operators (see eq. (1) of a valid quantum operation. It is easy to show that the Kraus operators defined by

$$\begin{aligned} A_0 &:= (\alpha|0\rangle\langle 0| + \beta|1\rangle\langle 1|)\otimes \mathbb{1}, \\ A_1 &:= (\beta|1\rangle\langle 0| + \alpha|0\rangle\langle 1|)\otimes(|1\rangle\langle 0| + |0\rangle\langle 1|) \end{aligned} \tag{7}$$

satisfy $A_0^\dagger A_0 + A_1^\dagger A_1 = \mathbb{1}\otimes\mathbb{1}$ and $A_i|\psi\rangle = p_i|\phi\rangle$, so that $|\phi\rangle\langle\phi| = A_0|\psi\rangle\langle\psi|A_0^\dagger + A_1|\psi\rangle\langle\psi|A_1^\dagger$. It is instructive to see how one can construct this operation physically using only LOCC transformations. Let us first add an ancilla in state $|0\rangle$ to Alice which results in the state

$$\frac{|00\rangle_A|0\rangle_B + |01\rangle_A|1\rangle_B}{\sqrt{2}}\,. \tag{8}$$

If we then perform the local unitary operation $|00\rangle \to \alpha|00\rangle + \beta|11\rangle$; $|01\rangle \to \beta|01\rangle + \alpha|10\rangle$ on Alice's two particles, we arrive at

$$\frac{|0\rangle_A(\alpha|00\rangle_{AB} + \beta|11\rangle_{AB}) + |1\rangle_A(\beta|10\rangle_{AB} + \alpha|01\rangle_{AB})}{\sqrt{2}}. \tag{9}$$

Finally, a local measurement on Alice's ancilla particle now yields two outcomes. If Alice finds $|0\rangle$ then Bob is informed and does not need to carry out any further operation; if Alice finds $|1\rangle$ then Bob needs to apply a σ_x operation to his particle. In both cases this results in the desired state $\alpha|00\rangle_{AB} + \beta|11\rangle_{AB}$.

Given that we can obtain with certainty any arbitrary pure state starting from $|\psi_2^+\rangle$, we can also obtain any mixed state ρ. This is because any mixed state ρ can always be written in terms of its eigenvectors as $\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|$, where each eigenvector is of the form $|\phi_i\rangle = U_i\otimes V_i(\alpha_i|00\rangle + \beta_i|11\rangle)$ for some set of unitaries U_i and V_i (this in turn is simply a consequence of the Schmidt decomposition). It is an easy exercise, left to the reader, to construct the operation that takes $|\psi_2^+\rangle$ to ρ.

A natural generalisation of this observation would be to consider LOCC transformations between general pure states of two parties [27]. Although this question is a little more difficult, a complete solution has been developed using the mathematical framework of the theory of *majorization*. The results that have been obtained not only provide necessary and sufficient conditions for the possibility of the LOCC interconversion between two pure states, they are also constructive as they lead to explicit protocols that achieve the task [28, 29, 30, 31]. These conditions may be expressed most naturally in terms of the *Schmidt coefficients* [10] of the states involved. It is a useful fact that any bi-partite pure quantum state $|\psi\rangle$ may be written in the form

$$|\psi\rangle = U_A\otimes U_B\sum_{i=1}^{N}\sqrt{\alpha_i}|i\rangle_A|i\rangle_B \tag{10}$$

where the positive real numbers α_i are the *Schmidt-coefficients* of the state $|\psi\rangle$ [b]. The local unitaries do not affect the entanglement properties, which is why we now write the initial

[b] That this is true can be proven as follows. Consider a general bipartite state $|\psi\rangle = \sum a_{ij}|i\rangle|j\rangle$. The amplitudes a_{ij} can be considered as the matrix elements of a matrix A. This matrix hence completely represents the

state vector $|\psi_1\rangle$ and final state vector $|\psi_2\rangle$ in their Schmidt-bases,

$$|\psi_1\rangle = \sum_{i=1}^{n} \sqrt{\alpha_i}\, |i_A\rangle\, |i_B\rangle\,, \qquad |\psi_2\rangle = \sum_{i=1}^{n} \sqrt{\alpha_i'}\, |i_A'\rangle\, |i_B'\rangle$$

where n denotes the dimension of each of the quantum systems. We can take the Schmidt coefficients to be given in decreasing order, i.e., $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$ and $\alpha_1' \geq \alpha_2' \geq \ldots \geq \alpha_n'$. The question of the interconvertibility between the states can then be decided from the knowledge of the real Schmidt coefficients only, as any two pure states with the same Schmidt coefficients may be interconverted straightforwardly by local unitary operations. In [28] it has been shown that a LOCC transformation converting $|\psi_1\rangle$ to $|\psi_2\rangle$ with unit probability exists if and only if the $\{\alpha_i\}$ are *majorized* by $\{\alpha_i'\}$, i.e. if for all $1 \leq l < n$ we have that

$$\sum_{i=1}^{l} \alpha_i \leq \sum_{i=1}^{l} \alpha_i' \tag{11}$$

and $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \alpha_i'$, where n denotes the number of nonzero Schmidt-coefficients [32]. Various refinements of this result have been found that provide the largest success probabilities for the interconversion between two states by LOCC, together with the optimal protocol (according to certain figures of merit) where such a deterministic interconversion is not possible [29, 30, 33]. These results allow us in principle to decide any question concerning the LOCC interconversion of pure states by employing techniques from linear programming [30].

It is a direct consequence of the above structures that there are *incomparable* states, i.e. pairs of states such that neither can be converted into the other with certainty. These states are called incomparable as neither can be viewed as more entangled than the other. Note that borrowed entanglement can make some pairs of incomparable states comparable again. Indeed, there are known examples where the LOCC transformation of $|\psi\rangle \to |\phi\rangle$ is not possible with probability one, but where given a suitable entangled state $|\eta\rangle$ the LOCC transformation of $|\psi\rangle|\eta\rangle \to |\phi\rangle|\eta\rangle$ is possible with certainty [33]. This phenomenon is now called *entanglement catalysis*, as the state $|\eta\rangle$ is returned unchanged after the transformation, and acts much like a catalyst. The majorization condition also reveals another disadvantageous feature of the single copy setting - there can be *discontinuities*. For instance, it can be shown that the maximal probability of success for the LOCC transformation from $(|00\rangle + |11\rangle)/\sqrt{2}$ to $0.8|00\rangle + 0.6|11\rangle$ is unity, while the probability for the transformation $(|00\rangle + |11\rangle)/\sqrt{2}$ to $(0.8|00\rangle + 0.6|11\rangle + \epsilon|22\rangle)/\sqrt{1+\epsilon^2}$ is strictly zero for any $\epsilon \neq 0$, i.e. even if the target states in the two examples are arbitrarily close. That the probability of success for the later transformation is zero can also be concluded easily from the fact that the Schmidt-number, i.e. the number of non-vanishing Schmidt-coefficients, cannot be increased in an LOCC protocol, even probabilistically.

The key problem is that we are being too restrictive in asking for *exact* state transformations. Physically, we should be perfectly happy if we can come very close to a desired state.

state (as long as a local basis is specified). If we perform the local unitary transformation $U \otimes V|\psi\rangle$ then the matrix A gets transformed as $A \to UAV^T$. It is a well established result of matrix analysis - the *singular value decomposition* [32] - that any matrix A can be *diagonalised* into the form $A_{ij} = \lambda_i \delta_{ij}$ by a suitable choice of (U, V), even if A is not square. The coefficients λ_i are the so-called *singular values* of A, and correspond to the Schmidt coefficients.

Indeed, admitting a small but finite value of ϵ there will be a finite probability to achieve the transformation. This removes the above discontinuity [34], but the success probability will now depend on the size of the imprecision that we allow. The following subsection will serve to overcome this problem for pure states by presenting a natural definition of interconvertibility in the presence of vanishing imprecisions, a definition that will constitute our first entanglement measure.

State manipulation in the asymptotic limit – The study of the LOCC transformation of pure states has so far enabled us to justify the concept of maximally entangled states and has also permitted us, in some cases, to assert that one state is more entangled than another. However, we know that exact LOCC transformations can only induce a partial order on the set of quantum states. The situation is even more complex for *mixed* states, where even the question of when it is possible to LOCC transform one state into another is a difficult problem with no transparent solution at the time of writing.

All this means that if we want to give a definite answer as to whether one state is more entangled than another for any pair of states, it will be necessary to consider a more general setting. In this context a very natural way to compare and quantify entanglement is to study LOCC transformations of states in the so called *asymptotic regime*. Instead of asking whether for a single pair of particles the initial state ρ may be transformed to a final state σ by LOCC operations, we may ask whether for some large integers m, n we can implement the 'wholesale' transformation $\rho^{\otimes n} \to \sigma^{\otimes m}$. The largest ratio m/n for which one may achieve this would then indicate the relative entanglement content of these two states. Considering the many-copy setting allows each party to perform collective operations on (their shares of) many copies of the states in question. Such a many copy regime provides many more degrees of freedom, and in fact paves part of the way to a full classification of pure entangled states. To pave the rest of the route we will also need to discuss what kind of approximations we might admit for the output of the transformations.

There are two basic approaches to this problem - we can consider either *exact* or *asymptotically exact* transformations. The distinction between these two approaches is important, as they lead to different scenarios that yield different answers. In the *exact* regime we allow no errors at all - we must determine whether the transformation $\rho^{\otimes n} \to \sigma^{\otimes m}$ can be achieved perfectly and with 100% success probability for a given value of m and n. The supremum of all achievable rates $r = m/n$ is denoted by $r_{exact}(\sigma \to \rho)$, and carries significance as a measure of the exact LOCC 'exchange rate' between states ρ, σ. This quantity may be explored and gives some interesting results [19]. However, from a physical point of view one may feel that the restriction to exact transformations is too stringent. After all, it should be quite acceptable to consider approximate transformations [24] that become arbitrarily precise when going to the asymptotic limit. Asymptotically vanishing imperfections, as quantified by the trace norm (i.e. $\mathrm{tr}|\sigma - \eta|$), will lead to vanishingly small changes in measurements of bounded observables on the output. This leads to the second approach to approximate state transformations, namely that of *asymptotically exact* state transformations, and this is the setting that we will consider for the remainder of this work. In this setting we consider imperfect transformations between large blocks of states, such that in the limit of large block sizes the imperfections vanish. For example, for a large number n of copies of ρ, one transforms $\rho^{\otimes n}$ to an output state σ_m that approximates $\sigma^{\otimes m}$ very well for some large m. If, in the limit of

$n \to \infty$ and for fixed $r = m/n$, the approximation of $\sigma^{\otimes m}$ by σ_m becomes arbitrarily good, then the rate r is said to be *achievable*. One can use the optimal (supremal) achievable rate r_{approx} as a measure of the relative entanglement content of ρ, σ in the asymptotic setting. This situation is reminiscent of Shannon compression in classical information theory - where the compression process loses all imperfections in the limit of infinite block sizes as long as the compression rate is below a threshold [35]. Clearly the asymptotically exact regime is less strongly constrained than the exact regime, so that $r_{approx} \geq r_{exact}$. Given that we are considering two limiting processes it is not clear whether the two quantities are actually equal and it can be rigorously demonstrated that they are different in general, see e.g. [19].

Such an asymptotic approach will alleviate some of the problems that we encountered in the previous section. It turns out that the asymptotic setting yields a unique total order on bi-partite pure states, and as a consequence, leads to a very natural measure of entanglement that is essentially unique. To this end let us start by defining our first entanglement measure, which happens also to be one of the most important measures - the *entanglement cost*, $E_C(\rho)$. For a given state ρ this measure quantifies the maximal possible rate r at which one can convert blocks of *2-qubit* maximally entangled states [36] into output states that approximate many copies of ρ, such that the approximations become vanishingly small in the limit of large block sizes. If we denote a general trace preserving LOCC operation by Ψ, and write $\Phi(K)$ for the density operator corresponding to the maximally entangled state vector in K dimensions, i.e. $\Phi(K) = |\psi_K^+\rangle\langle\psi_K^+|$, then the entanglement cost may be defined as

$$E_C(\rho) = \inf \left\{ r : \lim_{n\to\infty} \left[\inf_{\Psi} D(\rho^{\otimes n}, \Psi(\Phi(2^{rn}))) \right] = 0 \right\}$$

where $\mathrm{D}(\sigma, \eta)$ is a suitable measure of distance [37, 19]. A variety of possible distance measures may be considered. It has been shown that the definition of entanglement cost is independent of the choice of distance function, as long as these functions are equivalent to the trace norm in a way that is sufficiently independent of dimension (see [38] for further explanation). Hence we will fix the trace norm distance, i.e. $D(\sigma, \eta) = tr|\sigma - \eta|$, as our canonical choice of distance function.

It may trouble the reader that in the definition of $E_C(\rho)$ we have not actually taken input states that are blocks of rn copies of 2-qubit maximally entangled states, but instead have chosen as inputs single maximally entangled states between subsystems of increasing dimensions 2^{rn}. However, these two approaches are equivalent because (for integral rn) $\Phi(2^{rn})$ is local unitarily equivalent to $\Phi(2)^{\otimes rn}$.

The entanglement cost is an important measure because it quantifies a wholesale 'exchange rate' for converting maximally entangled states to ρ by LOCC alone. Maximally entangled states are in essence the 'gold standard currency' with which one would like to compare all quantum states. Although computing $E_C(\rho)$ is extremely difficult, we will later discuss its important implications for the study of channel capacities, in particular via another important and closely related entanglement measure known as the *entanglement of formation*, $E_F(\rho)$.

Just as $E_C(\rho)$ measures how many maximally entangled states are required to create copies of ρ by LOCC alone, we can ask about the reverse process: at what rate may we obtain maximally entangled states (of two qubits) from an input supply of states of the form ρ. This process is known in the literature either as *entanglement distillation*, or as *entanglement concentration* (usually reserved for the pure state case). The efficiency with which we can achieve this process defines another important basic asymptotic entanglement measure which is the *Distillable Entanglement*, $E_D(\rho)$. Again we allow the output of the procedure to *approximate* many copies of a maximally entangled state, as the exact transformation from $\rho^{\otimes n}$ to even one pure maximally entangled state is in general impossible [39]. In analogy to the definition of $E_C(\rho)$, we can then make the precise mathematical definition of $E_D(\rho)$ as

$$E_D(\rho) := \sup \left\{ r : \lim_{n\to\infty} \left[\inf_{\Psi} \mathrm{tr} |\Psi(\rho^{\otimes n}) - \Phi(2^{rn})| \right] = 0 \right\}.$$

$E_D(\rho)$ is an important measure because if entanglement is used in a two party quantum information protocol, then it is usually required in the form of maximally entangled states. So $E_D(\rho)$ tells us the rate at which noisy mixed states may be converted back into the 'gold standard' singlet state by LOCC. In defining $E_D(\rho)$ we have ignored a couple of important issues. Firstly, our LOCC protocols are always taken to be trace preserving. However, one could conceivably allow probabilistic protocols that have varying degrees of success depending upon various measurement outcomes. Fortunately, a thorough analysis by Rains [40] shows that taking into account a wide diversity of possible success measures still leads to the same notion of distillable entanglement. Secondly, we have always used 2-qubit maximally entangled states as our 'gold standard'. If we use other entangled *pure* states, perhaps even on higher dimensional Hilbert spaces, do we arrive at significantly altered definitions? We will very shortly see that this is not the case so there is no loss of generality in taking singlet states as our target.

Given these two entanglement measures it is natural to ask whether $E_C \stackrel{?}{=} E_D$, i.e. whether entanglement transformations become *reversible* in the asymptotic limit. This is indeed the case for pure state transformations where $E_D(\rho)$ and $E_C(\rho)$ are identical and equal to the *entropy of entanglement* [24]. The entropy of entanglement for a pure state $|\psi\rangle$ is defined as

$$E(|\psi\rangle\langle\psi|) := S(\mathrm{tr}_A|\psi\rangle\langle\psi|) = S(\mathrm{tr}_B|\psi\rangle\langle\psi|) \tag{12}$$

where S denotes the von-Neumann entropy $S(\rho) = -\mathrm{tr}[\rho \log_2 \rho]$, and tr_B denotes the partial trace over subsystem B. This reversibility means that in the asymptotic regime we may immediately write down the optimal rate of transformation between *any* two pure states $|\psi_1\rangle$ and $|\psi_2\rangle$. Given a large number N of copies of $|\psi_1\rangle\langle\psi_1|$, we can first distill $\approx NE(|\psi_1\rangle\langle\psi_1|)$ singlet states and then create from those singlets $M \approx NE(|\psi_1\rangle\langle\psi_1|)/E(|\psi_2\rangle\langle\psi_2|)$ copies of $|\psi_2\rangle\langle\psi_2|$. In the infinite limit these approximations become exact, and as a consequence $E(|\psi_1\rangle\langle\psi_1|)/E(|\psi_2\rangle\langle\psi_2|)$ is the optimal asymptotic conversion rate from $|\psi_1\rangle\langle\psi_1|$ to $|\psi_2\rangle\langle\psi_2|$. It is the reversibility of pure state transformations that enables us to define $E_D(\rho)$ and $E_C(\rho)$ in terms of transformations to or from singlet states - the use of any other entangled pure state (in any other dimensions) simply leads to a constant factor multiplied in front of these quantities.

Following these basic considerations we are now in a position to formulate a more rigorous and axiomatic approach to entanglement measures that captures the lessons that have been learned in the previous sections. In the final section we will then review several entanglement measures, presenting useful formulae and results and discuss the significance of these measures for various topics in quantum information.

4 Postulates for axiomatic Entanglement Measures

In the previous section we considered the quantification of entanglement from the perspective of LOCC transformations in the asymptotic limit. This approach is interesting because it can be solved completely for pure states. It demonstrates that LOCC entanglement manipulation is reversible in this setting, therefore imposing a unique order on pure entangled states via the entropy of entanglement. However, for mixed states and LOCC operations the situation is more complicated and reversibility is lost [41, 42].

The concomitant loss of a total ordering of quantum states (in terms of rates of LOCC entanglement interconversions) implies that in general an LOCC based classification of entanglement would be extremely complicated.

However, one can try to salvage the situation by taking a more axiomatic approach. One can *define* real valued functions that satisfy the basic properties of entanglement that we outlined earlier, and use these functions to attempt to *quantify* the amount of entanglement in a given quantum state. This is essentially the process that is followed in the definition of most entanglement measures. Various such quantities have been proposed over the years, such as the entanglement of distillation [24, 40], the entanglement cost [24, 43, 44, 38, 45], the relative entropy of entanglement [25, 46, 26] and the squashed entanglement [47]. Some of these measures have direct physical significance, whereas others are purely axiomatic. Initially these measures were used to give a physically motivated classification of entanglement that is simple to understand, and can even be used to assess the quality of entangled states produced in experiments. However, subsequently they have also been developed into powerful mathematical tools, with great significance for open questions such as the additivity of quantum channel capacities [48, 49, 50], quantifying quantum correlations in quantum-many-body systems [52, 55, 53, 54, 56], and bounding quantum computing fault tolerance thresholds [57, 58] to name a few.

In this section we will now discuss and present a few basic axioms that any measure of entanglement should satisfy. This will allow us to define further quantities that go beyond the two important mixed state measures ($E_C(\rho)$ and $D(\rho)$) that we have already introduced.

So what exactly are the properties that a good entanglement measure should possess? An entanglement measure is a mathematical quantity that should capture the essential features that we associate with entanglement, and ideally should be related to some operational procedure. Depending upon your aims, this can lead to a variety of possible desirable properties. The following is a list of possible postulates for entanglement measures, some of which are not satisfied by all proposed quantities [26, 63]:

1. A *bipartite* entanglement measure $E(\rho)$ is a mapping from density matrices into positive real numbers:

   $$\rho \rightarrow E(\rho) \in \mathbb{R}^+ \tag{13}$$

   defined for states of arbitrary bipartite systems. A normalisation factor is also usually included such that the maximally entangled state

   $$|\psi_d^+\rangle = \frac{|0,0\rangle + |1,1\rangle + .. + |d-1, d-1\rangle}{\sqrt{d}}$$

   of two qudits has $E(|\psi_d^+\rangle) = \log d$.

2. $E(\rho) = 0$ if the state ρ is separable.

3. E does not increase on average under LOCC, i.e.,

$$E(\rho) \geq \sum_i p_i E(\frac{A_i \rho A_i^\dagger}{tr A_i \rho A_i^\dagger}) \tag{14}$$

where the A_i are the Kraus operators describing some LOCC protocol and the probability of obtaining outcome i is given by $p_i = tr A_i \rho A_i^\dagger$ (see fig 2).

4. For pure state $|\psi\rangle\langle\psi|$ the measure reduces to the entropy of entanglement

$$E(|\psi\rangle\langle\psi|) = (S \circ \mathrm{tr}_B)(|\psi\rangle\langle\psi|)\ . \tag{15}$$

We will call any function E satisfying the first three conditions an *entanglement monotone*. The term *entanglement measure* will be used for any quantity that satisfies axioms 1,2 and 4, and also does not increase under *deterministic* LOCC transformations. In the literature these terms are often used interchangeably. Note that the conditions (1)-(4) may be replaced by an equivalent set of slightly more abstract conditions which will be explained below eq. (20). Frequently, some authors also impose additional requirements for entanglement measures:

• *Convexity* – One common example for an additional property required from an entanglement measure is the concept of convexity which means that we require

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

Requiring this mathematically very convenient property is sometimes justified as capturing the notion of the loss of information, i.e. describing the process of going from a selection of identifiable states ρ_i that appear with rates p_i to a mixture of these states of the form $\rho = \sum p_i \rho_i$. We would like to stress, however, that some care has to be taken in this context. Indeed, in the first situation, when the states are locally identifiable, the whole ensemble can be described by the quantum state

$$\sum_i p_i |i\rangle_M \langle i| \otimes \rho_i^{AB}, \tag{16}$$

where the $\{|i\rangle_M\}$ denote some orthonormal basis for a particle belonging to one of the two parties. Clearly a measurement of the marker particle M reveals the identity of the state of parties A and B. Losing the association between $|i\rangle_M$ and state ρ_i^{AB} then correctly describes the process of the forgetting, a process which is then described by tracing out the marker particle M to obtain $\rho = \sum p_i \rho_i$ [64, 65]. As this is a local operation we may then require that $E(\sum_i p_i |i\rangle_M \langle i| \otimes \rho_i^{AB}) \geq E(\rho)$, which is, of course, already required by condition 3 above. Hence there is no strict need to require convexity, except for the mathematical simplicity that it might bring. A compelling example of the technical simplicity that convexity can bring is the very simple test for entanglement monotonicity of a convex function f. Indeed, a convex function f does not increase under LOCC if and only if it satisfies (i) $f(U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger) = f(\rho_{AB})$ for all local unitary U_A, U_B and (ii) $f(\sum_i p_i \rho_{AB}^i \otimes |i\rangle\langle i|_X) = \sum_i p_i f(\rho_{AB}^i)$ where $X = A', B'$ and $|i\rangle$ form local, orthogonal bases [66].

• *Additivity* – Given an entanglement measure and a state σ one may ask for the condition $E(\sigma^{\otimes n}) = nE(\sigma)$ to be satisfied for all integer n. A measure satisfying this property is said to be *additive*. Unfortunately, there are some significant entanglement measures that do not satisfy this condition, and for this reason we have not included additivity as a basic postulate. However, given any measure E that is not additive there is a straightforward way of removing this deficiency. We may define the *regularized*, or *asymptotic* version:

$$E^{\infty}(\sigma) := \lim_{n\to\infty} \frac{E(\sigma^{\otimes n})}{n} \tag{17}$$

which is a measure that then automatically satisfies additivity.

A much stronger requirement could be to demand *full additivity*, by which we mean that for any pair of states σ and ρ we have $E(\sigma\otimes\rho) = E(\sigma)+E(\rho)$. This is a very strong requirement and in fact it may be too strong to be satisfied by all quantities that otherwise satisfy the four basic properties stated above. Indeed, even such basic measures as the distillable entanglement may not satisfy this property [67]. For these reason we have not included the full additivity in our set of properties. However, additivity can be a very useful mathematical property, and we will discuss it further in the context of specific measures.

• *Continuity* – Conditions (1-3) listed above seem quite natural - the first two conditions are little more than setting the scale, and the third condition is a generalisation of the idea that entanglement can only decrease under LOCC operations to incorporate probabilistic transformations. The fourth condition appears considerably stronger and perhaps arbitrary at first sight. However, it turns out that it is also quite a natural condition to impose. In fact we know that $S(\rho_A)$ represents the reversible rate of conversion between pure states in the asymptotic regime which strongly suggests that it is the appropriate measure of entanglement for pure states. This is reinforced by the following nontrivial observation: it turns out that *any* entanglement monotone that is (a) additive on pure states, and (b) "sufficiently continuous" must *equal* $S(\rho_A)$ on all pure states. Before we see what sufficiently continuous means we present a very rough argument for this statement. We know from the asymptotic pure state distillation protocol that from n copies of a pure state $|\phi\rangle$ we can obtain a state ρ_n that closely approximates the state $|\psi^-\rangle^{\otimes nE(|\phi\rangle)}$ to within ϵ, where $E(|\phi\rangle)$ is the entropy of entanglement of $|\phi\rangle$. Suppose therefore that we have an entanglement monotone L that is *additive* on pure states. Then we may write

$$nL(|\phi\rangle) = L(|\phi\rangle^{\otimes n}) \geq L(\rho_n) \tag{18}$$

where the inequality is due to condition 3 for entanglement monotones. If the monotone L is "sufficiently continuous", then $L(\rho_n) = L(|\psi^-\rangle^{\otimes nE(|\phi\rangle)}) + \delta(\epsilon) = nE(|\phi\rangle) + \delta(\epsilon)$, where $\delta(\epsilon)$ will be small. Then we obtain:

$$L(|\phi\rangle) \geq E(|\phi\rangle) + \frac{\delta(\epsilon)}{n}. \tag{19}$$

If the function L is sufficiently continuous as the dimension increases, i.e. $\delta(\epsilon)/n \to 0$ when $n\to\infty$, then we obtain $L(|\phi\rangle) \geq E(|\phi\rangle)$. Invoking the fact that the entanglement cost for pure states is also given by the entropy of entanglement gives the reverse inequality $L(|\phi\rangle) \leq E(|\phi\rangle)$ using similar arguments. Hence sufficiently continuous monotones that are additive on pure states will naturally satisfy $L(|\phi\rangle) = E(|\phi\rangle)$. Of course these arguments are not rigorous, as we have not undertaken a detailed analysis of how δ or ϵ grow with n. A rigorous analysis is presented in [63], where it is also shown that our assumptions may be slightly relaxed. The result of this rigorous analysis is that a function is equivalent to the entropy of entanglement on pure states *if and only if* it is (a) normalised on the singlet state, (b) additive on pure states, (c) non-increasing on *deterministic* pure state to pure state LOCC transformations, and (d) *asymptotically continuous* on pure states. The term *asymptotically continuous* is defined as the property

$$\frac{L(|\phi\rangle_n) - L(|\psi\rangle_n)}{1 + \log(\dim H_n)} \to 0 \tag{20}$$

whenever the trace norm $tr||\phi\rangle\langle\phi|_n - |\psi\rangle\langle\psi|_n|$ between two sequences of states $|\phi\rangle_n, |\psi\rangle_n$ on a sequence of Hilbert spaces $H_n \otimes H_n$ tends to 0 as $n \to 0$. It is interesting to notice that these constraints only concern pure state properties of L, and that they are *necessary and sufficient*. As a consequence of the above discussion we can conclude that we could have redefined the set of axiomatic requirements (1)-(4), without changing the set of admissible measures. We could have replaced axiom (4) with two separate requirements of (4'a) additivity on pure states and (4'b) asymptotic continuity on pure states. Together with axiom (3) this would automatically force any entanglement measure to coincide with the entropy of entanglement on pure states.

It is furthermore interesting to note that the failure of an entanglement measure to satisfy asymptotic continuity is strongly related to the counterintuitive effect of *lockability* [68, 69, 70]. The basic question behind lockability is: how much can entanglement of any bi- or multipartite system change when one qubit is discarded? A measure of entanglement is said to be *lockable* if the removal of a single qubit from a system can reduce the entanglement by an arbitrarily large amount. This qubit hence acts as a 'key' which once removed 'locks' the remaining entanglement. So which entanglement measures are lockable? The remarkable answer is this effect can occur for several entanglement measures, including the Entanglement Cost. On the other hand another class of measures that will be described later, *Relative Entropies of Entanglement*, are not lockable [69]. It can also be proven that any measure that is convex and is *not* asymptotically continuous is lockable [69].

Extremal Entanglement Measures– In the discussions so far we have formulated several requirements on entanglement measures and suggested that various measures exist that satisfy those criteria. It is now interesting to bound the range of such entanglement measures. One may in fact show that the entanglement cost $E_C(\rho)$ and the distillable entanglement $E_D(\rho)$ are in some sense *extremal* measures [71, 63], in that they are upper and lower bounds for many '*wholesale*' entanglement measures. To be precise, suppose that we have a quantity $L(\rho)$ satisfying conditions (1) - (3) above, that is also asymptotically continuous on mixed states, and also has a *regularisation*

$$\lim_{n\to\infty} \frac{L(\rho^{\otimes n})}{n}. \tag{21}$$

Then it can be shown that

$$E_C(\rho) \geq \lim_{n\to\infty} \frac{L(\rho^{\otimes n})}{n} \geq E_D(\rho). \tag{22}$$

In fact the conditions under which this statement is true are slightly more general than the ones that we have listed - for more details see [63].

Entanglement Ordering The above considerations have allowed us to impose quite a great deal of structure on entangled states and the next section will make this even more clear. It should be noted however that the axioms 1-4 as formulated above are *not* sufficient to give a *unique* total ordering in terms of the entanglement of the set of states. One can show that any two entanglement measures satisfying axiom 4 can only impose the same ordering on the set of entangled states if they are actually exactly the same. More precisely, if for two measures E_1 and E_2 and *any* pair of states σ_1 and σ_2 we have that $E_1(\sigma_1) \geq E_1(\sigma_2)$ implies $E_2(\sigma_1) \geq E_2(\sigma_2)$, then if both measures satisfy axiom 4 it must be the case that $E_1 \equiv E_2$ [72] (see [73, 74, 75] for ordering results for other entanglement quantities). Given that the entanglement cost and the distillable entanglement are strictly different on all entangled mixed states [76] this implies that there is not a unique order, in terms of entanglement, on the set of entangled states.

This suggests one of several viewpoints. We may for example have neglected to take account of the resources in entanglement manipulation with sufficient care, and doing so might lead to the notion of a unique total order and therefore a unique entanglement measure [77]. Alternatively, it may be possible that the setting of LOCC operations is too restrictive, and a unique total order and entanglement measure might emerge when considering more general sets of operations [19]. Both approaches have received some attention but neither has succeeded completely at the time of writing this article.

In the following we will simply accept the non-uniqueness of entanglement measures as an expression of the fact that they correspond to different operational tasks under which different forms of entanglement may have different degrees of usefulness.

5 A survey of entanglement measures

In this section we discuss a variety of bipartite entanglement measures and monotones that have been proposed in the literature. All the following quantities are entanglement *monotones*, in that they cannot increase under LOCC. Hence when they can be calculated they can be used to determine whether certain (finite or asymptotic) LOCC transformations are possible. However, some measures have a wider significance that we will discuss as they are introduced. Before we continue, we consider some features of the distillable entanglement, particularly with regard to its computation, as this will be important for some of our later discussion.

The distillable entanglement – The distillable entanglement, $E_D(\rho)$, provides us with the rate at which noisy mixed states ρ may be converted into the 'gold standard' singlet state by LOCC alone. It formal definition is

$$E_D(\rho) := \sup \left\{ r : \lim_{n\to\infty} \left[\inf_{\Psi} \mathrm{tr}|\Psi(\rho^{\otimes n}) - \Phi(2^{rn})| \right] = 0 \right\}.$$

The complexity of this variational definition has the unfortunate consequence that despite the importance of the distillable entanglement as an entanglement measure, very little progress has been made in terms of its computation. It is known for pure states (where it equals the entropy of entanglement), and for some simple but very special states [26, 78] (see the end of this paragraph). To obtain such results and to gain insight into the amount of distillable entanglement it is particularly important to be able to provide bounds on its value. *Upper* *bounds* can, by virtue of eq. (22) and requirement 3 for entanglement monotones, be provided by any other entanglement monotone and measure but non-monotonic bounds are also of interest (see the remainder of this section on entanglement measures). Calculating *lower bounds* is more challenging. Some lower bounds can be obtained by the construction of explicit entanglement purification procedures [43] in particular for Bell diagonal states [79, 80]. As every state can be reduced to a Bell diagonal state by random bi-local rotations of the form $U \otimes U$ (a process known as *twirling*), these methods result in general lower bounds applicable to all states. Improving these bounds is very difficult as it generally requires the explicit construction of complex purification procedures in the asymptotic limit of many copies.

In this context it is of considerable interest to study the *conditional entropy*, which is defined as $C(A|B) := S(\rho_{AB}) - S(\rho_B)$ for a bipartite state ρ_{AB}. It was known for some time that $-C(A|B)$ gives a lower bound for both the entanglement cost and another important measure known as the *relative entropy of entanglement* [78]. However, this bound was also recently shown to be true for the one way distillable entanglement:

$$E_D(\rho_{AB}) \geq D_{A\rightarrow B}(\rho_{AB}) \geq \max\{S(\rho_B) - S(\rho_{AB}), 0\} \tag{23}$$

where $D_{A\rightarrow B}$ is the distillable entanglement under the restriction that the classical communication may only go one way from Alice to Bob [81]. This bound is known as the *Hashing Inequality* [43], and is significant as it is a computable, non-trivial, *lower bound* to $E_D(\rho)$, and hence supplies a non-trivial lower bound to many other entanglement measures. While this bound is generally not tight, it should be noted that there are examples for which it equals the distillable entanglement, these include Bell diagonal states of rank 2 [37] and some other special classes of state such as $\sigma = A|00\rangle\langle 00| + B|00\rangle\langle 11| + B^*|11\rangle\langle 00| + (1-A)|11\rangle\langle 11|$ for which relative entropy of entanglement (ie an upper bound to E_D) can be computed [26, 40] and is found to equal the hashing inequality.

The following subsection will present a variety of other entanglement measures and quantities that provide upper bounds on the distillable entanglement.

• *Entanglement Cost* – For a given state ρ the entanglement cost quantifies the maximal possible rate r at which one can convert blocks of *2-qubit* maximally entangled states into output states that approximate many copies of ρ, such that the approximations become vanishingly small in the limit of large block sizes. If we denote a general trace preserving LOCC operation by Ψ, and write $\Phi(K)$ for the density operator corresponding to the maximally entangled state vector in K dimensions, i.e. $\Phi(K) = |\psi_K^+\rangle\langle\psi_K^+|$, then the entanglement cost may be defined as

$$E_C(\rho) = \inf\left\{r : \lim_{n\rightarrow\infty}\left[\inf_{\Psi} tr|(\rho^{\otimes n} - \Psi(\Phi(2^{rn}))|\right] = 0\right\}$$

This quantity is again very difficult to compute indeed. It is known to equal the entropy of entanglement for pure bi-partite states. It can also be computed for trivial mixed states $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ where the states $|\psi_i\rangle$ may be discriminated locally perfectly without destroying the states. A simple example is $|\psi_1\rangle = |00\rangle$ and $|\psi_2\rangle = (|11\rangle + |22\rangle)/\sqrt{2}$.

Fortunately, a closely related measure of entanglement, namely the entanglement of formation, provides some hope as it may actually equal the entanglement cost. Therefore, we move on to discuss its properties in slightly more detail.

- *Entanglement of Formation* – For a mixed state ρ this measure is defined as

$$E_F(\rho) := \inf\{\sum_i p_i E(|\psi_i\rangle\langle\psi_i|) \ : \ \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|\}.$$

Given that this measure represents the minimal possible average entanglement over all pure state decompositions of ρ, where $E(|\psi\rangle\langle\psi|) = S(\mathrm{tr}_B\{|\psi\rangle\langle\psi|\})$ is taken as the measure of entanglement for pure states, it can be expected to be closely related to the entanglement cost of ρ. Note however that the entanglement cost is an asymptotic quantity concerning $\rho^{\otimes n}$ in the limit $n \to \infty$. It is not self-evident and in fact unproven that the entanglement of formation accounts for that correctly. Note however, that the *regularised* or *asymptotic* version of the entanglement of formation, which is defined as

$$E_F^\infty(\rho) := \lim_{n\to\infty} \frac{E_F(\rho^{\otimes n})}{n}$$

can be proven rigorously to equal the entanglement cost [38], i.e.

$$E_F^\infty(\rho) = E_C(\rho). \tag{24}$$

Obviously, the computation of either, the entanglement cost or the asymptotic entanglement of formation, are extraordinarily difficult tasks. However, there are indications, though no general proof, that the entanglement of formation is additive, i.e. $E_F(\rho) = E_F^\infty(\rho) = E_C(\rho)$, a result that would simplify the computation of $E_C(\rho)$ significantly if it could be proven. Further to some numerical evidence for the correctness of this property it is also known that the entanglement of formation is additive for maximally correlated states in $d \times d$ dimensions, ie states $\rho_{mc} = \sum_{ij} a_{ij} |ii\rangle\langle jj|$ [42]. More generally it is a *major* open question in quantum information to decide whether E_F is a fully additive quantity, i.e. whether

$$E_F(\rho^{AB} \otimes \sigma^{AB}) = E_F(\rho^{AB}) + E_F(\sigma^{AB}). \tag{25}$$

This problem is known to be equivalent to the *strong superadditivity* of E_F

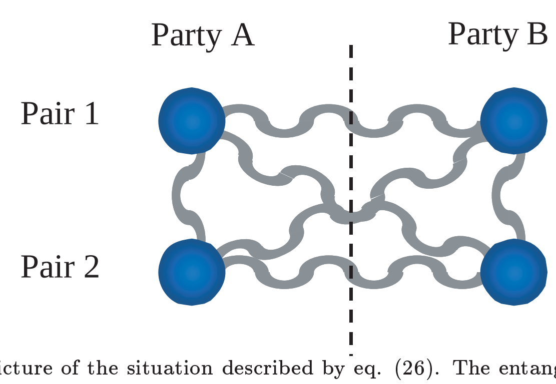

Fig. 3. Schematic picture of the situation described by eq. (26). The entanglement of formation of an arbitrary four particle state $|\psi\rangle$, with particles held by parties A and B is given is given on the left hand side of eq. (26). The right hand side of eq. (26) is the sum of the entanglement of formation of the states $\rho_1 = tr_{A_2B_2}|\psi\rangle\langle\psi|$ and $\rho_2 = tr_{A_1B_1}|\psi\rangle\langle\psi|$ obtained by tracing out the lower upper half of the system.

$$E_F(\rho_{12}^{AB}) \; ? \geq ? \; E_F(\rho_1^{AB}) + E_F(\rho_2^{AB}) \tag{26}$$

where the indices 1 and 2 refer to two pairs or entangled particles while A and B denote the different parties (see fig. 3).

The importance of these additivity problems is twofold. Firstly, additivity would imply that $E_F = E_C$ leading to a considerable simplification of the computation of the entanglement cost. Secondly, the entanglement of formation is closely related to the classical capacity of a quantum channel which is given by the Holevo capacity [82], and it can be shown that the additivity of E_F is also *equivalent* to the additivity of the classical communication capacity of quantum channels [48, 49, 50]!

The variational problem that defines E_F is extremely difficult to solve in general and at present one must either resort to numerical techniques for general states [83], or restrict attention to cases with high symmetry (e.g. [84, 85, 86]), or consider only cases of low dimensionality. Quite remarkably a closed form solution is known for bi-partite qubit states [44, 45, 83] that we present here. This exact formula is based on the often used two-qubit *concurrence* which is defined as

$$C(\rho) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{27}$$

where the λ_i are, in decreasing order, the square roots of the eigenvalues of the matrix $\rho\sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y$ where ρ^* is the elementwise complex conjugate of ρ. For general bi-partite qubit states it has been shown that [45]

$$E_F(\rho) = s(\frac{1 + \sqrt{1 - C^2(\rho)}}{2}) \tag{28}$$

with

$$s(x) = -x \log_2 x - (1 - x) \log_2 (1 - x). \tag{29}$$

The two-qubit $E_F(\rho)$ and the two-qubit concurrence are monotonically related which explains why some authors prefer to characterise entanglement using only the concurrence rather than the E_F. It should be emphasised however that it is only the entanglement of formation that is an entanglement measure, and that the concurrence obtains its meaning via its relation to the entanglement of formation and not vice versa. For higher dimensional systems this connection breaks down - in fact there is not even a unique definition of the concurrence. Therefore, the use of the entanglement of formation even in the two-qubit setting, is preferable.

• *Entanglement measures from convex roof constructions* – The entanglement of formation E_F is an important example of the general concept of a *convex roof* construction. The convex roof $\hat{f}$ of a function f is defined as the largest convex function that is for all arguments bounded from above by the function f. A simple example in one variable is given by $f(x) = x^4 - 2\alpha^2 x^2$ and its convex roof

$$\hat{f}(x) = \begin{cases} x^4 - 2\alpha^2 x^2 & \text{for } |x| \geq \alpha \\ -\alpha^4 & \text{for } |x| \leq \alpha \end{cases}$$

Fig. 4 illustrates this idea graphically with an example for the convex roof for a function of a single variable. Generally, for a function f defined on a convex subset of $\mathbb{R}^n$, the convex roof

$\hat{f}$ can be constructed via the variational problem

$$\hat{f}(x) = \inf_{x=\sum_i p_i x_i} \sum_i p_i f(x_i), \tag{30}$$

where the infimum is taken over all possible probability distributions p_i and choices of x_i such that $x = \sum_i p_i x_i$. It is easy to see that $\hat{f}$ is convex, that $\hat{f} \leq f$ and that any other convex function g that is smaller than f also satisfies $g \leq \hat{f}$.

The importance of the convex roof method is based on the fact that it can be used to construct entanglement monotones from any unitarily invariant and concave function of density matrices [87]. As this construction is very elegant we will discuss how it works in some detail. Suppose that we already have a function E of *pure* states, that is known to be an entanglement monotone on *pure* states. This means that for an LOCC transformation from an input pure state $|\psi\rangle$ to output pure states $|\psi_i\rangle$ with probability p_i, we have that:

$$E(|\psi\rangle) \geq \sum_i p_i E(|\psi\rangle_i). \tag{31}$$

Such pure state entanglement monotones are very well understood, as it can be shown that a function is a pure state monotone iff it is a unitarily invariant concave function of the single-site reduced density matrices [87].

Let us consider the convex-roof extension $\hat{E}$ of such a pure state monotone E to mixed states. A general LOCC operation can be written as a sequence of operations by Alice and Bob. Suppose that Alice goes first, then she will perform an operation that given outcome j performs the transformation:

$$\rho \rightarrow \rho_j = \frac{1}{p_j} \sum_k A_k \rho A_k^\dagger \tag{32}$$

where the A_k are Alice's local Kraus operators corresponding to outcome j, and $p_j{=}\mathrm{tr}\{\sum_k A_k \rho A_k^\dagger\}$ is the probability of getting outcome j. If $k > 1$ for any particular outcome, then Alice's operation is *impure*, in that an input pure state may be taken to a mixed output. However, any such LOCC *impure* operation may be implemented by first performing a LOCC *pure* operation, where Alice and Bob retain information about all k, followed by 'forgetting' the values of k at the end [c]. It can be shown quite straightforwardly that if an entanglement measure is convex, then the process of 'forgetting' cannot increase the average output entanglement beyond the average output entanglement of the intermediate pure operation. Hence if one shows that a convex quantity is an entanglement monotone for *pure* LOCC operations, then it will be an entanglement monotone in general.

This means that we need only prove that $\hat{E}$ is an entanglement monotone for *pure* operations acting upon input mixed states. This can be done as follows [87]. Let ρ be an input state with optimal decomposition $\rho = \sum q(i)|\phi_i\rangle\langle\phi_i|$, i.e.

$$\hat{E}(\rho) = \sum_i q(i) E(|\phi\rangle_i). \tag{33}$$

[c] i.e. A pure operation is one in which each different measurement outcome corresponds to only *one* Kraus operator

Suppose that we act upon this state with a measuring LOCC operation, where outcome j signifies that we have implemented the (not trace-preserving) *pure* map Λ_j (i.e. corresponding to a single Kraus-operator). Let us define:

$$\begin{aligned} p(j|i) &:= \mathrm{tr}\{\Lambda_j(|\phi_i\rangle)\}, \\ p(j) &:= \mathrm{tr}\{\Lambda_j(\rho)\}. \end{aligned}$$

It is clear that $p(j) = \sum_i q(i)p(j|i)$, as required by the standard probabilistic interpretation of ensembles. Hence given outcome j the state ρ transforms to:

$$\begin{aligned} \rho_j &= \frac{1}{p(j)} \sum_i q(i)\Lambda_j(|\phi\rangle_i) \\ &= \frac{1}{p(j)} \sum_i p(i,j) \frac{\Lambda_j(|\phi\rangle_i)}{p(j|i)} \\ &= \sum_i p(i|j) \frac{\Lambda_j(|\phi\rangle_i)}{p(j|i)}. \end{aligned} \tag{34}$$

Hence by the convexity of $\hat{E}$ we have that:

$$\hat{E}(\rho_j) \leq \sum_i p(i|j)\hat{E}\left(\frac{\Lambda_j(|\phi\rangle_i)}{p(j|i)}\right) \tag{35}$$

and because $\hat{E}$ is a monotone for operations from pure to pure states, and as each $\Lambda_j(|\phi\rangle_i)$ is pure by assertion, we find that:

$$\begin{aligned} \sum_j p(j)\hat{E}(\rho_j) &\leq \sum_j p(j) \sum_i p(i|j)\hat{E}\left(\frac{\Lambda_j(|\phi\rangle_i)}{p(j|i)}\right) \\ &= \sum_i q(i) \sum_j p(j|i)\hat{E}\left(\frac{\Lambda_j(|\phi\rangle_i)}{p(j|i)}\right) \\ &\leq \sum_i q(i)\hat{E}(|\phi_i\rangle) \\ &= \hat{E}(\rho) \end{aligned} \tag{36}$$

Hence it can be seen that the convex-roof of any pure state entanglement monotone is automatically an entanglement monotone for LOCC transformations from mixed states to mixed states. Together with the result that a function of pure states is an entanglement monotone iff it is a unitarily invariant concave function of the single-site density matrices [87], this provides a very elegant way of constructing many convex-roof entanglement monotones. It is interesting to note that although this method can also be used to construct monotones under separable operations, it does not work for constructing monotones under the set of PPT transformations, as unlike the case of LOCC/ separable operations, an *impure* PPT operation *cannot* always be equated to a *pure PPT* operation plus *forgetting* [6].

• *Relative entropy of entanglement* – So far we discussed the extremal entanglement measures, entanglement cost and entanglement of distillation. For some time it was unclear whether they were equal or whether there are any entanglement measures that lie between

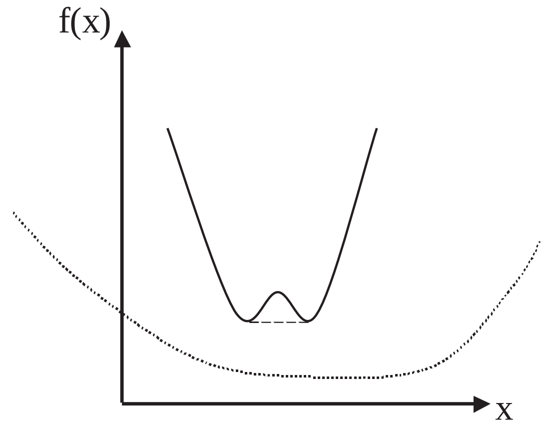

Fig. 4. A schematic picture of the convex roof construction in one dimension. The non-convex function $f(x)$ is given by the solid line. The dotted curve is a convex function smaller than f and the convex roof, the largest convex function that is smaller than f, is drawn as a dashed curved (it coincides in large parts with f).

these two. The regularised version of the *relative entropy of entanglement* provides an example of a measure that lies between E_C and E_D.

One way of understanding the motivation for its definition is by considering total correlations. These are measured by the quantum mutual information [10]

$$I(\rho_{AB}) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})\,. \tag{37}$$

Employing the *quantum relative entropy*

$$S(\rho||\sigma) := \mathrm{tr}\{\rho\log\rho - \rho\log\sigma\} \tag{38}$$

which is a measure of distinguishability between quantum states one may then rewrite the quantum mutual information as

$$I(\rho_{AB}) = S(\rho_{AB}||\rho_A \otimes \rho_B)\,. \tag{39}$$

If the total correlations are quantified by a comparison of the state ρ_{AB} with the uncorrelated state $\rho_A \otimes \rho_B$ then it is intuitive to try and measure the quantum part of these correlations by a comparison of ρ_{AB} with the closest separable state - a classically correlated state devoid of quantum correlations. This approach gives rise to the general definition of the relative entropy of entanglement [26, 25, 46, 78] with respect to a set X as

$$E_R^X(\rho) := \inf_{\sigma\in X} S(\rho||\sigma). \tag{40}$$

This definition leads to a class of entanglement measures known as the *relative entropies of entanglement* (see [77] for a possible operational interpretation). In the bipartite setting the set X can be taken as the set of separable states, states with positive partial transpose, or non-distillable states, depending upon what you are regarding as 'free' states. In the multiparty setting there are even more possibilities [88, 46] but for each such choice a valid

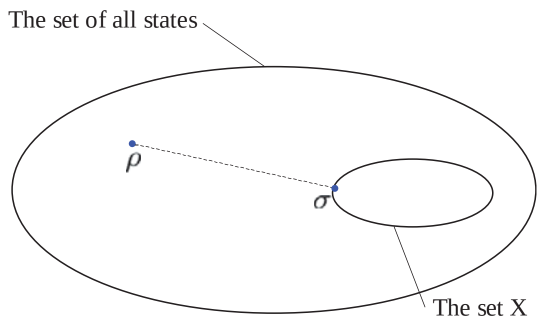

Fig. 5. The relative entropy of entanglement is defined as the smallest relative entropy distance from the state ρ to states σ taken from the set X. The set X may be defined as the set of separable states, non-distillable states or any other set that is mapped onto itself by LOCC.

entanglement measure is obtained as long as the set X is mapped onto itself under LOCC (one may even consider more general classes of operations as long as X is mapped onto itself). Employing the properties of the quantum relative entropy it is then possible to prove that it is a convex entanglement measure satisfying all the conditions 1 - 4 [26] which is also asymptotically continuous [89]. The bipartite relative entropies have been used to compute tight upper bounds to the distillable entanglement of certain states [90], and as an invariant to help decide the asymptotic interconvertibility of multipartite states [91, 92, 96]. The relative entropy of entanglement is bounded from below by the conditional entropy

$$E_R(\sigma) \geq \max\{S(\sigma_A), S(\sigma_B)\} - S(\sigma_{AB})$$

which can be obtained from the fact that for any bi-partite non-distillable state ρ we have

$$\begin{aligned} S(\sigma_A) + S(\sigma_A||\rho_A) &\leq S(\sigma_{AB}) + S(\sigma_{AB}||\rho_{AB}), \\ S(\sigma_B) + S(\sigma_B||\rho_B) &\leq S(\sigma_{AB}) + S(\sigma_{AB}||\rho_{AB}). \end{aligned}$$

The relative entropy measures are generally not additive, as bipartite states can be found where

$$E_R^X(\rho^{\otimes n}) \neq \; nE_R^X(\rho). \tag{41}$$

The regularized relative entropy of entanglement

$$E_{R,X}^{\infty} := \lim_{n\to\infty} \frac{E_R^X(\rho^{\otimes n})}{n}$$

is therefore of some interest. In various cases exhibiting a high degree of symmetry the regularised versions of some relative entropy measures can be calculated employing ideas from semi-definite programming and optimization theory [97]. These cases include the *Werner states*, i.e. states that are invariant under the action of unitaries of the form $U\otimes U$, and which take the form $\sigma(p) = p\sigma_a + (1-p)\sigma_s$, where $p \in (1/2, 1]$ and σ_a (σ_s) are states proportional to the projectors onto the anti-symmetric (symmetric) subspace. It can be shown that [90]

$$E_{R,PPT}^{\infty}(\sigma(p)) = \begin{cases} 1 - H(p), & p \leq \frac{d+2}{2d} \\ \lg\frac{d+2}{d} + (1-p)\lg\frac{d-2}{d+2}, & p > \frac{d+2}{2d} \end{cases} \tag{42}$$

where $H(p) = -p \lg p - (1-p)\lg(1-p)$. It is notable that while this expression is continuous in p it is not differentiable for $p = 1/2 + 1/d$. These results can be extended to the more general class of states that is invariant under the action of $O \otimes O$, where O is an orthogonal transformation [98].

Other distance based measures – In eq. (40) one may consider replacing the quantum relative entropy by different distance measures to quantify how far a particular state is from a chosen set of disentangled states. Many interesting examples of other functions that can be used for this purpose may be found in the literature (see e.g. [25, 26, 99]). It is also worth noting that the relative entropy functional is *asymmetric*, in that $S(\rho||\sigma) \neq S(\sigma||\rho)$. This is connected with asymmetries that can occur in the discrimination of probability distributions [26]. One can consider reversing the arguments and tentatively define an LOCC monotone $J^X(\rho) := \inf\{S(\sigma||\rho) : \sigma \in X\}$. The resulting function has the advantage of being additive, but unfortunately it has the problem that it can be infinite on pure states [100]. An additive measure that does not suffer from this deficiency will be presented later on in the form of the 'squashed' entanglement.

• *The Distillable Secret Key–* The Distillable Secret Key, $K_D(\rho)$, quantifies the asymptotic rate at which Alice and Bob may distill secret classical bits from many copies of a shared quantum state. Alice and Bob may use a shared quantum state to distribute a classical bit of information - for instance if they share a state $1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)$, then they may measure it in the $|0\rangle, |1\rangle$ basis to obtain an identical classical bit $0, 1$, which could form the basis of a cryptographic protocol such as one-time pad (see e.g. [10] for a description of one-time pad). However,if we think of a given bipartite mixed state ρ_{AB} as the reduction of a pure state held between Alice, Bob, and a malicious third party Eve, then it is possible that Eve could obtain information about the secret bit from measurements on her subsystem. In defining K_D it is assumed that each copy of ρ_{AB} is purified *independently* of the other copies. If we reconsider the example of the state $1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)$, we can easily see that it is not secure. For instance, it could actually be a reduction of a GHZ state $|000\rangle + |111\rangle$ held between Alice, Bob and Eve, in which case Eve could also have complete information about the 'secret' bit. The quantity K_D is hence zero for this state, and is in fact zero for all separable states.

One way of getting around the problem of Eve is to use entanglement distillation. If Alice and Bob distill bipartite pure states, then because pure states must be uncorrelated with any environment, any measurements on those pure states will be uncorrelated with Eve. Moreover, if the distilled pure states are EPR pairs, then because each local outcome $|0\rangle, |1\rangle$ occurs with equal probability, each EPR pair may be used to distribute exactly 1 secret bit of information. This means that $K_D(\rho) \geq D(\rho)$. However, entanglement distillation is not the only means by which a secret key can be distributed, it examples of PPT states are known where $K_D(\rho) > 0$, even though $D(\rho) = 0$ for all PPT states [101]. It has also been shown that the regularized relative entropy with respect to separable states is an upper bound to the distillable secret key, $E^{\infty}_{R,SEP}(\rho) \geq K_D(\rho)$ [101].

• *Logarithmic Negativity* – The partial transposition with respect to party B of a bipartite state ρ_{AB} expanded in a given local orthonormal basis as $\rho = \sum \rho_{ij,kl} |i\rangle\langle j| \otimes |k\rangle\langle l|$ is defined as

$$\rho^{T_B} := \sum_{i,j,k,l} \rho_{ij,kl} |i\rangle\langle j| \otimes |l\rangle\langle k|. \tag{43}$$

The spectrum of the partial transposition of a density matrix is independent of the choice of local basis, and is independent of whether the partial transposition is taken over party A or party B. The positivity of the partial transpose of a state is a necessary condition for separability, and is sufficient to prove that $E_D(\rho) = 0$ for a given state [102, 103, 104]. The quantity known as the *Negativity* [105, 73], $N(\rho)$, is an entanglement monotone [106, 107, 108, 65] that attempts to quantify the negativity in the spectrum of the partial transpose. We will define the Negativity as

$$N(\rho) := \frac{||\rho^{T_B}|| - 1}{2}, \tag{44}$$

where $||X|| :=\text{tr}\sqrt{X^\dagger X}$ is the trace norm. While being a convex entanglement monotone, the negativity suffers the deficiency that it is not additive. A more suitable choice for an entanglement monotone may therefore be the so called *Logarithmic Negativity* which is defined as

$$E_N(\rho) := \log_2 ||\rho^{T_B}|| \,. \tag{45}$$

The monotonicity of the negativity immediately implies that E_N is an entanglement monotone that cannot increase under the more restrictive class of deterministic LOCC operations, ie $\Phi(\rho) = \sum_i A_i \rho A_i^\dagger$. While this is not sufficient to qualify as an entanglement monotone it can also be proven that it is a monotone under probabilistic LOCC transformations [65]. It is additive by construction but fails to be convex. Although E_N is manifestly continuous, it is not asymptotically continuous, and hence does not reduce to the entropy of entanglement on all pure states.

The major practical advantage of E_N is that it can be calculated very easily. In addition it also has various operational interpretations as an upper bound to $E_D(\rho)$, a bound on teleportation capacity [108], and an asymptotic entanglement cost for exact preparation under the set of PPT operations [19].

- *The Rains bound* – The logarithmic negativity, E_N, can also been combined with a relative entropy concept to give another monotone known as the *Rains' Bound* [17], which is defined as

$$B(\rho) := \min_{all\ states\ \sigma} \left[S(\rho||\sigma) + E_N(\sigma) \right] . \tag{46}$$

The function $S(\rho||\sigma) + E_N(\sigma)$ that is to be minimized is not convex which suggests the existence of local minima making the numerical minimization infeasible. Nevertheless, this quantity is of considerable interest as one can observe immediately that $B(\rho)$ is a lower bound to $E_R^{PPT}(\rho)$ as $E_N(\sigma)$ vanishes for states σ that have a positive partial transpose. It can also be shown that $B(\rho)$ is an upper bound to the Distillable Entanglement. It is interesting to observe that for Werner states $B(\rho)$ happens to be equal to $\lim_{n\to\infty} E_R^{PPT}(\rho^{\otimes n})/n$ [90, 17], a connection that has been explored in more detail in [98, 19, 110].

- *Squashed entanglement* – Another interesting entanglement measure is the squashed entanglement [47] (see also [111]) which is defined as

$$
\begin{aligned}
&E_{sq} := \inf \left[\frac{1}{2} I(\rho_{ABE}) \quad : \ \mathrm{tr}_E\{\rho_{ABE}\} = \rho_{AB} \right] \\
&\text{where :} \\
&I(\rho_{ABE}) := S(\rho_{AE}) + S(\rho_{BE}) - S(\rho_{ABE}) - S(\rho_E)\,.
\end{aligned}
$$

In this definition $I(\rho_{ABE})$ is the *quantum conditional mutual information*, which is often also denoted as $I(A;B|E)$. The motivation behind E_{sq} comes from related quantities in classical cryptography that determine correlations between two communicating parties and an eavesdropper. The squashed entanglement is a convex entanglement monotone that is a lower bound to $E_F(\rho)$ and an upper bound to $E_D(\rho)$, and is hence automatically equal to $S(\rho_A)$ on pure states. It is also additive on tensor products, and is hence a useful non-trivial lower bound to $E_C(\rho)$. It has furthermore been proven that the squashed entanglement is continuous [109], which is a non-trivial statement because in principle the minimization must be carried out over *all* possible extensions, including infinite dimensional ones. Note that despite the complexity of the minimization task one may find upper bounds on the squashed entanglement from explicit guesses which can be surprisingly sharp. For the totally anti-symmetric state σ_a for two qutrits one obtains immediately (see Example 9 in [47]) that $E_D(\sigma_a) \leq E_{sq}(\sigma_a) \leq \log_2 \sqrt{3}$ which is very close to the sharpest known upper bound on the distillable entanglement for this state which is $\log_2 5/3$ [17, 90]. The Squashed entanglement is also known to be lockable [47, 7], and is an upper bound to the secret distillable key [7].

- *Robustness quantities and norm based monotones* – This paragraph discusses various other approaches to entanglement measures and then moves on to demonstrate that they and some of the measures discussed previously can actually be placed on the same footing.

Robustness of Entanglement – Another approach to quantifying entanglement is to ask how much noise must be mixed in with a particular quantum state before it becomes separable. For example

$$P(\rho) := \inf_{\sigma}\{\lambda \,|\, \sigma \,\text{a state}\,;\ (1-\lambda)\rho + \lambda\sigma \ \in \ SEP\,;\ \lambda \geq 0\} \tag{47}$$

measures the minimal amount of *global* state σ that must be mixed in to make ρ separable. Despite the intuitive significance of equation (47), for mathematical reasons it is more convenient to parameterize this noise in a different way:

$$
\begin{aligned}
R_g(\rho) :=& \quad \inf t \\
\text{such that}& \quad t \geq 0 \\
\text{and}& \quad \exists \text{ a state } \sigma \\
\text{such that}& \quad \rho + t\sigma \text{ is separable.}
\end{aligned}
$$

This quantity, R_g, is known as the *Global Robustness* of entanglement [57], and is monotonically related to $P(\rho)$ by the identity $P(\rho) = R_g(\rho)/(1 + R_g(\rho))$. However, the advantage of using $R_g(\rho)$ rather than $P(\rho)$ is that the first quantity has very natural mathematical properties that we shall shortly discuss. The global robustness mixes in arbitrary noise σ to reach a separable state, however, one can also consider noise of different forms, leading to other forms of robustness quantity. For instance the earliest such quantity to be defined, which is simply called the *Robustness*, R_s, is defined exactly as R_g except that the noise σ must be drawn from the set of separable states [112, 113, 119]. One can also replace the set of separable states in the above definitions with the set of PPT states, or the set of non-distillable states. The robustness monotones can often be calculated or at least bounded non-trivially, and have found applications in areas such as bounding fault tolerance [57, 58].

Best separable approximation – Rather than mixing in quantum states to destroy entanglement one may also consider the question of how much of a separable state is contained in an entangled state. The ensuing monotone is known as the *Best Separable Approximation* [114], which we define as

$$\begin{aligned} BSA(\rho) := \quad & \inf \mathrm{tr}\{\rho - A\} \\ \text{such that} \quad & A \geq 0\ ;\ A \in SEP \\ \text{and} \quad & (\rho - A) \geq 0. \end{aligned}$$

This measure is not easy to compute analytically or numerically. Note however, that replacing the set SEP by the set PPT allows us to write this problem as a semidefinite programme [97] for which efficient algorithms are known.

One shape fits all – It turns out that the robustness quantities, the best separable approximation as well as the negativity are all part of a general family of entanglement monotones. Such connections were first observed in [108], where it was noted that the Negativity and Robustness are part of a general family of monotones that can be constructed via a concept known as a *base norm* [115]. We will explain this connection in the following. However, our discussion will deviate a little from the arguments presented in [108], as this will allow us to include a wider family of entanglement monotones such as $R_g(\rho)$ and $BSA(\rho)$.

To construct this family of monotones we require two sets X, Y of operators satisfying the following conditions: (a) X, Y are closed under LOCC operations (even measuring ones), (b) X, Y are convex cones (i.e. also closed under multiplication by non-negative scalars), (c) each member of $X\,(Y)$ can be written in the form $\alpha_{X(Y)}\times$positive-semidefinite operator, where $\alpha_{X\,(Y)}$ are fixed real constants, and (d) any Hermitian operator h may be expanded as:

$$h = a\Omega - b\Delta \tag{48}$$

where $\Omega \in X, \Delta \in Y$ are normalised to have trace α_X, α_Y respectively, and $a, b \geq 0$. Given two such sets X, Y and any state ρ we may define an entanglement monotone as follows:

$$R_{X,Y}(\rho) := \inf_{\Omega \in X, \Delta \in Y} \{b \quad | \ \rho = a\Omega - b\Delta, a, b \geq 0\} \tag{49}$$

Note that if Ω, Δ are also constrained to be quantum states (i.e. $\alpha_X = \alpha_Y = 1$), then we may rewrite this equation:

$$\begin{aligned} & R_{X,Y}(\rho) = \\ & \inf\{b \mid b \geq 0,\ \exists \Delta \in Y, \Omega \in X \text{ s.t. } \frac{\rho + b\Delta}{1+b} = \Omega\} \end{aligned}$$

Hence equation (49) defines a whole family of quantities that have a similar structure to robustness quantities.

In the more general case where $\alpha_X, \alpha_Y \neq 1$, the quantities $R_{X,Y}(\rho)$ will not be robustness measures, but they will still be entanglement monotones. This can be shown as follows, where we will suppress the subscripts $_{X,Y}$ for clarity. Suppose that a LOCC operation acts on ρ to give output $\rho_i = \Lambda_i(\rho)/q_i$ with probability q_i. Suppose also that the optimum expansion of the initial state ρ is:

$$\rho = a\Omega - R\Delta$$

Then the output ensemble can be written as:

$$\begin{aligned} & \{q_i \ ; \ \frac{a\Lambda_i(\Omega) - R\Lambda_i(\Delta)}{q_i}\} \\ \equiv \quad & \{q_i \ ; \ \tilde{a}_i \frac{\alpha_X \Lambda_i(\Omega)}{\mathrm{tr}\{\Lambda_i(\Omega)\}} - \tilde{R}_i \frac{\alpha_Y \Lambda_i(\Delta)}{\mathrm{tr}\{\Lambda_i(\Delta)\}}\} \end{aligned} \tag{50}$$

where

$$\tilde{a}_i = \frac{a\,\mathrm{tr}\{\Lambda_i(\Omega)\}}{\alpha_X q_i} \quad ; \quad \tilde{R}_i = \frac{R\,\mathrm{tr}\{\Lambda_i(\Delta)\}}{\alpha_Y q_i}$$

Now because of the structure of each operator in X, Y, we have that $\tilde{a}_i, \tilde{R}_i \geq 0$, and hence for each outcome i the expansion in (50) is a valid decomposition. This means that the average output entanglement satisfies:

$$\sum_i q_i R(\rho_i) \leq \sum_i q_i \tilde{R}_i = R \sum_i \frac{\mathrm{tr}\{\Lambda_i(\Delta)\}}{\alpha_Y} = R \tag{51}$$

and hence the $R_{X,Y}$ give entanglement monotones. It is also not difficult to show that the $R_{X,Y}$ are convex functions. In the case that the two sets X and Y are identical, then the quantity

$$||h||_{X,X} := \inf_{\Omega,\Delta \in X} \{a + b \mid h = a\Omega - b\Delta, a, b \geq 0\}\,.$$

can be shown to be a norm, and in fact it is a norm of the so-called *base norm* kind. As $||h||_{X,X}$ can be written as a simple function of the corresponding $R_{X,X}$, this gives the robustness quantities a further interesting mathematical structure.

All the monotones mentioned at the beginning of this subsection fit into this family - the '*Robustness*' arises when both X, Y are the set of separable operators; the '*Best Separable approximation*' arises when X is the set of separable operators, Y is the set {positive semi-definite operators$\times -1$}; the global robustness arises when X is the set of separable operators, Y is the set of all positive semidefinite operators [112, 113, 119, 57]; the Negativity arises when $||\rho||_{X,Y}$ where both X, Y are the set of normalised Hermitian matrices with positive partial transposition. Note that the '*Random Robustness*' is not a monotone and so does not fit into this scheme, for definition and proof of non-monotonicity see [112, 113].

The greatest cross norm monotone – Another form of norm based entanglement monotone is the *cross norm* monotone proposed in [116, 117, 118]. The *greatest cross norm* of an operator A is defined as:

$$||A||_{\mathrm{gcn}} := \inf \left[\sum_{i=1}^{n} ||u_i||_1 ||v_i||_1 \ : \ A = \sum_i u_i \otimes v_i \right] \tag{52}$$

where $||y||_1 := \mathrm{tr}\{\sqrt{y^\dagger y}\}$ is the trace norm, and the infimum is taken over all decompositions of A into finite sums of product operators. For finite dimensions it can be shown that a density matrix ρ_{AB} is separable iff $||\rho||_{\mathrm{gcn}}=1$, and that the quantity:

$$E_{\mathrm{gcn}}(\rho) := ||\rho||_{\mathrm{gcn}} - 1 \tag{53}$$

is an entanglement monotone [116, 117, 118]. As it is expressed as a complicated variational expression, $E_{\mathrm{gcn}}(\rho)$ can be difficult to calculate. However, for pure states and cases of high symmetry it may often be computed exactly. Although $E_{\mathrm{gcn}}(\rho)$ does not fit precisely into the family of base norm monotones discussed above, there is a relationship. If the sum in (52) is restricted to *Hermitian* u_i and v_i (which is of course only allowed if A is Hermitian), then we recover precisely the base norm $||A||_{X,Y}$, where X, Y are taken as the set of separable states. Hence E_{gcn} is an upper bound to the robustness [116, 117, 118].

• *Entanglement Witness monotones* – Entanglement Witnesses are tools used to try to determine whether a state is separable or not. A Hermitian operator W is defined as an Entanglement Witness if:

$$\begin{aligned} \forall\, \rho \in SEP \qquad & \mathrm{tr}\{W\rho\} \geq 0 \\ & \textit{and} \\ \exists \rho \;\text{ s.t.} \qquad & \mathrm{tr}\{W\rho\} < 0. \end{aligned} \tag{54}$$

Hence W acts as a linear hyperplane separating some entangled states from the convex set of separable ones. Many entanglement witnesses are known, and in fact the CHSH inequalities

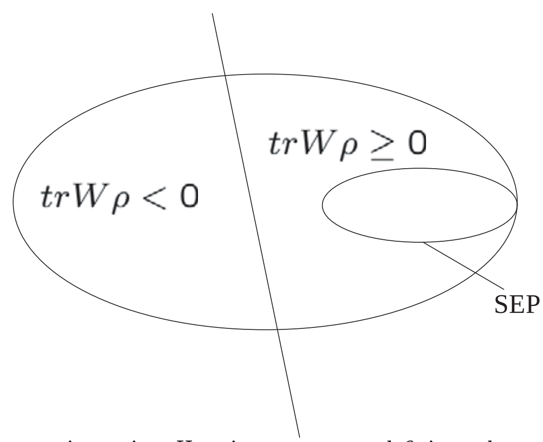

Fig. 6. An entanglement witness is a Hermitean operator defining a hyperplane in the space of positive operators such that for all separable states we have $trW\rho \geq 0$ and there is a ρ for which $trW\rho < 0$.

are well known examples. One can take a suitable Entanglement Witness (EW) and use the amount of 'violation'

$$E_{wit}(W) = \max\{0, -\mathrm{tr}\{W\rho\}\} \tag{55}$$

as a measure of the non-separability of a given state. Many entanglement monotones can be constructed by choosing (bounded) sets of of EWs and defining monotones as the minimal violation over all witnesses taken from the chosen set - see e.g. [119]. It turns out that this approach also offers another unified way of understanding the robustness and negativity measures discussed in the previous item [119].

This concludes our short survey of basic entanglement measures. Our review has mostly been formulated for two-party systems with finite dimensional constituents. In the remaining two subsections we will briefly summarize the problems that we are faced with in more general settings - where we are faced with more parties and infinite dimensional systems. We will present some of the results that have been obtained so far, and highlight some unanswered questions.

6 Infinite dimensional systems

In the preceding sections we have explicitly considered only finite dimensional systems. However, one may also develop a theory of entanglement for the infinite dimensional setting. This setting is often also referred to as the *continuous variable* regime, as infinite dimensional pure states are usually considered as wavefunctions in continuous position or momentum variables. The quantum harmonic oscillator is an important example of a physical system that needs to be described in an infinite dimensional Hilbert space, as it is realized in many experimental settings, e.g. as modes of quantized light.

General states – A naive approach to infinite dimensional systems encounters several complications, in particular with regards to continuity. Firstly, we will need to make some minimal requirements on the Hilbert space, namely that the system has the property that $\mathrm{tr}\{\exp^{H/T} < \infty\}$ where H is a Hamltonian without limit points in the spectrum [119]. It turns out that demanding this technical requirement enables one to avoid certain types of pathological behaviour [120]. The harmonic oscillator is an example of a system satisfying this constraint. Even so, without further constraints, entanglement measures cannot be continuous because by direct construction one may demonstrate that in any arbitrarily small neighborhood of a pure product state, there exist pure states with *arbitrarily strong* entanglement as measured by the entropy of entanglement [121]. The following example makes this explicit. Chose $\sigma_0 = |\psi_0\rangle\langle\psi_0|$ where $|\psi_0\rangle = |\phi_A^{(0)}\rangle \otimes |\phi_B^{(0)}\rangle$, and consider a sequence of pure states $\sigma_k = |\psi_k\rangle\langle\psi_k|$ defined by

$$|\psi_k\rangle \quad = \quad \sqrt{1-\epsilon_k}|\psi_0\rangle + \sqrt{\frac{\epsilon_k}{k}} \sum_{n=1}^{k} |\phi_A^{(n)}\rangle \otimes |\phi_B^{(n)}\rangle, \tag{56}$$

where $\epsilon_k = 1/\log(k)^2$ and $\{|\phi_{A/B}^{(n)}\rangle : n \in \mathbb{N}_0\}$ are orthonormal bases. Then $\{\sigma_k\}_{k=1}^{\infty}$ converges to σ_0 in trace-norm, i.e., $\lim_{k\to\infty} \|\sigma_k - \sigma_0\|_1 = 0$ while $\lim_{k\to\infty} E(\sigma_k) = \infty$. Obviously, E is not continuous around the state σ_0.

However, this perhaps surprising feature can only occur if the mean energy of the states σ_k grows unlimited in k. If one imposes additional constraints such as restricting attention to states with bounded mean energy then one finds that the continuity of entanglement measures can be recovered [121]. More precisely, given the Hamiltonian H and the set $\mathcal{S}_M = \{\rho \in \mathcal{S} | tr[\rho H] \leq M\}$ where $\mathcal{S}$ is the set of all density matrices, then we find for example that for $\sigma \in \mathcal{S}_M(\mathcal{H})$, $M > 0$, being a pure state that is supported on a finite-dimensional subspace of $\mathcal{S}(\mathcal{H})$, and $\{\sigma_n\}_{n=1}^{\infty}$, $\sigma_n \in \mathcal{S}_{nM}(\mathcal{H}^{\otimes n})$, being a sequence of states satisfying

$$\lim_{n\to\infty} \|\sigma_n - \sigma^{\otimes n}\| = 0, \tag{57}$$

then

$$\lim_{n\to\infty} \frac{|E_F(\sigma^{\otimes n}) - E_F(\sigma_n)|}{n} = 0. \tag{58}$$

Similar statements hold true for the entropy of entanglement and the relative entropy of entanglement. The technical details can be found in [121]. Even with this constraint however, the description of entanglement and its quantification is extraordinarily difficult, although some concrete statements can be made [122]. Note however, that for continuous entanglement measures that are strongly super-additive (in the sense of eq. (26) in the situation given in fig. 3) one can provide lower bounds on entanglement measures in terms of a simpler class of state, the Gaussian states [123]. This motivates the consideration of more constrained sets of states.

Gaussian states – A further simplification that can be made is to consider only the set of *Gaussian* quantum states. This set of states is important because not only do they play a key role in several fields of theoretical and experimental physics, but they also have some attractive mathematical features that enable many interesting problems to be tackled using basic tools from linear algebra. We will concentrate on this class of states, as they have been subject to the most progress. The systems that are being considered possess n canonical degrees of freedom representing for example n harmonic oscillators, or n field modes of light. These canonical operators are usually arranged in vector form

$$O = (O_1, \ldots, O_{2n})^T = (X_1, P_1, \ldots, X_n, P_n)^T. \tag{59}$$

Then the canonical commutation relations take the form $[O_j, O_k] = i\sigma_{j,k}$, where we define the *symplectic* matrix as follows:

$$\sigma := \bigoplus_{j=1}^{n} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{60}$$

States ρ may now also be characterized by functions that are defined on phase space. Given a vector $\xi \in \mathbb{R}^{2n}$, the Weyl or Glauber operator is defined as:

$$W_\xi = e^{i\xi^T \sigma O}. \tag{61}$$

These operators generate displacements in phase space, and are used to define the *characteristic function* of ρ:

$$\chi_\rho(\xi) = \mathrm{tr}[\rho W_\xi]. \tag{62}$$

This can be inverted by the transformation [124]:

$$\rho = \frac{1}{(2\pi)^n} \int d^{2n}\xi \chi_\rho(-\xi) W_\xi, \tag{63}$$

and hence the characteristic function uniquely specifies the state. Gaussian states are now defined as those states whose characteristic function is a Gaussian [9], i.e.,

$$\chi_\rho(\xi) = \chi_\rho(0) e^{-\frac{1}{4}\xi^T \Gamma \xi + D^T \xi}, \tag{64}$$

where Γ is a $2n \times 2n$-matrix and $D \in \mathbb{R}^{2n}$ is a vector. In defining Gaussian states in this way it is easy to see that the reduced density matrix of any Gaussian state is also Gaussian - to compute the characteristic function of a reduced density matrix we simply set to zero any components of ξ corresponding to the modes being traced out.

As a consequence of the above definition, a Gaussian characteristic function can be characterized via its first and second moments only, such that a Gaussian state of n modes requires only $2n^2+n$ real parameters for its full description, which is polynomial rather than exponential in n. The first moments form the displacement vector $d_j = \langle O_j \rangle_\rho = \mathrm{tr}[O_j \rho]$ $j = 1, ..., 2n$ which is linked to the above D by $D = \sigma d$. They can be made zero by means of a unitary translation in the phase space of individual oscillators and carry no information about the entanglement properties of the state.

The second moments of a quantum state are defined as the expectation values $\langle O_j O_k \rangle$. Because of the canonical commutation relationships the value of $\langle O_k O_j \rangle$ is fixed by the value of $\langle O_j O_k \rangle$ (the operators O_j,O_k either commute, or their commutator is proportional to the identity), and so all second moments can be embodied in the real symmetric $2n\times 2n$ covariance matrix γ which is defined as

$$\begin{aligned} \gamma_{j,k} &= 2\mathrm{Re}\,\mathrm{tr}\left[\rho\left(O_j - \langle O_j\rangle_\rho\right)\left(O_k - \langle O_k\rangle_\rho\right)\right] \\ &= \mathrm{tr}\left[\rho\left(\{O_j, O_k\} - 2\langle O_j\rangle_\rho \langle O_k\rangle_\rho\right)\right] \end{aligned} \tag{65}$$

where $\{\}$ denotes the anticommutator. The link to the above matrix Γ is $\Gamma = \sigma^T \gamma \sigma$. With this convention, the covariance matrix of the n-mode vacuum is simply $\mathbb{1}_{2n}$. Clearly, not all real symmetric $2n \times 2n$-matrix represent quantum states as these must obey the Heisenberg uncertainty relation. In terms of the second moments the 'uncertainty principle' can be written as the matrix inequality

$$\gamma + i\sigma \geq 0\,. \tag{66}$$

Note that for one mode this uncertainty principle is actually *stronger* than the usual Heisenberg uncertainty principle presented in textbooks, and in fact equation (66) is the strongest uncertainty relationship that may be imposed on the 2nd-moments $\langle O_j O_k \rangle$. This is because it turns out that *any* real symmetric matrix γ satisfying the uncertainty principle (66) corresponds to a valid quantum state. Proving equation (66) is actually not too difficult [125, 126] - we start with a $2n$ component vector of complex numbers y, and define an operator $Y := \sum_j y_j (O_j - \langle O_j \rangle)$. Then the positivity of ρ implies that $\mathrm{tr}\{\rho Y^\dagger Y\} \geq 0 \,\forall\, y$. A little algebra, and use of the canonical commutation relationships, shows that $\mathrm{tr}\{\rho Y^\dagger Y\} \geq 0 \,\forall\, y \;\Leftrightarrow\; \gamma + i\sigma \geq 0$.

This observation has quite significant implications concerning the separability of two-mode Gaussian states shared by two parties. Indeed, a necessary condition for the separability of Gaussian states can be formulated on the basis of the partial transposition, or more precisely partial time reversal, expressed on the level of covariance matrices. In a system with canonical degrees of freedom time reversal is characterized by the transformation that leaves the positions invariant but reverses the relevant momenta $X \mapsto X,\ P \mapsto -P$. It can be shown that a two-party Gaussian state is separable exactly if the covariance matrix corresponding to the partially transposed state again satisfies the uncertainty relations [127, 128, 129, 130, 131]. More advanced questions concerning the interconvertibility of pairs of states under local operations can also often be answered fully in terms of the elements of the covariance matrix [132, 133, 134, 136]. In particular, the question of the interconvertability of pure bi-partite Gaussian states of an arbitrary number of modes can be decided in full generality [136].

Gaussian operations – The development of the theory of entanglement of Gaussian states requires also the definition of the concept of Gaussian operations. Gaussian operations may be defined as those operations that map *all* Gaussian input states onto a Gaussian output state. This definition is not constructive but fortunately more useful characterizations exist. Physically useful is the fact that Gaussian operations correspond exactly to those operations that can be implemented by means of optical elements such as beam splitters, phase shifts and squeezers together with homodyne measurements [134, 133, 137].

The most general real linear transformation S which implements the mapping

$$S : O \longmapsto O' = SO \tag{67}$$

will have to preserve the canonical commutation relations $[O'_j, O'_k] = i\sigma_{jk}\mathbb{1}$ which is exactly the case if S satisfies

$$S\sigma S^T = \sigma\,. \tag{68}$$

This condition is satisfied by the real $2n\times 2n$ matrices S that form the so-called real symplectic group $Sp(2n,\mathbb{R})$. Its elements are called symplectic or canonical transformations. It is useful to know that any orthogonal transformation is symplectic. To any symplectic transformation S also $S^T, S^{-1}, -S$ are symplectic. The inverse of S is given by $S^{-1} = \sigma S^T \sigma^{-1}$ and the determinant of every symplectic matrix is $\det[S] = 1$ [139, 138]. Given a real symplectic transformation S there exists a unique unitary transformation U_S acting on the state space such that the Weyl operators satisfy $U_S W_\xi U_S^\dagger = W_{S\xi}$ for all $\xi \in \mathbb{R}^2$. On the level of covariance matrices γ of an n-mode system a symplectic transformation S is reflected by a congruence

$$\gamma \longmapsto S\gamma S^T. \tag{69}$$

Generalized Gaussian quantum operations may also be defined analogously to the finite dimensional setting, ie by appending Gaussian state ancillas, performing joint Gaussian unitary evolution followed by tracing out the ancillas or performing homodyne detection on them [134, 133, 137, 9].

Normal forms – Given a group of transformations on a set of matrices it is always of great importance to identify normal forms for matrices that can be achieved under this group of transformations. Of further interest and importance are invariants under the group transformations. For the set of Hermitean matrices and the full unitary group these correspond to the concepts of diagonalization and eigenvalues. In the setting of covariance matrices and the symplectic group we are led to the Williamson normal forms and the concept of symplectic eigenvalues. Indeed, Williamson [140] (see [126] for a more easily accessible reference) proved that for any covariance matrix Γ on n harmonic oscillators there exists a symplectic transformation S such that

$$S\Gamma S^T = \bigoplus_{j=1}^{n} \begin{pmatrix} \mu_j & 0 \\ 0 & \mu_j \end{pmatrix} \tag{70}$$

The diagonal elements μ_i are the so-called *symplectic eigenvalues* of a covariance matrix Γ which are the invariants under the action of the symplectic group. The set $\{\mu_1, \dots, \mu_n\}$ is usually referred to as the *symplectic spectrum*. The symplectic spectrum can be obtained directly from the absolute values of the eigenvalues of $i\sigma^{-1}\Gamma$. The transformation to the Williamson normal form implements a normal mode decomposition thereby reducing any computational problem, such as the computation of the entropy, to that for individual uncoupled modes. Each block in the Williamson normal form represents a thermal state for which the evaluation of most physical quantities is straightforward.

Entanglement quantification – Equipped with these tools we may now proceed to discuss the quantification of entanglement in the Gaussian continuous variable arena. Despite all the above technical tools the quantification of entanglement for Gaussian states is complicated and only very few measures may be defined let alone computed.

• *Entropy of entanglement:* On the level of pure state we may again employ the entropy of entanglement which we may now express in terms of the covariance matrix. Assume Alice and Bob are in possession of $n_A + n_B$ harmonic oscillators in a Gaussian state described by the covariance matrix Γ and Alice holds n_A of these oscillators. Then it can be shown that the entropy of entanglement is given by

$$S = \sum_{i=1}^{n_A} \left(\frac{\mu_i + 1}{2} \log_2 \frac{\mu_i + 1}{2} - \frac{\mu_i - 1}{2} \log_2 \frac{\mu_i - 1}{2} \right) \tag{71}$$

where the μ_i are the *symplectic* eigenvalues of Alice's reduced state described by the covariance matrix Γ_A which is simply the submatrix of Γ referring to the system pertaining to Alice. These symplectic eigenvalues are, as remarked above, the positive eigenvalues of $i\sigma^{-1}\Gamma_A$. The proof of the above formula is obtained by transforming the covariance to its Williamson normal form and subsequently determine the entropy of the single mode states. Note that on the set of Gaussian states the entropy is evidently continuous and it can be shown that this remains the case for the set of states with bounded mean energy [121].

• *Entanglement of formation:* In the finite dimensional setting the defintion of the entanglement of formation has been unambiguous. In the Gaussian state setting however this is no longer the case. One may define the entanglement of formation of a Gaussian state either (i) with respect to decompositions in pure Gaussian states or (ii) with respect to decompositions in arbitrary pure states. In case (i) it has been proven that the so-defined entanglement of formation is an entanglement monotone under Gaussian operations and that it can be computed explicitly in the case where both parties hold a single harmonic oscillator each. Remarkably, this entanglement of formation is even additive for symmetric two-mode states [142]. For the case of a single copy of a mixed symmetric Gaussian two mode state it can also be demonstrated that the definition (i) coincides with definition (ii) [141, 142]. The entanglement of formation can be shown to be continuous for systems with energy constraint [143].

• *Distillable Entanglement:* The distillable entanglement in the continuous variable setting is, as expected, extremely difficult to compute. Furthermore, its definition is not unambiguous as one may define distillation with respect to (i) Gaussian operations only, or (ii) general quantum operations. It is remarkable that it has been proven that the setting (i) does not actually permit entanglement distillation at all [133, 134, 135]. Therefore, non-Gaussian operations need to be considered. Then, in setting (ii), for Gaussian states it can be shown to be continuous and interestingly it can also be demonstrated that for any ρ there exists a Gaussian state ρ_G with the same first and second moments such that $E_D(\rho_G) \leq D(\rho)$. Finding explicit procedures implementing distillation protocols is very difficult which makes it very difficult to determine lower bounds on the distillable entanglement. Various other measures of entanglement, such as those described below, may be used to find upper bounds on the distillable entanglement.

• *Relative entropy of entanglement:* As for the entanglement of formation there are now various possible definitions of the relative entropy of entanglement all of which are at least as difficult to compute as in the finite dimensional setting. If the relative entropy of entanglement should serve as a provable upper bound on the distillable entanglement under general LOCC, then it will have to be computed with respect to the set of separable general continuous variable states. This is obviously a very involved quantity and only known on pure states where it equals the entropy of entanglement. If one considers the relative entropy of entanglement of a state with bounded mean energy with respect to the unrestricted set of separable states, then it can be shown that the relative entropy of entanglement is continuous [121]. A more tractable setting is that of the relative entropy of entanglement with respect to the set of Gaussian separable states but in this case its interpretation is unclear.

• *Logarithmic negativity:* As in the finite dimensional setting, most entanglement measures are exceedingly difficult to compute. The exception is again the logarithmic negativity which is an entanglement monotone [65] but differs, on pure states, from the entropy of entanglement. For a system of $n = n_A + n_B$ harmonic oscillators in a Gaussian state described by the covariance matrix Γ, the logarithmic negativity can again be expressed in terms of symplectic eigenvalues. Indeed, considering the covariance matrix Γ^{T_B} of the partially transposed state we find

$$E_N = -\sum_{i=1}^{n} \log_2[\min(1, \tilde{\mu}_k)] \tag{72}$$

where the $\tilde{\mu}_k$ form the symplectic spectrum for the partially transposed state described by covariance matrix Γ^{T_B}, ie the symplectic eigenvalues. This formula is again proven by applying a normal mode decomposition, this time to the partially transposed covariance matrix, reducing the problem to a single mode question. It is interesting to note that on Gaussian states the logarithmic negativity also possesses an interpretation as a special type of entanglement cost [19].

The tools for the manipulation and quantification are used in the assessment of the quality of practical optical entanglement manipulation protocols. It should also be noted that these tools have been used successfully to study entanglement properties of quasi-free fields on lattices (i.e. lattices of harmonic oscillators) initiating the study of the scaling behaviour of entanglement between contiguous blocks in the ground state of interacting quantum systems [144]. The above methods and quantities permitted the rigorous proofs of the scaling of entanglement between contiguous blocks in the ground state of a linear harmonic chain with a Hamiltonian that is quadratic in position and momentum[144] and a rigorous connection between the entanglement of an arbitrary set of harmonic oscillators and its surrounding with the boundary area [145, 146]. This illustrates the usefulness of the results that have been obtained in continuous variable entanglement theory over the last years.

Multi-particle entanglement – Although the two-party setting has provided many interesting examples of quantum entanglement, the multiparty setting allows us to explore a much wider range of effects. Phenomena such as quantum computation especially when based on cluster states [147], entanglement enhanced measurements [148, 149], multi-user quantum communication [150, 151, 152, 153] and the GHZ paradox all require consideration of systems with more than two particles. For this reason it is important to investigate entanglement in the multi-party setting. We will proceed along similar lines to the bi-partite setting, first discussing briefly basic properties of states and operations and then describing various approaches to the quantification of multi-particle entanglement.

States and Operations – In the following we are going to concentrate again on local operations and classical communication whose definition extend straightforwardly to the multi-party setting. Some remarks will also be made concerning PPT operations which are here defined as operations that preserve ppt-ness of states across *all* possible bi-partite splits. That is, any three-party state shared between A, B and C that remains positive under partial transposition of particle A or B or C is mapped again onto a state with this property.

In the bi-partite setting we initiated our discussions with the identification of some general properties of multi-party entangled states such as the identification of disentangled states and maximally entangled states. At this stage crucial differences between the two-party and the multi-party setting become apparent. Let us begin by trying to identify the equivalent of the two-party maximally entangled states. In the bi-partite setting we already identified qubit states of the form $(|00\rangle + |11\rangle)/\sqrt{2}$ maximally entangled because every other qubit state can be obtained from it with certainty using LOCC only. One natural choice for a state with this property could be the GHZ-state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_C + |1\rangle_A|1\rangle_B|1\rangle_C). \tag{73}$$

This state has the appealing property that its entanglement across any bi-partite cut e.g. party A versus parties B and C assume the largest possible value of 1 ebit. Also, a local measurement in the $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ basis for example on party A allows us to create deterministically a maximally entangled two-party state of parties B and C. Then we can obtain any other two-party entangled state for parties B and C by LOCC. Unfortunately, however there are tri-partite entangled states that cannot be obtained from the GHZ state using LOCC alone. One such example is the W-state [154]

$$|W\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A|0\rangle_B|1\rangle_C + |0\rangle_A|1\rangle_B|0\rangle_C + |1\rangle_A|0\rangle_B|0\rangle_C). \tag{74}$$

Note however that LOCC operations applied to a GHZ-state allow us to approximate the W-state as closely as we like, albeit with decreasing success probability. In the four party setting however it can be shown that there are pairs of pure states that cannot even be obtained from each other approximately employing LOCC alone [155]. This clearly shows that on the single-copy level it is not possible to establish a generic notion of a maximally entangled state.

Of course we have already learnt in the bi-partite setting that the requirement of exact transformations on single copies can lead to phenomena such as incomparable states and does not yield a simple and unified picture of entanglement. In the bi-partite setting such a unified picture for pure state entanglement emerges however in the asymptotic setting of arbitrarily many identically prepared states. One might therefore wonder whether a similar approach will be successful in multi-partite systems. These hopes will be dashed in the following. In the asymptotic setting we would need to establish the possibility for the reversible interconversion in the asymtptotic setting. If that were possible we could rightfully claim that all tri-partite entanglement is essentially equivalent and only appears in different concentrations that we could then quantify unambiguously. The simplest situation that one may consider to explore this possibility is the interconversion between GHZ and the EPR pairs across parties AB, AC and BC, ie in the limit $N \to \infty$ we would like to see

$$|GHZ\rangle^{\otimes N} \leftrightharpoons |EPR\rangle_{AB}^{\otimes n_{AB}} \otimes |EPR\rangle_{AB}^{\otimes n_{AC}} \otimes |EPR\rangle_{AB}^{\otimes n_{BC}} . \tag{75}$$

To decide this question one needs to identify sufficiently many entanglement monotones. In the case of reversibility these entanglement monotones will remain constant. The local entropies represent such a monotone. These are not enough to decide the question but it turns out that $E_R(\rho_{AB}) + S(\rho_{AB})$, ie the sume of the relative entropy of entanglement of the reduction to two parties and the entanglement between these two parties and the third, is also an entanglement monotone in this setting. This is then sufficient to prove that the above process cannot be achieved reversibly [91]. This result suggests that as opposed to the bi-partite setting there is not such a simple and unique concept of a maximally entangled state in the multi-partite setting.

One may however try and and make progress by generalizing the idea of a single entangled state from which all other states can be obtained reversibly in the asymptotic setting. Instead one may consider a set of states from which all other state may be obtained asymptotically reversibly. The smallest such set is usually referred to as an MREGS which stands for Minimal Reversible Entanglement Generating Set [159]. It was natural to try and see whether the set $\{|GHZ\rangle_{ABC}, |EPR\rangle_{AB}, |EPR\rangle_{AC}, |EPR\rangle_{BC}\}$ is sufficient to generate the W-state reversibly. Unfortunately, even this conjecture was proved wrong [158, 92]. Similar results have also been obtained in the four-party setting [93]. Therefore, an MREGS would also have to contain the W-state as well. It is currently an open question whether under LOCC operations any finite MREGS actually exists.

In another approach to overcome the difficulties presented above one may consider extensions of the set of operations that is available for entanglement transformations. A natural generalization are PPT operations that have already made an appearance in the bi-partite setting. Adopting PPT operations indeed simplifies the situation somewhat. In the single copy setting any k-partite entangled state can be transformed, with finite success probability, into any other k-partite entangled state by PPT operations [94, 95]. The success probabilities can be surprisingly large, e.g. the transformation from GHZ to W state succeeds with more than 75% [94]. It is noteworthy that PPT operations also overcome the constraint that is imposed by the non-increase of the Schmidt-number under LOCC. Indeed, PPT operations (and also the use of LOCC with bound entanglement as a free resource) allow us to increase the Schmidt number. This result already implicit in [19] was made explicit in [19, 94]. It was hoped for that this strong increase in probabilities and the vanishing of the Schmidt number constraint would lead to reversibility in the multi-partite setting, ie a finite MREGS under PPT operations. This question is however still remains open [96].

Up until now we have restricted attention to pure multi-party entangled states. Now let us consider the definition of separable multi-particle states. The most natural definition for disentangled states arises from the idea that we call a state disentangled if we can create it from a pure product state by the action of LOCC only. This implies that separable states are of the form

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i \otimes ... \tag{76}$$

where the $A, B, C..$ label different parties. However, one can go beyond this definition. Indeed, the state $(|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2} \otimes |0\rangle_C$ is clearly entangled and therefore not separable in the above sense. However, it also does not exhibit three-party entanglement as the third party C is uncorrelated from the other two. Therefore may call this tri-partite state 2-entangled. One may now try and generalize this idea to mixed states. For example we could define as the set of 2-entangled states any ρ that may be written in the form

$$\rho = \sum_i p_i \rho_A^{(i)} \otimes \rho_{BC}^{(i)} + \sum_i q_i \rho_B^{(i)} \otimes \rho_{AC}^{(i)} + \sum_i r_i \rho_C^{(i)} \otimes \rho_{AB}^{(i)} \tag{77}$$

with positive p_i, q_i and r_i. Then, for N parties one may then define k-entangled states as a natural generalization of the above 3-party definition. While this definition appears natural it encounters problems when we consider several identical copies of states of the form given above. In that case one can obtain a 3-entangled state by LOCC acting on two copies of the above 2-entangled state. As a simple example consider a three party state where Alice has two qubits and Bob and Charlie each hold one. Then a state of the form: $\frac{1}{2}[|0\rangle\langle 0|_{A1} \otimes EPR(A2, B) \otimes |0\rangle\langle 0|_C + |1\rangle\langle 1|_{A1} \otimes |0\rangle\langle 0|_B \otimes EPR(A2, C)]$ is only 2-entangled. However, given two copies of this state the 'classical flag' particle $A1$ can enable Alice to obtain (with some probability) one EPR pair with Bob, and one with Charlie. She can then use these EPR pairs and teleportation to distribute any three party entangled state she chooses. States of three qubits displaying a similar phenomenon can also be constructed. Hence we are faced with a subtle dilemma - either this notion of 'k-entanglement' is not closed under LOCC, or it is not closed under taking many copies of states. Note however that these states may still have relevance for example in the study of fault-tolerant quantum computation [58].

Quantifying Multi-partite entanglement – Already in the bi-partite setting it was realized that there are many non-equivalent ways to quantify entanglement [72]. This concerned mainly the mixed state case, while in the pure state case the entropy of entanglement is a distinguished measure of entanglement. In the multipartite setting this situation changes. As was discussed above it appears difficult to establish a common currency of multipartite entanglement even for pure states due to the lack of asymptotically reversible interconversion of quantum states. The possibility to define k-entangled states and the ensuing ambiguities lead to additional difficulties in the definition of entanglement measures in multi-partite systems.

Owing to this there are many ways to go about quantifying multipartite entanglement. Some of these measures will be natural generalizations from the bi-partite setting while others will be specific to the multi-partite setting. These measures and their known properties will be the subject of the remainder of this section.

Entanglement Cost and Distillable Entanglement – In the bi-partite setting it was possible to define unambiguously the entanglement of pure states establishing a common "currency" for entanglement. This then formed the basis for unique definitions of the entanglement cost and the distillable entanglement. The distillable entanglement determined the largest rate, in the asymptotic limit, at which one may obtain pure maximally entangled states from an initial supply of mixed entangled states using LOCC only. However, in the multi-particle setting there is no unique target state that one may aim for. One may of course provide a target state specific definition of distillable entanglement, for example the largest rate at which one may prepare GHZ states [59], cluster states [60, 62] or any other class that one is interested in[156, 157] . As these individual resources are not asymptotically equivalent each of these measures will capture different properties of the state in question.

One encounters similar problems when attempting to define the entanglement cost. Again, one may use singlet states as the resource from which to construct the state by LOCC but one may also consider other resources such as GHZ or W states. For each of these settings one may then ask for the best rate at which one can create a target state using LOCC in the asymptotic limit. Therefore we obtain a variety of possible definitions of entanglement costs.

While the interpretation of each of these measures is clear it is equally evident that it is not possible to arrive at a unique picture from abstract considerations alone. The operational point of view becomes much more important as different resources may be readily available in different experimental settings and then motivating different definitions of the entanglement cost and the distillable entanglement.

• *Relative Entropic Measures. Distance measures* – In the bipartite setting we have discussed various distance based measures in which one minimizes the distance of a state with respect to a set of states that does not increase in size under LOCC. One such set was that of separable states and a particularly important distant measure is the relative entropy of entanglement. This lead to the relative entropy of entanglement. As we discussed in the first part of this section the most natural extension of the definition of separable states in the multipartite setting is given by

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i \otimes ... \tag{78}$$

where the $A, B, C..$ label different parties. In analogy with the bipartite definition one can hence define a multipartite relative entropy measure:

$$E_R^X(\rho) := \inf_{\sigma \in X} S(\rho||\sigma) \tag{79}$$

where X is now the set of multipartite separable states. As in the bipartite case the resulting quantity is an entanglement monotone which, for pure states, coincides with the entropy of entanglement. Therefore, on pure states, this measure is additive while it is known to be sub-additive on mixed states. Remarkably, the multipartite relative entropy of entanglement is *not* even additive for pure states - a counterexample is provided by the totally anti-symmetric state

$$|A\rangle = \frac{1}{\sqrt{6}} \sum_{ijk} \epsilon_{ijk} |ijk\rangle \tag{80}$$

where ϵ_{ijk} is the totally anti-symmetric tensor [96]. One can also compute the relative entropy of entanglement for some other tri-partite states. Examples of particular importance in this respect are the W-state for which we find

$$E_R|W\rangle = \log_2 \frac{9}{4} \tag{81}$$

and the states $|GHZ(\alpha)\rangle = \alpha|000\rangle + \beta|111\rangle$ for which we find

$$E_R|W\rangle = -|\alpha|^2 \log_2 |\alpha|^2 - |\beta|^2 \log_2 |\beta|^2 \,. \tag{82}$$

More examples can be found quite easily.

Also in our discussion of multi-partite entanglement we introduced the notion of k-entangled states. let us denote the set of k-entangled state of an N-partite system by $\mathcal{S}_k^N$. If ew explicitly consider the single copy setting, then it is clear that that the set $\mathcal{S}_k^N$ does not increase under LOCC. As a consequence it can be used as the basis for generalizations of the relative entropy of entanglement simply replacing the set X above by $\mathcal{S}_k^N$. We have learnt however that the set $\mathcal{S}_k^N$ may grow when allowing for two or more copies of the state. This immediately implies that the so constructed measure will exhibit sub-additivity again. Given that even the standard definition for the multi-partite relative entropy of entanglement is sub-additive this should not be regarded as a deficiency. Indeed, this subadditivity may be viewed as a strength as it could lead to particularly strong bounds on the associated distillable entanglement.

Exactly the same principle may be used to extend any of the distance based entanglement quantifiers to multi-party systems - one simply picks a suitable definition of the 'unentangled' set X (i.e. a set which is closed under LOCC operations, and complies with some notion of locality), and then defines the minimal distance from this set as the entanglement measure. As stated earlier, one may also replace the class of separable states with other classes of limited entanglement - e.g. states containing only bipartite entanglement. Such classes are *not* in general closed under LOCC in the many copy setting and so the resulting quantities may exhibit strong subadditivity and their entanglement monotonicity needs to be verified carefully.

• *Robustness measures. Norm based measures.* The robustness measures discussed in the bipartite case extend straightforwardly to the multiparty case. In the bipartite case we constructed the robustness monotones from two sets of operators X, Y that were closed under LOCC operations, and in addition satisfied certain convexity and 'basis' properties. To define analogous monotones in the multiparty case we must choose sets of multiparty operators that have these properties. One could for example choose the sets X, Y to be the set of k-separable positive operators, for any integer k.

• *Entanglement of Assistance. Localizable entanglement. Collaborative Localizable entanglement.* One way of characterizing the entanglement present in a multiparty state is to understand how local actions by the parties may generate entanglement between two distinguished parties. For example, in a GHZ state $1/\sqrt{2}(|000\rangle+|111\rangle)$ of three parties, it is possible to generate an EPR pair between any two parties using only LOCC operations - if one party measures in the $1/\sqrt{2}(|0\rangle \pm |1\rangle)$ basis, then there will be a residual EPR pair between the remaining two parties. This is the case even though the reduced state of the two parties is by itself unentangled. The first attempt to quantify this phenomenon was the *Entanglement of Assistance* proposed by [160]. The *Entanglement of Assistance* is a property of 3-party states, and quantifies the maximal bipartite entanglement that can be generated on average between two parties A, B if party C measures her particle and communicates the result to A, B. A related measure known as the *Localizable Entanglement* was proposed and investigated in [52, 53, 55, 54] for the general multiparty case - this is defined as the maximum entanglement that can be generated between two parties if all *remaining* n parties act using LOCC on the particles that they possess [51]. Both these measures require an underlying measure of bipartite entanglement to quantify the the entanglement between the two singled-out parties. In the original articles [160, 52] the pure state entropy of entanglement was used, however, one can envisage the use of other entanglement measures [161]. The Localizable Entanglement has been shown to have interesting relations to correlation functions in condensed matter systems [52, 53, 55, 54].

As multiparty entanglement quantifiers, both the Entanglement of Assistance and the Localizable entanglement have the drawback that they can deterministically *increase* under LOCC operations between all parties [161]. This phenomenon occurs because these measures are defined under the restriction that Alice and Bob cannot be involved in classical communication with any other parties - it turns out that in some situations allowing this communication can increase the entanglement that can be obtained between Alice and Bob [161]. This observation lead the authors of [161] to define the *Collaborative* Localizable Entanglement as the maximal bipartite entanglement (according to some chosen measure) that may be obtained (on average) between Alice and Bob using LOCC operations involving *all* parties. It is clear that by definition these collaborative entanglement measures are entanglement monotones.

It is interesting to note that although the bare Localizable entanglement is not a monotone, its regularised version *is* a monotone for multiparty pure states [162]. In [162] it is shown that the regularised version of the Localizable entanglement reduces to the minimal entropy of entanglement across any bipartite cut that divides Alice and Bob, which is clearly a LOCC monotonous quantity by the previous discussion of bipartite entanglement measures.

• *Geometric measure.* In the case of pure multiparty states one could try to quantify the 'distance' from the set of separable states by considering various functions of the maximal overlap with a product state [99]. One interesting choice of function is the logarithm. This was used in [163] to define the following entanglement quantifier:

$$G(|\psi\rangle) := -\log\left\{\sup(|\langle\psi|\alpha\otimes\beta\otimes\gamma...\rangle|^2)\right\}, \tag{83}$$

where the supremum is taken over all pure product states. This quantity is non-negative, equals zero iff the state $|\psi\rangle$ is separable, and is manifestly invariant under local unitaries. One can extend this quantity to mixed states using a convex roof construction. However G is not an entanglement monotone, and it is *not* additive for multiparty pure states [164]. Nevertheless, G is worthy of investigation as it has useful connections to other entanglement measures, and also has an interesting relationship with the question of channel capacity additivity [164]. We could also have described G as a norm based measure, as the quantity

$\sup(|\langle\psi|\alpha\otimes\beta\otimes\gamma...\rangle|)$ is a norm (of vectors) known to mathematicians as the *injective tensor norm* [165].

• *'Tangles' and related quantities. Entanglement quantification by local invariants.* An interesting property of bipartite entanglement is that it tends to be *monogamous*, in the sense that if three parties A, B, C have the same dimensions, and if two of the parties A and B are very entangled, then a third party C can only be weakly entangled with either A or B. If AB are in a singlet state then they cannot be entangled with C at all. In [166] this idea was put into the form of a rigorous inequality for three qubit states using a entanglement quantifier known as the *tangle*, $\tau(\rho)$. For a *qubit* $\times\, n$ dimensional systems the tangle is defined as

$$\tau(\rho) = \left\{ \inf \sum_i p_i C^2(|\psi_i\rangle\langle\psi_i|) \right\} \tag{84}$$

where $C^2(|\psi\rangle\langle\psi|)$ is the square of the concurrence of pure state $|\psi\rangle$ and the infimum is taken over all pure state decompositions. The concurrence can be used in this way as any pure state of a $2 \times n$ system is equivalent to a two qubit pure state. It has been shown that $\tau(\rho)$ satisfies the inequality [166, 167]

$$\tau(A:B) + \tau(A:C) + \tau(A:D) + ... \leq \tau(A:BCD...)$$

where the notation $A : X_1X_2...$ means that τ is computed across the bipartite splitting between party A and parties $X_1X_2...$ This shows that the amount of bipartite entanglement between party A and several individual parties $B, C, D, ..$ is bounded from above by the amount of bipartite entanglement between party A and parties $BCD...$ collectively.

In the case of three qubit pure states the *residual tangle*

$$\tau_3 = \tau(A:BC) - \tau(A:B) - \tau(A:C)$$

is a local-unitary invariant that is independent of which qubit is selected as party A, and might be proposed as a 'quantifier' of three party entanglement for pure states of 3-qubits. However, there are states with genuine three party entanglement for which the residual tangle can be zero (the W-state serves as an example [166]). However, the residual tangle can only be non-zero if there is genuine tripartite entanglement, and hence can be used as a indicator of three party entanglement.

Another way to construct multiparty entanglement measures for multi-qubit *pure* systems is simply to single out one qubit, compute the entanglement between that qubit and the rest of the system, and then average over all possible choices of the singled out qubit. As any *pure* bipartite system of dimensions $2 \times m$ can be written in terms of two Schmidt coefficients, one can apply all the formalism of two-qubit entanglement. This approach has been taken, for example, in the paper by Meyer and Wallach [168]. That the quantity proposed in [168] is essentially only a measure of the bipartite entanglement across various splittings was shown by Brennen [170]. Extensions of this approach are presented in [169].

Local unitary invariants: The residual tangle is only one of many *local* unitary invariants that have been developed for multiparty systems. Such local invariants are very important for understanding the structure of entanglement, and have also been used to construct prototype entanglement measures. Examples of local invariants that we have already mentioned are the Schmidt coefficients and the Geometric measure. In the multiparty case we may define the *local* invariants as those functions that are invariant under a *local* group transformation of fixed dimensions. If each particle is assumed for simplicity to have the same dimension d, then these local groups are of the form $A \otimes B \otimes C...$ where $A, B, C..$ are taken from a particular d-dimensional group representation such as the unitary group $U(d)$ or the group of invertible matrices $GL(d)$. The physical significance of the local $GL(d)$ invariants is that if two states have different values for such an invariant then they cannot even be interconverted probabilistically using stochastic LOCC ('SLOCC') operations. In the case of local unitary groups one typically only need consider invariants that are *polynomial* functions of the density matrix elements - this is because it can be shown that two states are related by a local unitary iff they have the same values on the set of polynomial invariants [171]. For more general groups a complete set of polynomial invariants cannot always be constructed, and one must also consider local invariants that are not polynomial functions of states - one example is a local GL invariant called the 'Schmidt rank', which is the minimal number of product state-vector terms in which a given multiparty pure state may be coherently expanded. It can be shown that one can construct an entanglement monotone (the 'Schmidt measure') as the convex-roof of the logarithm of this quantity [172].

Finding non-trivial local invariants is quite challenging in general and can require some sophisticated mathematics. However, for pure states of some dimensions it is possible to use such invariants to construct a variety of entanglement quantifiers in a similar fashion to the tangle. These quantifiers are useful for identifying different types of multiparty entanglement. We refer the reader to articles [171, 173, 174, 175, 176, 177, 178, 179] and references therein for further details.

7 Summary, Conclusions, and Open Problems

Quantum entanglement is a rich field of research. In recent years considerable effort has been expended on the characterization, manipulation and quantification of entanglement. The results and techniques that have been obtained in this research are now being applied not only to the quantification of entanglement in experiments but also, for example, for the assessment of the role of entanglement in quantum many body systems and lattice field theories. In this article we have surveyed many results from entanglement theory with an emphasis on the quantification of entanglement and basic theoretical tools and concepts. Proofs have been omitted but useful results and formulae have been provided in the hope that they prove useful for researchers in the quantum information community and beyond. It is the hope that this article will be useful for future research in quantum information processing, entanglement theory and its implications for other areas such as statistical physics.

Despite the tremendous progress in the characterisation of entanglement in recent years, there are still several major open questions that remain. Some significant open problems include:

Multiparty entanglement: The general characterisation of multiparty entanglement is a major open problem, and yet it is particularly significant for the study of quantum computation and the links between quantum information and many-body physics. Particular unresolved questions include:

- *Finiteness of MREGS for three qubit states* – In an attempt to achieve a notion of reversibility in the multi-partite setting, the concept of MREGS was introduced [159]. This was a set of N-partite states for fixed local dimension from which all other such states may be obtained asymptotically reversibly. It was hoped for that such a set may contain only a finite number of states. However, there are suggestions [91, 158, 92, 93] that this may not the case.

- *Distillation results for specific target states* – In the bi-partite setting the uniqueness of maximally entangled states led to clear definitions for the distillable entanglement. As outlined above this is not so in the multi-party setting. Given a specific interesting multiparty target state (e.g. GHZ states, cluster states etc.), or set of multiparty target states, what are the best possible distillation protocols that we can construct? Are there good bounds that can be derived using multiparty entanglement measures? Some specific examples have been considered [59, 60, 61] but more general results are still missing.

Additivity questions: Of all additivity problems, deciding whether the entanglement of formation E_F is additive is perhaps the most important unresolved question. If E_F is additive this would greatly simplify the evaluation of the entanglement cost. It would furthermore imply the additivity of the classical capacity of a quantum channel [48, 50, 49]. Related to the additivity question is the question of the monotonicity of the entanglement cost under general LOCC. This may be proven reasonably straightforwardly if the entanglement cost itself is fully additive. However, without this assumption no proof is known to the authors, and in fact a recent argument seems to show that full additivity of the entanglement cost is equivalent to its monotonicity [180]. In addition to E_F, there are many other measures for which additivity is unknown. Examples include the Distillable Entanglement and the Distillable Key.

Distillable entanglement – Distillable entanglement is a well motivated entanglement measure of significant importance. Its computation is however supremely difficult in general and even the determination of the distillability of a state is difficult. Indeed, good techniques or algorithms for deciding whether a bipartite state is distillable or not, and for bounding the distillable entanglement, are still largely missing.

- *Are there NPT bound entangled states?* – In the bi-partite setting there are currently three known distinct classes of states in terms of their entanglement properties under LOCC. These are the separable states, the non-separable states with positive partial transpose (which are also non-distillable), and finally the distillable states. Some evidence exists that there is another class of states that do not possess a positive partial transpose but are nevertheless non-distillable [181, 182].

- *Bounds on the Distillable entanglement.* Any entanglement measure provides an upper bound on the distillable entanglement. Various bounds have been provided such as the squashed entanglement [47, 7], the Rains bound [17] and asymptotic relative entropy of entanglement [25, 26]. The last two of these coincide for Werner states [90] and it is an open question whether they always coincide, and whether they are larger or smaller than the squashed entanglement.

Entanglement Measures – The present article has presented a host of entanglement measures. Many of their properties are known but crucial issues remain to be resolved. Amongst these are the following.

- *Operational interpretation of the relative entropy of entanglement* – While the entanglement cost and the distillable entanglement possess evident operational interpretations no such clear interpretation is known for the relative entropy of entanglement. A possible interpretation in terms of the distillation of local information has been conjectured and partially proven in [77].

- *Calculation of various entanglement measures* – There are very few measures of entanglement that can be computed exactly and possess or are expected to possess an operational interpretation. A notable exception is the entanglement of formation for which a formula exists for the two qubit case [44]. Is it possible to compute, or at least derive better bounds, for the other variational entanglement measures? One interesting possibility is the 2-qubit case - in analogy to E_F, is there a closed form for the relative entropy of entanglement or the squashed entanglement?

- *Squashed entanglement* – As an additive, convex, and asymptotically continuous entanglement monotone the Squashed entanglement is known to possess almost all potentially desirable properties as an entanglement measure [47, 7]. Nevertheless, there are a number of open interesting questions - in particular: (1) is the Squashed entanglement strictly non-zero on inseparable states, and (2) can the Squashed entanglement be formulated as a finite dimensional optimisation problem (with Eve's system of bounded dimension)?

- *Asymptotic continuity and Lockability questions* – It is unknown whether measures such as the Distillable Key, the Distillable Entanglement, and the Entanglement cost are asymptotically continuous, and it is unknown whether the Distillable entanglement or Distillable Key are lockable [68, 69, 70]. This is important to know as lockability quantifies 'continuity under tensor products', and so is a physically important property - if a system is susceptible to loss of particles, then any characteristic quantified by a lockable measure will tend to be very fragile in the presence of such noise.

Entanglement Manipulation – Entanglement can be manipulated under various sets of operations, including LOCC and PPT operations. While some understanding of what is possible and impossible has been obtained, a complete understanding has not been reached yet.

- *Characterization of entanglement catalysis* – For a single copy of bi-partite pure state entanglement the LOCC transformations are fully characterized by the theory of majorization [28, 29, 30]. It was discovered that there are transformations $|\phi\rangle \rightarrow |\psi\rangle$ such that its success probability under LOCC is $p < 1$ but for which an entangled state $|\eta\rangle$ exists such that $|\phi\rangle|\eta\rangle \rightarrow |\psi\rangle|\eta\rangle$ can be achieved with certainty under LOCC [33]. A complete characterization for states admitting entanglement catalysis is currently not known.

- *Other classes of non-global operation. Reversibility under PPT operations* – It is well established that even in the asymptotic limit LOCC entanglement transformations of mixed states are irreversible. However in [19] it was shown that that the antisymmetric Werner state may be reversibly interconverted into singlet states under PPT operations [17]. It is an open question whether this result may be extended to all Werner states or even to all possible states. In addition to questions concerning PPT operations, are there other classed of non-global operation that can be useful? If reversibility under PPT operations does not hold, do any other classes of non-global operations exhibit reversibility?

More open problems in quantum information science can be found in the Braunschweig webpage of open problems [171]. We hope that this list will stimulate some of the readers of this article into attacking some of these open problems and perhaps report solutions, even partial ones.

Acknowledgments

We have benefitted greatly from discussions on this topic with numerous researchers over several years. In relation to this specific article, we must thank K. Audenaert, F. Brandão, M. Horodecki, O. Rudolph, and A. Serafini for helping us to clarify a number of issues, as well as G.O. Myhr, L. Clarisse, P. Hyllus, and A. Feito-Boirac for careful reading and helpful suggestions. We would also like to thank M. Christandl, J. Eisert, J. Oppenheim, A. Winter, and R.F. Werner for sharing with us their thoughts on open problems. This work is part of the QIP-IRC (www.qipirc.org) supported by EPSRC (GR/S82176/0), the EU Integrated Project Qubit Applications (QAP) funded by the IST directorate as contract no. 015848, the EU Thematic network QUPRODIS (IST-2001-38877), The Leverhulme Trust, the Royal Commission for the Exhibition of 1851 and the Royal Society.

References

1. M. Bell, K. Gottfried and M. Veltmann, *John S. Bell on the foundations of quantum mechanics*, World Scientific Publishing, Singapore.
2. J.S. Bell, Physica **1**, 195 (1964).
3. L. Hardy, Contemp. Phys. **39**, 419 (1998).
4. M.B. Plenio and V. Vedral, Contemp. Phys. **39**, 431 (1998).
5. B. Schumacher and M. D. Westmoreland, E-print arxiv quant-ph/0004045.
6. M. Horodecki, Quant. Inf. Comp. **1**, 3 (2001).
7. M. Christandl, PhD Thesis, quant-ph/0604183.
8. P. Horodecki and R. Horodecki, Quant. Inf. Comp. **1**, 45 (2001).
9. J. Eisert and M. B. Plenio, Int. J. Quant. Inf. **1**, 479 (2003).
10. M. Nielsen and I. Chuang, *Quantum information and computation* C.U.P. 2000
11. However, it is important to realise that strong correlations can be obtained by non-local theories that in other respects might be considered quite classical [12]. Hence it requires much more discussion than we will present here to decide whether certain correlations are really *quantum*, or *classically non-local*.
12. N. J. Cerf, N. Gisin, S. Massar, and S. Popescu, Phys. Rev. Lett. **94**, 220403 (2005).
13. J. Eisert, K. Jacobs, P. Papadopoulos and M.B. Plenio, Phys. Rev. A **62**, 052317 (2000).
14. D. Collins, N. Linden and S. Popescu, Phys. Rev. A **64**, 032302 (2001).

15. S. Virmani and M.B. Plenio, Phys. Rev. A **67**, 062308 (2003).
16. C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
17. E.M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).
18. T. Eggeling, K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf, Phys. Rev. Lett. **87**, 257902 (2001).
19. K. Audenaert, M. B. Plenio, and J. Eisert, Phys. Rev. Lett. **90**, 027901 (2003).
20. R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
21. L. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
22. F.G.S.L. Brandão, E-print arxiv quant-ph/0510078
23. L. Masanes, E-print arxiv quant-ph/0510188
24. C. H. Bennett, H. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
25. V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
26. V. Vedral and M.B. Plenio, Phys. Rev. A **57**, 1619 (1998).
27. H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
28. M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
29. G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
30. D. Jonathan and M.B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).
31. L. Hardy, Phys. Rev. A **60**, 1912 (1999).
32. R. Bhatia, *Matrix Analysis* (Springer, Berlin, 1997).
33. D. Jonathan and M.B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).
34. G. Vidal, D. Jonathan and M. A. Nielsen, Phys. Rev. A **62**, 012304 (2000).
35. T.M. Cover and J.A. Thomas, *Elements of Information Theory* (Wiley Interscience, New York, 1991)
36. Common synonyms for two-qubit maximally entangled states include *'singlet states', 'Bell pairs'* or *'EPR pairs'*. Even though these terms strictly mean different things, we will follow this widespread abuse of terminology.
37. E.M. Rains, E-print arxiv quant-ph/9707002
38. P. Hayden, M. Horodecki, and B.M. Terhal, J. Phys. A **34**, 6891 (2001).
39. A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).
40. E. Rains, Phys. Rev. A **60**, 173 (1999); ibid **60**, 179 (1999).
41. G. Vidal and J.I. Cirac, Phys. Rev. Lett. **86**, 5803 (2001).
42. M. Horodecki, A. Sen(De) and U. Sen, Phys. Rev. A **67**, 062314 (2003).
43. C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
44. W.K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
45. W.K. Wotters, Quant. Inf. Comp. **1**, 27 (2001).
46. V. Vedral, M.B. Plenio, K. Jacobs and P.L. Knight, Phys. Rev. A **56**, 4452 (1997).
47. M. Christandl and A. Winter, J. Math. Phys **45**, 829 (2004).
48. P.W. Shor, Comm. Math. Phys. **246**, 453 (2004).
49. K.M.R. Audenaert and S.L. Braunstein, Comm. Math. Phys. **246**, 443 (2003).
50. A. A. Pomeransky, Phys. Rev. A **68**, 032317 (2003).
51. J. Smolin, F. Verstraete and A. Winter, Phys. Rev. A **72**, 052317 (2005)
52. F. Verstraete, M.-A. Martin-Delgado and J.I. Cirac, Phys. Rev. Lett. **92**, 087201 (2004)
53. F. Verstraete, M. Popp, and J. I. Cirac, Phys. Rev. Lett. **92**, 027901 (2004)
54. M. Popp, F. Verstraete, M. A. Martin-Delgado and J. Cirac, Phys. Rev. A. **71**, 042306 (2005).
55. J.K. Pachos and M.B. Plenio, Phys. Rev. Lett. **93**, 056402 (2004)
56. A. Key, D.K.K. Lee, J.K. Pachos, M.B. Plenio, M. E. Reuter, and E. Rico, Optics and Spectroscopy **99**, 339 (2005).
57. A. Harrow and M. Nielsen, Phys. Rev. A **68**, 012308 (2003)
58. S. Virmani, S.F. Huelga, and M.B. Plenio, Phys. Rev. A. **71**, 042328 (2005)
59. M. Murao, M.B. Plenio, S. Popescu, V. Vedral and P.L. Knight, Phys. Rev. A **57**, 4075 (1998).
60. H. Aschauer, W. Dür and H.J. Briegel, Phys. Rev. A **71**, 012319 (2005).

61. K. Goyal, A. McCauley and R. Raussendorf, E-print arxiv quant-ph/0605228
62. K. Chen and H-K Lo, quant-ph/0404133.
63. M.J. Donald, M. Horodecki, and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).
64. M.B. Plenio and V. Vitelli, Contemp. Phys. **42**, 25 (2001).
65. M.B. Plenio, Phys. Rev. Lett. **95**, 090503 (2005).
66. M. Horodecki, Open Syst. Inf. Dyn. **12**, 231 (2005).
67. P.W. Shor, J.A. Smolin and B.M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
68. D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal Phys. Rev. Lett. **92**, 067902 (2004) .
69. K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim, Phys. Rev. Lett. **94**, 200501 (2005).
70. B. Synak-Radtke and M. Horodecki, J. Phys. A: Math. Gen. **39**, L423-L437 (2006).
71. M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).
72. S. Virmani and M.B. Plenio, Phys. Lett. A **288**, 62 (2000).
73. J. Eisert and M.B. Plenio, J. Mod. Opt. **46**, 145 (1999).
74. K. Zyczkowski and I. Bengtsson, Ann. Phys. **295**, 115 (2002).
75. A. Miranowicz and A. Grudka, J. Opt. B: Quantum Semiclass. Optics **6**, 542 (2004).
76. D. Yang, M. Horodecki, R. Horodecki and B. Synak-Radtke, Phys. Rev. Lett. **95**, 190501 (2005).
77. M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen and B. Synak, Phys. Rev. A **71**, 062307 (2005) .
78. M.B. Plenio, S. Virmani, and P. Papadopoulos, J. Phys. A **33**, L193 (2000).
79. K.G.H. Vollbrecht and F. Verstraete, Phys. rev. A **71**, 062325 (2005).
80. E. Hostens, J. Dehaene and B. de Moor, Phys. Rev. A., **73**, 062337 (2006).
81. I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).
82. A. S. Holevo, IEEE Trans.Info.Theor. **44**, 269 (1998).
83. K. Audenaert, F. Verstraete and B. De Moor, Phys. Rev. A **64**, 052304 (2001).
84. K.G.H. Vollbrecht and R.F. Werner, Phys. Rev. A **64**, 062307 (2001).
85. J. Eisert, T. Felbinger, P. Papadopoulos, M.B. Plenio and M. Wilkens, Phys. Rev. Lett. **84**, 1611 (2000).
86. B. Terhal and K.G.H. Vollbrecht, Phys. Rev. Lett. **85**, 2625 (2000).
87. G. Vidal, J. Mod. Opt. **47**, 355 (2000).
88. M.B. Plenio and V. Vedral, J. Phys. A **34**, 6997 (2001).
89. M.J. Donald and M. Horodecki, Physics Letters A **264**, 257 (1999).
90. K. Audenaert, J. Eisert, E. Jané, M.B. Plenio, S. Virmani, and B. DeMoor, Phys. Rev. Lett. **87**, 217902 (2001).
91. N. Linden, S. Popescu, B. Schumacher and M. Westmoreland, Quant. Inf. Proc, **4**, 241 (2005).
92. E. Galvão, M.B. Plenio and S. Virmani, J. Phys. A **33**, 8809 (2000).
93. S. Wu and Y. Zhang, Phys. Rev. A **63**, 012308 (2001).
94. S. Ishizaka, Phys. Rev. Lett. **93**, 190501 (2004).
95. S. Ishizaka and M.B. Plenio, Phys. Rev. A **71**, 052303 (2005)
96. S. Ishizaka and M.B. Plenio, Phys. Rev. A **72**, 042325 (2005).
97. S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press 2004.
98. K. Audenaert, B. DeMoor, K.G.H. Vollbrecht and R.F. Werner, Phys. Rev A **66**, 032310 (2002).
99. T. Wei and P. Goldbart, Phys. Rev. A. **68**, 042307 (2003).
100. J. Eisert, K. Audenaert, and M.B. Plenio, J. Phys. A **36**, 5605 (2003).
101. K. Horodecki, M. Horodecki and P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
102. A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
103. P. Horodecki, Phys. Lett. A **232**, 333 (1997).
104. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
105. K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys. Rev. A **58**, 883 (1998).
106. J. Lee, M.S. Kim, Y.J. Park, and S. Lee, J. Mod. Opt. **47**, 2151 (2000).
107. J. Eisert, PhD thesis (University of Potsdam, February 2001).

108. G. Vidal and R.F. Werner, Phys. Rev. A **65**, 32314 (2002).
109. R. Alicki and M. Fannes, E-print arxiv quantum-ph/0312081
110. S. Ishizaka, Phys. Rev. A **69**, 020301(R) (2004).
111. R. R. Tucci, quant-ph/9909041; R. R. Tucci, quant-ph/0202144.
112. G. Vidal and R. Tarrach, Phys. Rev. A. **59**, 141 (1999).
113. M. Steiner, Phys. Rev. A **67**, 054305 (2003).
114. M. Lewenstein and A. Sanpera **80**, 2261 (1998).
115. R. Nagel 'Order Unit and Base Norm Spaces', in *Foundations of Quantum Mechanics and Ordered Linear Spaces*, Eds. A. Hartkämper and H. Neumann, Springer-Verlag (1974).
116. O. Rudolph, J. Phys. A: Math Gen **33**, 3951 (2000).
117. O. Rudolph, J. Math. Phys. **42**, 2507 (2001).
118. O. Rudolph, quant-ph/0202121.
119. F.G.S.L. Brandão, Phys. Rev. A **72**, 040303(R) (2005).
120. This excludes for example the hydrogen atom from our considerations as it has a limit point in the spectrum at the ionization level.
121. J. Eisert, Ch. Simon and M.B. Plenio, J. Phys. A **35**, 3911 (2002)
122. S. Parker, S. Bose and M.B. Plenio, Phys. Rev. A **61**, 032305 (2000).
123. M.M. Wolf, G. Giedke and J.I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
124. K. Cahill and R. Glauber, Phys. Rev. **177**, 1857 (1969).
125. see e.g. H. P. Robertson, Phys. Rev. **46**, 794 (1934) ; A. Serafini, Phys. Rev. Lett. **96**, 110402 (2006).
126. R. Simon, N. Mukunda, B. Dutta, Phys. Rev. A. **49**, 1567 (1994)
127. R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
128. L.-M. Duan, G. Giedke, J.I. Cirac and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000)
129. R.F. Werner and M.M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
130. G. Giedke, B. Kraus, M. Lewenstein, and J.I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001)
131. G. Giedke, L.-M. Duan, J.I. Cirac and P. Zoller, Quantum. Inf. Comput. **1**, 79 (2001).
132. J. Eisert and M.B. Plenio, Phys. Rev. Lett. **89**, 097901 (2002).
133. J. Eisert, S. Scheel, and M.B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).
134. G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).
135. The no-go theorem for Gaussian entanglement distillation is actually quite subtle, as even defining Gaussian distillation is non-trivial. Consider for example the version of the no-go theorem proven in [134] - there entanglement distillation is defined as a process which allows you to reach a two-mode squeezed state with arbirarily high squeezing. Although [134] show that this is not possible, from an operational perspective one can use Gaussian operations to improve the quality of the entanglement present. For instance, consider a bi-partite four-mode state ρ which consists of a two-mode highly entangled state tensored with a product pure state. Given two copies of ρ, Alice and Bob can merely throw away the product components and are left with a single four-mode state that possesses greater utility for quantum information processing. Hence according to an operational definition of entanglement distillation (say improvement of teleportation fidelity), it is possible to distill Gaussian entanglement using Gaussian operations from Gaussian states of 2 $\times$ 2 modes. This apparent contradiction arises because there are different ways in which one can quantify the increase of entanglement of quantum states - in principle this subtle distinction may also be an issue in the finite dimensional regime.
136. G. Giedke, J. Eisert, J.I. Cirac and M.B. Plenio, Quantum. Inf. Comput. **3**, 211 (2003).
137. J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002).
138. R. Simon, E.C.G. Sudarshan, and N. Mukunda, Phys. Rev. A **36**, 3868 (1987).
139. Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana **45**, 471 (1995).
140. J. Williamson, Am. J. Math. **58**, 141 (1936).
141. G. Giedke, M.M. Wolf, O. Krüger, R.F. Werner, and J.I. Cirac, Phys. Rev. Lett. **91**, 107901 (2003)
142. M.M. Wolf, G. Giedke, O. Krüger, R.F. Werner and J.I. Cirac, Phys. Rev. A **69**, 052320 (2004).

143. M.E. Shirokov, E-print quant-ph/0411091.
144. K. Audenaert, J. Eisert, M.B. Plenio and R.F. Werner, Phys. Rev. A **66**, 042327 (2002).
145. M.B. Plenio, J. Eisert, J. Dreißig, M. Cramer, Phys. Rev. Lett. **94**, 060503 (2005).
146. M. Cramer, J. Eisert, M.B. Plenio and J. Dreissig, Phys. Rev. A **73**, 012309 (2006)
147. R. Raussendorf and H.-J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
148. D. J.Wineland, J. J. Bollinger, W.M. Itano, F. L. Moore, and D. J. Heinzen, Phys. Rev. A **46**, R6797 (1992).
149. S.F Huelga, C. Macchiavello, T. Pellizzari, A.K. Ekert, M. B. Plenio, J.I. Cirac, Phys. Rev. Lett. **79**, 3865 (1997).
150. M. Murao, D. Jonathan, M.B. Plenio and V. Vedral, Phys. Rev. A **59**, 156 (1999).
151. M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
152. A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999)
153. M. Murao, D. Jonathan, M.B. Plenio and V. Vedral, Phys. Rev. A **61**, 032311 (2000).
154. W. Dür, G. Vidal, and J. I. Cirac Phys. Rev. A **62**, 062314 (2000).
155. F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Phys. Rev. A **65**, 052112 (2002).
156. E. Hostens, J. Dehaene and B. de Moor, Phys. Rev. A., **73**, 042316 (2006)
157. C. Kruszynska, A. Miyake, H. J. Briegel and W. Dür, quant-ph/0606090.
158. A. Acin, G. Vidal and J. I. Cirac, Quant. Inf. Comp. **3**, 55 (2003).
159. C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin and A. V. Thapliyal, Phys. Rev. A. **63**, 012307 (2001).
160. D. DiVincenzo, C. Fuchs, H. Mabuchi, J. Smolin and A. Uhlmann, Lecture Notes in Comp. Science **1509**, 247 (1999) .
161. G. Gour and R. W. Spekkens, Phys. Rev. A **73**, 062331 (2006).
162. M. Horodecki, J. Oppenheim, and A. Winter, Nature **436**, 673 (2005).
163. T. Wei, M. Ericsson, P. Goldbart and W. Munro, Quant. Inf. Comp. **4**, 252 (2004).
164. R. Werner and A. Holevo, J. math. Phys. **43**, 4353 (2002).
165. see e.g. A. Defant and K. Floret, '*Tensor Norms and Operator Ideals*', North-Holland (1993).
166. V. Coffman, J. Kundu, and W. Wootters, Phys. Rev. A. **61**, 052306 (2000).
167. T. Osborne and F. Verstraete, Phys. Rev. Lett. **96**, 220503 (2006).
168. D. A. Meyer and N. R. Wallach, J. Math. Phys. **43**, 4273 (2002)
169. C. Emary, J. Phys A. **37**, 8293 (2004).
170. G. K. Brennen, Quant. Inf. Comp. **3**, 619 (2003).
171. The web site at the Universität Braunschweig *http://www.imaph.tu-bs.de/qi/problems/3.html* contains an interesting review of this problem and further references.
172. J. Eisert and H. J. Briegel, Phys. Rev. A **64**, 022306 (2001).
173. A. Miyake, Phys. Rev. A. **67**, 012108 (2003).
174. P. Levay, Journal of Physics A **38**, 9075 (2005).
175. I. Pitowsky, quant-ph/0608050.
176. J.-G. Luque, J.-Y. Thibon, quant-ph/0506058.
177. E. Briand, J.-G. Luque, J.-Y. Thibon, quant/0304026.
178. A. Osterloh, J. Siewert, Phys. Rev. A **72**, 012337 (2005).
179. A. Osterloh, J. Siewert, Int. J. Quant. Inf. 4, 531 (2006).
180. M. Horodecki, private communication.
181. D.P. DiVincenzo, R. Jozsa, P.W. Shor, J.A. Smolin, B.M. Terhal, and A.V. Thapliyal, Phys. Rev. A **61**, 062312 (2000).
182. W. Dür, J.I. Cirac, M. Lewenstein and D. Bruß, Phys. Rev. A **61**, 062313 (2000).