ELSEVIER

Theoretical Computer Science 287 (2002) 313–335

Theoretical Computer Science

www.elsevier.com/locate/tcs

Detecting quantum entanglement

Barbara M. Terhal

IBM Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598, USA

Abstract

We review the criteria for separability and quantum entanglement, both in a bipartite as well as a multipartite setting. We discuss Bell inequalities, entanglement witnesses, entropic inequalities, bound entanglement and several features of multipartite entanglement. We indicate how these criteria bear on the experimental detection of quantum entanglement. © 2002 Elsevier Science B.V. All rights reserved.

PACS: 03.67.Hk; 03.65.Bz; 03.67.−a; 89.70.+c

Keywords: Quantum entanglement; Quantum information theory; Quantum computation

1. Introduction

The phenomenon of quantum entanglement lies at the heart of quantum mechanics. And what lies at the heart of quantum mechanics, may lie at the heart of a future technology. It is not surprising then that over the last 5 years a theory of quantum entanglement has started to emerge that tries to capture, quantify and assess the power of quantum entanglement.

First, it was by the protocol of quantum teleportation [5] that quantum entanglement was introduced as a resource in quantum communication: it has become a rule of quantum communication law that 1 bit of entanglement (1 ebit) enables 1 unknown qubit to be sent by means of 2 classical bits.

But it has been realized over the last year that quantum entanglement is not only a fundamental resource in quantum communication, but can also be viewed as a resource in quantum computation. Gottesman and Chuang [22] have shown that it is possible to perform universal quantum computation, by starting with three-party entangled GHZ states and subsequently performing single qubit operations and measurements in the Bell basis. In the linear optics quantum computation proposal by Knill et al. [36]

E-mail address: terhal@watson.ibm.com (B.M. Terhal).

0304-3975/02/$ - see front matter
PII: S0304-3975(02)00139-1

the quantum gate that lies beyond the capabilities of linear optics, can in fact be implemented by the creation of a multipartite entangled state. Quantum entanglement also lies at the core of the quantum computation proposal by Rausschendorf and Briegel [46]. In this proposal the authors show that universal quantum computation is possible by means of a series of single qubit measurements that are performed on an initial state which is a certain highly entangled 'cluster' state. The entangled state functions as a substrate on which the quantum computation takes place.

In this article, we review the progress that has been made in establishing one of the cornerstones of the theory of quantum entanglement, namely the development of criteria for entanglement and separability, both in the bipartite as well as the multipartite setting. In the last section of this paper, we will consider how entanglement witnesses can be used in deciding by experiment whether a quantum state is entangled. We will not discuss the topic of entanglement measures, which can be viewed as a subject complementary to the one which we consider in this review article. We would like to refer the reader to Ref. [30] for a more comprehensive overview on bipartite quantum entanglement.

We will write X, Y and Z for the three Pauli matrices. A positive semidefinite operator A with nonnegative eigenvalues is denoted as $A \geqslant 0$. A n-dimensional Hilbert space is denoted as $\mathscr{H}_n$, and operators on this space ($n \times n$ matrices) $\in B(\mathscr{H}_n)$. Furthermore, the class of quantum operations which are constructed by Local Operations supplemented by Classical Communication is sometimes abbreviated as LOCC.

1.1. What is quantum entanglement

A bipartite pure quantum state $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ is called entangled when it cannot be written as $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ for some $|\psi_A\rangle \in \mathscr{H}_A$ and $|\psi_B\rangle \in \mathscr{H}_B$. A mixed state or density matrix ρ, which is a positive semidefinite operator on the space $\mathscr{H}_A \otimes \mathscr{H}_B$, is called entangled when it cannot be written in the following form:

$$\rho = \sum_i p_i |\psi_i^A\rangle\langle\psi_i^A| \otimes |\psi_i^B\rangle\langle\psi_i^B| \tag{1}$$

for some set of states $|\psi_i^A\rangle \in \mathscr{H}_A$, $|\psi_i^B\rangle \in \mathscr{H}_B$ and $p_i \geqslant 0$. If the density matrix ρ can be written in the form of Eq. (1), then the density matrix ρ is called separable.

The distinction between separable states and entangled states has an operational meaning in the following sense. A source (or black box) produces a mixed state ρ; the mixedness could come about when aside from systems A and B there are additional degrees of freedom to which we have no access. If ρ is an entangled density matrix, then some coherent interaction must have taken place between A and B. If ρ is separable, then no guarantee exists of whether the interaction in the black box was coherent or not.

Consider a multipartite system with parties labeled by $A_1, \ldots, A_n$. The density matrix is called separable when no entanglement exists between the parties, i.e. $\rho = \sum_i p_i |\psi_i^{A_1}\rangle\langle\psi_i^{A_1}| \otimes \cdots \otimes |\psi_i^{A_n}\rangle\langle\psi_i^{A_n}|$. For the various degrees and forms of quantum entanglement that can exist among parties, we will consider specific classes of states in Section 3.

A note of caution about how to interpret the state of a physical system in terms of quantum entanglement may be in place here. The previous standard definitions of quantum entanglement tacitly assume that (1) every state in the bi- or multi-partite Hilbert space is in principle available as a physical state and (2) local (involving single tensor factors) as well as global quantum operations, measurements and unitary transformations, can be performed on the Hilbert space. In this respect the wavefunction of two identical bosons $\Psi(x_1,x_2)=\psi(x_1)\otimes\psi(x_2)+\psi(x_2)\otimes\psi(x_1)$ cannot be called entangled, since it falls short of these criteria. Understandably, when considering more complex physical systems, the dividing line between what is entangled and what is not entangled, may become somewhat fuzzy. The guideline in deciding these matters, I believe, should be the question: "Do we have an operational form of quantum entanglement? What resource does the particular state constitute in quantum communication and computation?" In Ref. [48] for example the authors consider the entanglement that can exist in 2-fermion systems.

2. Bipartite criteria

2.1. Bell inequalities

Historically one can say that the first separability criterion was formulated by John Bell [3]. Bell's intention however was not to establish a separability criterion, but to evaluate the power of local hidden variable theories in describing local measurement outcomes on quantum mechanical states.

His inequality, and similar inequalities such as the CHSH inequality [12] found later, is obeyed by any local hidden variable theory, whereas the correlations in measurement outcomes on, for example, the singlet state $|\Psi^-\rangle=1/\sqrt{2}(|01\rangle-|10\rangle)$ violate the inequality. Furthermore, the outcomes of local measurements on any separable density matrix can be simulated by a local hidden variable theory. This can be easily understood from Fig. 1 which gives an idea of the workings of a local hidden variable theory. For every pure entangled state there exists a Bell inequality that is violated [43] and therefore there exists a series of measurements and outcomes through which we can ascertain that our state is entangled.

The weakness of Bell inequalities as criteria for entanglement or separability, lies in the fact that it is not known whether violations exist for many entangled mixed states. For example, it has been shown that for a special class of mixed states, the so-called PPT bound entangled states (see Section 2.2), all CHSH-inequalities are obeyed [57]. If we loosen the rules of the game and allow preprocessing of our state ρ or many copies of our state $\rho^{\otimes n}$ by means of LOCC, then a much larger class of states ρ will violate a Bell inequality. We demand that only local operations and classical communication enter in this game, since these are the operations which cannot increase the quantum entanglement in a state. This class of operations, crucial in the theory of quantum entanglement, is graphically depicted in Fig. 2. All density matrices which are distillable (see Section 2.3) will then violate a Bell inequality in this manner.

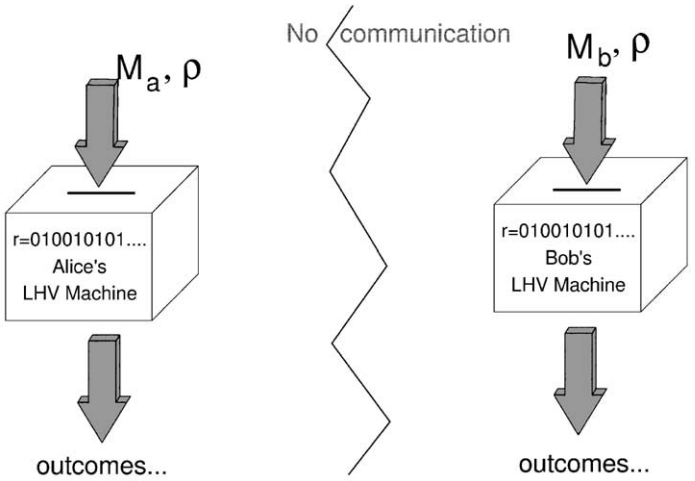

Fig. 1. Local hidden variable theories: Alice and Bob each have an arbitrarily powerful machine in their lab which takes as input the description of their local measurements $\mathcal{M}_A$ and $\mathcal{M}_B$ and a description of the state ρ on which the measurement will take place. Inside their machine may be a random shared bit string r of arbitrary length. The output of the machines is supposed to statistically simulate the outputs of the real measurements $\mathcal{M}_A$ and $\mathcal{M}_B$ that were performed on the state ρ, in the sense that the joint and marginal probabilities for various outcomes and choices of measurements are identical to those of the real measurement on ρ.

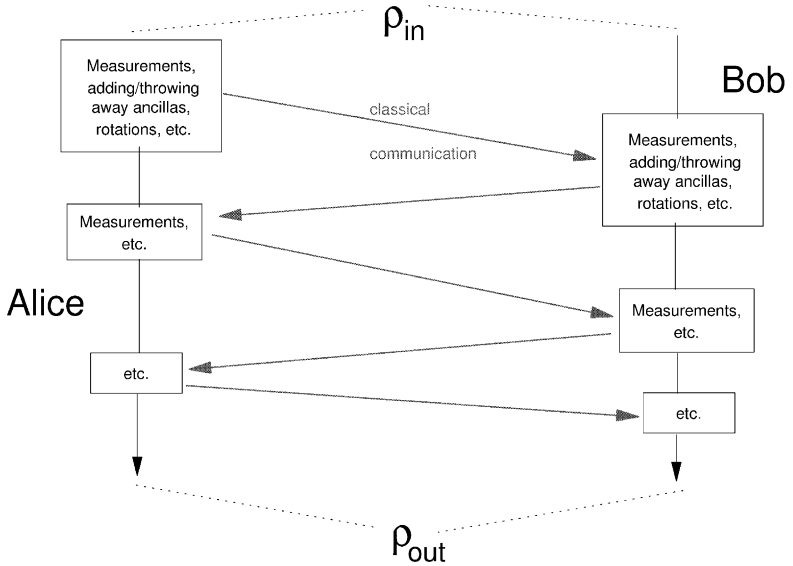

Fig. 2. Local operations and classical communication: at each round Alice's (Bob's) local actions may depend on Bob's (Alice's) previous actions and outcomes.

2.2. Entanglement witnesses and positive linear maps

The framework of Bell inequalities fits in a larger scheme of entanglement witnesses. In fact, each Bell inequality can be viewed as a particular example of an entanglement witness [53]. A prime example is the operator form of the CHSH inequality: the Bell-CHSH operator ($\vec{a}, \vec{a'}, \vec{b}, \vec{b'}$ are unit-vectors) reads

$$\mathscr{B} = \vec{a}\cdot\vec{\sigma}\otimes(\vec{b}+\vec{b'})\cdot\vec{\sigma} + \vec{a'}\cdot\vec{\sigma}\otimes(\vec{b}-\vec{b'})\cdot\vec{\sigma}. \tag{2}$$

The expectation value of $\mathscr{B}$ with respect to all separable states

$$\mathrm{Tr}\,\mathscr{B}\rho_{\mathrm{sep}} \leqslant 2, \tag{3}$$

whereas $\mathrm{Tr}\,\mathscr{B}\rho$ can exceed this value for an entangled state ρ. The operator $2\mathbf{1} - \mathscr{B}$ is an example of an entanglement witness. Even though there does not necessarily exist a Bell inequality for every entangled state (for certain Werner states, for example, there is no single copy violation of a Bell inequality [56]), there does exist a witness for every entangled state. This is the content of the following theorem:

Theorem 1 (Horodecki [27]). *A density matrix ρ on $\mathscr{H}_A\otimes\mathscr{H}_B$ is entangled if and only if there exists a Hermitian matrix $H = H^\dagger$, an entanglement witness, such that*

$$\mathrm{Tr}\,H\rho < 0 \tag{4}$$

and for all separable states ρ_{sep},

$$\mathrm{Tr}\,H\rho_{\mathrm{sep}} \geqslant 0. \tag{5}$$

Thus by a measurement of the entanglement witness observable H we will be able to decide whether a particular state is entangled, since when we find a negative expectation value for H, we must conclude that the state cannot be separable.

There exists a direct relation between entanglement witnesses and positive linear maps which are not completely positive [33]. A linear map $\mathscr{L}: B(\mathscr{H}_n)\to B(\mathscr{H}_m)$ is called positive, when it maps all $X\geqslant 0$ onto $\mathscr{L}(X)\geqslant 0$. The map $\mathscr{L}$ is completely positive if and only if $\mathbf{1}_n\otimes\mathscr{L}$ is a positive map. The most famous and physically relevant example of a positive map is matrix transposition T in a chosen basis. The map T is not completely positive, as can be illustrated by applying it on half of a (unnormalized) maximally entangled state:

$$\begin{aligned}(\mathbf{1}\otimes T)[|00\rangle + |11\rangle)(\langle 00| + \langle 11|] \\ = |00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|.\end{aligned} \tag{6}$$

The resulting operator has an eigenvector $|01\rangle - |10\rangle$ with negative eigenvalue -1. It was noted by Peres [44] that applying $\mathbf{1}\otimes T$ on a separable density matrix always

gives another density matrix

$$(\mathbf{1}\otimes T)\left(\sum_i p_i|\psi_i^A\rangle\langle\psi_i^A|\otimes|\psi_i^B\rangle\langle\psi_i^B|\right)$$
$$=\sum_i p_i\,|\,\psi_i^A\rangle\langle\psi_i^A\,|\otimes|\,\psi_i^{B^*}\rangle\langle\psi_i^{B^*}|\geqslant 0 \tag{7}$$

and therefore the condition $(\mathbf{1}\otimes T)(\rho)\geqslant 0$, sometimes called the Peres–Horodecki criterion, constitutes a separability criterion.

The relation between entanglement witnesses and positive linear map is the following. We take a maximally entangled state in $\mathscr{H}_n\otimes\mathscr{H}_n$, for example the state $|\Psi^+\rangle=\sum_{i=1}^n|i,i\rangle$. The Hermitian operator $H\in B(\mathscr{H}_n\otimes\mathscr{H}_m)$ defined by

$$H=(\mathbf{1}\otimes\mathscr{L})(|\Psi^+\rangle\langle\Psi^+|) \tag{8}$$

has the property of Eq. (5) if and only if $\mathscr{L}: B(\mathscr{H}_n)\to B(\mathscr{H}_m)$ is a positive map. Furthermore, H is an entanglement witness, as in Eq. (4), if and only if $\mathscr{L}$ is not a completely positive map.

The theory of positive maps which are not completely positive has not been completely developed. What is known is that in spaces such as $\mathscr{H}_2\otimes\mathscr{H}_2$ and $\mathscr{H}_2\otimes\mathscr{H}_3$, all positive maps $\mathscr{L}$ relate to the matrix transposition map T, i.e. they can all be written as

$$\mathscr{L}=\mathscr{S}_1+\mathscr{S}_2\circ T, \tag{9}$$

where $\mathscr{S}_1$ and $\mathscr{S}_2$ are completely positive maps and T is matrix transposition in any chosen basis [58]. This implies that for these small dimensions, $\mathscr{H}_2\otimes\mathscr{H}_2$ or $\mathscr{H}_2\otimes\mathscr{H}_3$, the entanglement witnesses are of the form

$$H=P+(\mathbf{1}\otimes T)(Q), \tag{10}$$

where $Q\geqslant 0, P\geqslant 0$ and T is matrix transposition in any chosen basis.

In higher dimensions the situation is more involved. There do exist positive maps which are not *decomposable*, meaning that they are not of the form of Eq. (9). A consequence is that in higher dimensions, there exist *entangled* states which satisfy the Peres–Horodecki criterion, i.e. $(\mathbf{1}\otimes T)(\rho)\geqslant 0$ where T is matrix transposition in any basis. These are the bound entangled density matrices with positive partial transposition (PPT) (see the next section). The first example of an indecomposable positive map in $\mathscr{H}_3\otimes\mathscr{H}_3$ was found by Choi [11]. The first method of constructing some indecomposable entanglement witnesses in arbitrary high dimensions was presented in Ref. [52]. In Refs. [38] and [37] this construction was generalized with the following consequences. It was shown in Ref. [38] that every indecomposable entanglement witness is of the form

$$H=P+(\mathbf{1}\otimes T)(Q)-\varepsilon\mathbf{1}, \tag{11}$$

where, in order to ensure that H has the property of Eq. (5), we have

$$0<\varepsilon\leqslant\inf_{\psi_A,\psi_B}\langle\psi_A,\psi_B\,|\,(P+(\mathbf{1}\otimes T)(Q))\,|\psi_A,\psi_B\rangle. \tag{12}$$

Here $P \geqslant 0$, $Q \geqslant 0$ and they are such that $\mathrm{Tr}\, P\delta = 0$ and $\mathrm{Tr}\, Q(\mathbf{1} \otimes T)(\delta) = 0$ for an 'edge' state δ. An edge state δ is a bound entangled PPT state which has the property that for all $\varepsilon > 0$ and all product states $|\psi_A, \psi_B\rangle$, $\delta - \varepsilon |\psi_A, \psi_B\rangle\langle\psi_A, \psi_B|$ is not positive or does not have PPT. As such, the edge states are on the boundary of the closed set of entangled PTT states. The entanglement witness H in Eq. (11) detects the entanglement of the edge state δ.

The entanglement of bound entangled PPT states ρ in the interior of the set of PPT states is also detected by these witnesses [38]. By choosing $\mathrm{Tr}\,(P + (\mathbf{1} \otimes T)(Q))\rho = 0$ we ensure that the indecomposable witness H in Eq. (11) detects the entanglement in ρ, i.e. $\mathrm{Tr}\, H\rho < -\varepsilon < 0$.

Thus, given an edge state δ, its entanglement witness can be determined. A complete characterization of these edge states is still an open question; in Ref. [38] they are shown to be based on pairs of subspaces $\mathscr{H}_1$ and $\mathscr{H}_2$ such that (1) for every product state $|\psi_A, \psi_B\rangle \in \mathscr{H}_1$, $|\psi_A, \psi_B^*\rangle \notin \mathscr{H}_2$ and (2) the rank of $\mathrm{Tr}_i P_{\mathscr{H}_1}$ is equal to the rank of $\mathrm{Tr}_i P_{\mathscr{H}_2}$ for $i = A, B$, where P is the projector onto the subspace. For the choice $\mathscr{H}_1 = \mathscr{H}_2$, an example of such a subspace (containing, in this case, no product vectors) is the space orthogonal to an unextendible product basis [6]. It would be very interesting to find a method for constructing such subspaces in general.

Indecomposable positive maps are highly nontrivial objects. As was noted by Choi they provide special counterexamples to Hilbert's 17th problem. In Appendix A we will review this connection.

2.3. Operational criteria: LOCC and distillability

The resource view of quantum entanglement emerged with the discovery of quantum teleportation [5]. A natural next question, which was asked and partially answered by Bennett et al. in Ref. [7] is, in what sense does mixed state entanglement enables quantum data transmission? This line of study, which is still ongoing, has led to operational criteria for 'useful' entanglement. We can classify entangled states in terms of their distillability. Distillation of a mixed state ρ is a process which is implemented by LOCC on a large set of copies of the state $\rho^{\otimes n}$. The process outputs a smaller set of states $\sigma^{\otimes k}$ on a space of dimension $2^k \times 2^k$ such that $\langle \Psi^{-\otimes k} | \sigma^{\otimes k} | \Psi^{-\otimes k} \rangle \to 1$ when $n \to \infty$. Here $|\Psi^-\rangle$ is the singlet state. The asymptotic fraction k/n is called the distillable entanglement D of the density matrix ρ. It has been shown that all entangled density matrices in $\mathscr{H}_2 \otimes \mathscr{H}_2$ are distillable [28]. In fact, a generalization of this result exists: all states which violate the so-called *reduction criterion* are known to be distillable [25]. The reduction criterion is violated for a density matrix ρ when either

$$\mathbf{1} \otimes \rho_B - \rho \not\geqslant 0 \quad \text{or} \quad \rho_A \otimes \mathbf{1} - \rho \not\geqslant 0. \tag{13}$$

It is noteworthy that satisfaction of the reduction criterion is identical [25] to positivity under partial application of the decomposable positive map $\mathscr{L}(X) = \mathbf{1}\,\mathrm{Tr}\, X - X$, since $(\mathbf{1} \otimes \mathscr{L})(\rho) = \rho_A \otimes \mathbf{1} - \rho$. Since the map $\mathscr{L}$ is decomposable, Eq. (9), it follows that every state which satisfies the Peres–Horodecki criterion will also satisfy the reduction criterion.

The class of density matrices which are not distillable are called *bound entangled* density matrices. At least one group of density matrices exists for which it is possible to rigorously prove that they are bound entangled density matrices. These are entangled density matrices ρ which do not violate the Peres–Horodecki criterion. This criterion is important in the theory of quantum entanglement, since it has been shown [29] that nonviolation of the Peres–Horodecki criterion is preserved under LOCC. This is not hard to see, when we consider a larger class of quantum operations, the separable superoperators, of which the LOCC actions are a subset. A separable superoperator or measurement [45] has operation elements that are of separable form $\{A_i \otimes B_i, \sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathbf{1}\}$. Given is a density matrix ρ such that $(\mathbf{1} \otimes T)(\rho) \geqslant 0$. For every i, we can write

$$(\mathbf{1} \otimes T)[A_i \otimes B_i \rho A_i^\dagger \otimes B_i^\dagger] = (A_i \otimes B_i^*)(\mathbf{1} \otimes T)(\rho)(A_i^\dagger \otimes B_i^{\mathrm{T}}) \geqslant 0, \tag{14}$$

under the premise that ρ satisfies the Peres–Horodecki criterion. Thus under the action of a separable superoperator or measurement, PPTness is preserved. Since the output of a distillation process (arbitrarily good approximations to singlet states) does violate the Peres–Horodecki criterion, it must follow that entangled states with the PPT property cannot be distilled. The first bound entangled states were found by Horodecki [23]. In Refs. [6] and [13] constructions were given for classes of bound entangled states based on unextendible product bases.

A second class of states has been conjectured to be nondistillable [15,18]. Examples of these states are particular Werner states in $\mathscr{H}_n \otimes \mathscr{H}_n$, of the form:

$$\rho_\lambda = \frac{1}{\lambda(n^2-1)-1}(\lambda \mathbf{1} - (\lambda+1)(\mathbf{1} \otimes T)(|\Psi^+\rangle\langle\Psi^+|)), \tag{15}$$

where $|\Psi^+\rangle = 1/\sqrt{n} \sum_{i=1}^n |i,i\rangle$. For all finite $\lambda \geqslant 0$, these Werner states violate the Peres–Horodecki criterion. The states are conjectured to be nondistillable for $\lambda \in [2/(n-2), \infty)$.

The structure among the set of (conjectured) nondistillable states is by itself fairly complex. It has been shown recently that the tensorproduct of two nondistillable states, one of the PPT kind and one nondistillable Werner state, Eq. (15), in $\mathscr{H}_3 \otimes \mathscr{H}_3$, can be a distillable state [50]. Furthermore, it is not clear what classes of bound entangled states are asymptotically interconvertible by local actions and classical communication. In order to investigate this 'fine-structure' we may need to look for positive maps $\mathscr{L}$ for which "positivity under partial application of $\mathscr{L}$" is preserved under LOCC.

2.4. Functional separability criteria

Even though entanglement witnesses completely characterize the set of separable states, they do not provide a simple computational method (except for the Peres–Horodecki condition) for deciding whether a density matrix is entangled. It is desirable to have alternative or additional criteria that may help us in deciding this and characterizing separable versus entangled states. The criteria that we will discuss in this

section are all obeyed by separable density matrices, so that in case of a violation we know that ρ is entangled.

The first criterion is a combination of the Peres–Horodecki criterion and a check on the rank of the density matrix. When we find that ρ has PPT, ρ may either be separable or bound entangled. In Ref. [31] it was proved that a density matrix $\rho \in B(\mathscr{H}_n \otimes \mathscr{H}_m)$ with PPT and a rank which is smaller than or equal to $\max(n,m)$ is separable. For PPT density matrices for which the sum of the rank of ρ and $(\mathbf{1} \otimes T)(\rho)$ is smaller than or equal to $2mn - m - n + 2$, the authors in Ref. [31] provide an algorithm for checking whether ρ is separable.

It can be shown that from a nonviolation of the reduction criterion several other criteria can be derived:

Lemma 2. *For all separable states the reduction criterion is not violated and this implies that if ρ is separable,*

$$S_\alpha(\rho_A) \leqslant S_\alpha(\rho) \quad \textit{and} \quad S_\alpha(\rho_B) \leqslant S_\alpha(\rho). \tag{16}$$

for $\alpha = 0$, $\alpha \in [1,2]$ and $\alpha = \infty$ where $S_\alpha(\rho)$ for $0 < \alpha < \infty$ ($\alpha \neq 1$) is the quantum Renyi entropy

$$S_\alpha(\rho) = \frac{1}{1-\alpha} \log \operatorname{Tr} \rho^\alpha. \tag{17}$$

For $\alpha = 0$, we have $S_0(\rho) = \log R(\rho)$ where $R(\rho)$ is the rank of ρ, $\lim_{\alpha \to 1} S_\alpha = S(\rho)$ where S is the von Neumann entropy $S(\rho) = -\operatorname{Tr} \rho \log \rho$ and for $\alpha = \infty$ we have $S_\infty = -\log \|\rho\|$.

The case $\alpha = \infty$ was proved in Ref. [25] and the case $\alpha = 0$ was proved in Ref. [32]. The cases $\alpha \to 1$ and $\alpha = 2$ can be derived from the reduction criterion [24]. For $\alpha \to 1$, we use the operator-monotoniticity [2] of the log function to infer that

$$\log \rho_A \otimes \mathbf{1} \geqslant \log \rho. \tag{18}$$

Now we use that when $X \geqslant 0$, $\operatorname{Tr} \rho X \geqslant 0$ for all $\rho \geqslant 0$. Thus, multiplying with ρ on both sides and subsequently taking the trace gives the desired entropy inequality for $\alpha \to 1$. If $\rho_A \otimes \mathbf{1} \geqslant \rho$, then $(\rho_A \otimes \mathbf{1})^\delta \geqslant \rho^\delta$ for $\delta \in (0,1]$, since t^δ is operator-monotone for δ in this interval [2]. If we multiply the inequality with δ by ρ on both sides and trace, we get

$$\operatorname{Tr}_A \rho_A^{1+\delta} \geqslant \operatorname{Tr} \rho^{1+\delta}, \tag{19}$$

which, after taking logarithms on both sides, proves the result for $\alpha \in (1,2]$.

In Ref. [10] the conditional quantum operator was defined

$$\rho_{A|B} = \exp[\log \rho - \log \mathbf{1}_A \otimes \rho_B]. \tag{20}$$

With this definition the conditional entropy $S(A|B) = -\operatorname{Tr} \rho \log \rho_{A|B}$ is the difference between the total entropy of the state $S(\rho)$ and the local entropy $S(\rho_B)$. Lemma 2

states that for all states obeying the reduction criterion (separable states and at least all nondistillable states) such a conditional entropy (and similarly some α-entropic extensions) is nonnegative.

Nielsen and Kempe [42] recently found a different separability criterion.

Lemma 3 (Nielsen and Kempe, [42]). *For all separable density matrices* ρ

$$\vec{\lambda}_{\rho_A} \succ \vec{\lambda}_\rho \quad \text{and} \quad \vec{\lambda}_{\rho_B} \succ \vec{\lambda}_\rho, \tag{21}$$

where $\vec{\lambda}_\sigma$ *is the ordered vector of eigenvalues of the density matrix* σ. *Here the symbol* $\succ$ *means majorization, i.e.* $\vec{\lambda} \succ \vec{\mu}$, *when* $\sum_{i=1}^{k} \lambda_i \geqslant \sum_{i=1}^{k} \mu_i$ *for all* k.

Similar to the entropic criteria given above, this majorization criterion affirms the intuition that separable density matrices are globally at least as mixed as locally. A new corollary of the majorization criterion are the entropic inequalities in Eq. (16) for $\alpha \in [0,1]$. This follows from the fact that the quantum Renyi entropy $S_\alpha(\rho)$ is a *concave* function of the probabilities $\vec{\lambda}_\rho$ for all $\alpha \in [0,1]$. It can be shown that the majorization condition (Uhlmann's relation) implies the entropic inequalities for all $\alpha \geqslant 0$.

The two criteria, the reduction criterion of Eq. (13) and Lemma 3 are strikingly similar. There exist states however for which the reduction criterion is violated whereas the majorization criterion is satisfied; this is the example of a 2-qubit entangled state in Ref. [42]. The reduction criterion is violated for this state, since in $\mathscr{H}_2 \otimes \mathscr{H}_2$ the reduction criterion is equivalent to the Peres–Horodecki criterion, and all entangled 2-qubit states violate this criterion. The conjectured nondistillable Werner states, Eq. (15), obey both the reduction as well as the majorization criterion. It is possible, but unproven, that any state which satisfies the reduction criterion also satisfies the majorization criterion.

Unfortunately, nonviolation of the reduction criterion and nonviolation of the majorization criterion are *not* properties that are preserved under local actions and classical communications. To take an example, consider the following density matrix $\sigma = \mathbf{1}_A/d \otimes |\Psi^+\rangle\langle\Psi^+| \otimes \mathbf{1}_B/d$ where $\mathbf{1}_A/d$ ($\mathbf{1}_B/d$) is a density matrix for Alice (Bob), $|\Psi^+\rangle$ is a maximally entangled state in $\mathscr{H}_n \otimes \mathscr{H}_n$ and d is large. The state $P_+ = |\Psi^+\rangle\langle\Psi^+|$ violates the reduction criterion

$$\mathbf{1}/n - P_+ \not\geqslant 0. \tag{22}$$

We can always choose $d > n$ large enough such that both the reduction criteria are satisfied for σ:

$$\mathbf{1}_A \otimes [\mathbf{1}_A \otimes \mathbf{1}_B/n - P_+/d] \otimes \mathbf{1}_B \geqslant 0$$

and

$$\mathbf{1}_A \otimes [\mathbf{1}_A/n \otimes \mathbf{1}_B - P_+/d] \otimes \mathbf{1}_B \geqslant 0. \tag{23}$$

By the local action of tracing over the register with $\mathbf{1}_A/d$ and $\mathbf{1}_B/d$, we obtain the state P_+ which does violate the reduction criterion. Thus there exists states which initially

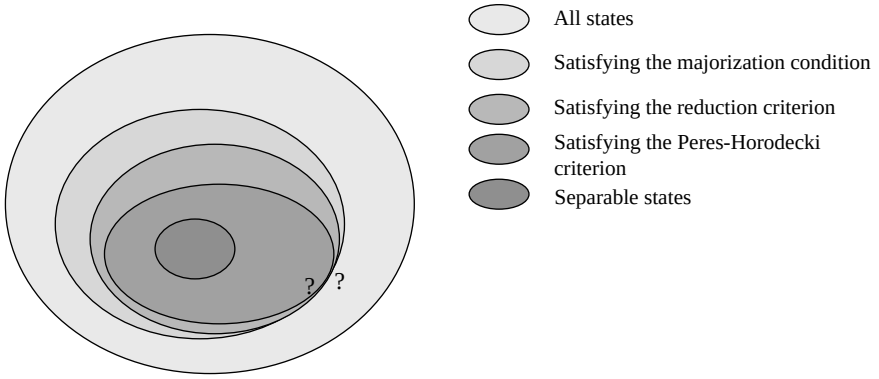

Fig. 3. Relations between various bipartite separability criteria. It is not known whether the Reduction Criterion set and the Peres–Horodecki set are contained in the Majorization set. In $\mathcal{H}_2 \otimes \mathcal{H}_2$ all sets, except the outer one, collapse onto each other and mark the separation of the set of separable states from the entangled states.

do not violate the reduction criterion, but nonetheless are distillable. The same example can serve to show that the majorization criterion can be violated *only after* some local action.

In Fig. 3 we have sketched an overview of the known relations between the various bipartite separability criteria.

3. Multipartite entanglement

Every time we consider a multipartite system in a bipartite fashion, that is, we split the set of parties in two subsets, and consider the entanglement between the subsets, we can apply the criteria that we have listed in the previous section. In this section, we will focus on features of multipartite quantum entanglement which are special to multipartite quantum entanglement.

3.1. Violations of local realism and bell inequalities

The Greenberger–Horne–Zeilinger state $|GHZ\rangle = 1/\sqrt{2}(|000\rangle - |111\rangle)$ is an example of a three party state which violates the predictions of local realism [41]. The GHZ-state is an eigenvector of operators $X \otimes Y \otimes Y$, $Y \otimes X \otimes Y$, $Y \otimes Y \otimes X$ with eigenvalues $+1$ and $X \otimes X \otimes X$ with eigenvalue -1. These first three operators form the generators of an abelian group G which contains $X \otimes X \otimes X$. For these four operators, from a measurement of X or Y on two of the spins we can deduce the outcome of the third since $|GHZ\rangle$ is an eigenstate. Therefore, according to local realism, we may assign values to the local operators X_i and Y_i according to some function f

$$f : X_i \to \{-1, +1\} \quad f : Y_i \to \{-1, +1\}, \tag{24}$$

where X_i acts on the ith particle, obeying the eigenequation constraints. The function f gives rise to a function $h: g \in G \to \{-1,+1\}$, i.e. $h(X \otimes Y \otimes Y) = f(X)f(Y)f(Y)$. A violation of local realism occurs when it is impossible to construct a local function f (consistent with the eigenvalue equations for the generators) such that h is a *group homomorphism*, i.e. $h(g_1 \circ g_2) = h(g_1) \circ h(g_2)$ for all $g_1, g_2 \in G$. In the case of the GHZ-state, the violation comes about by observing that the local assignments (the function f) for the generators $X \otimes Y \otimes Y$, $Y \otimes X \otimes X$ and $X \otimes X \otimes Y$ always give $h(X \otimes X \otimes X) = 1$ whereas the GHZ-state has eigenvalue -1 with respect to $X \otimes X \otimes X$.

In Ref. [14] violations of local realism were found for a special class of multipartite entangled states. These are states used in quantum error correction codes based on the stabilizer formalism. The states are by definition the eigenvectors of an abelian group made from tensor products of Pauli matrices and **1**.

These violations do not yet present us with a separability criterion. The only claim is that if the outcomes of local measurements of X and Y were to correspond *exactly* to, say, the outcomes on the GHZ-state, then we may conclude that these measurement outcomes cannot be described by a local hidden variable theory. However, to establish a full separability criterion, we would need to analyze what ranges of outcomes could still be reproduced by a separable state or local hidden variable theory and what outcomes cannot.

The n-qubit Bell–Klyshko operator [21] or Mermin's inequality [40] in operator form (see for example Ref. [57]) do constitute a separability criterion in this way. The Bell–Klyshko operator can be defined recursively

$$\mathscr{B}_n = \mathscr{B}_{n-1} \otimes \frac{1}{2}(\vec{a}_n \cdot \vec{\sigma} + \vec{a}'_n \cdot \vec{\sigma}) + \mathscr{B}'_{n-1} \otimes \frac{1}{2}(\vec{a}_n \cdot \vec{\sigma} - \vec{a}'_n \cdot \vec{\sigma}), \tag{25}$$

where $\mathscr{B}'_{n-1} = \mathscr{B}_{n-1}(\vec{a}_1 \leftrightarrow \vec{a}'_1, \vec{a}_2 \leftrightarrow \vec{a}'_2, \ldots, \vec{a}_{n-1} \leftrightarrow \vec{a}'_{n-1})$ and $\mathscr{B}_2$ is the Bell-CHSH operator in Eq. (2). Its expectation value for all separable states is bounded as $\operatorname{Tr} \mathscr{B}_n \rho_{\text{sep}} \leqslant 2$, whereas a value as large as $2^{(n+1)/2}$ can be obtained for the cat state $|GHZ_n\rangle = 1/\sqrt{2}(|0^{\otimes n}\rangle + |1^{\otimes n}\rangle)$. As in the bipartite case, these operators are examples of entanglement witnesses.

3.2. Entanglement witnesses and linear maps

In Ref. [26] the notion of entanglement witnesses was formally extended to the domain of multipartite quantum systems. The multipartite analog of Theorem 1 separates the multipartite separable states from any entangled state; for every state ρ, not of the form $\rho = \sum_i p_i |\psi_i^{A_1}\rangle\langle\psi_i^{A_1}| \otimes \cdots \otimes |\psi_i^{A_n}\rangle\langle\psi_i^{A_n}|$, there exists a Hermitian operator H, the entanglement witness, such that

$$\operatorname{Tr} H\rho_{\text{sep}} \geqslant 0 \tag{26}$$

for all separable states ρ and $\operatorname{Tr} H\rho < 0$. Interestingly, these multipartite witnesses can be shown [26] to relate to linear maps $\mathscr{L}: B(\mathscr{H}^2 \otimes \mathscr{H}^3 \otimes \cdots \otimes \mathscr{H}^n) \to B(\mathscr{H}^1)$ with

the property that for all product vectors $|x_2,\ldots,x_n\rangle$,

$$\mathscr{L}(|x_2,\ldots,x_n\rangle\langle x_2,\ldots,x_n|) \geqslant 0. \tag{27}$$

The linear map $\mathscr{L}$ is thus not necessarily positive on $B(\mathscr{H}^2\otimes\mathscr{H}^3\otimes\cdots\otimes\mathscr{H}^n)$; this is an important difference with the bipartite case. The 1–1 relation between a witness H with the property of Eq. (26) and the map $\mathscr{L}$ with the property of Eq. (27) is the following:

$$H = (\mathbf{1}_1\otimes\mathscr{L}^\dagger)(|\Psi^+\rangle\langle\Psi^+|), \tag{28}$$

where $|\Psi^+\rangle$ is a maximally entangled state in $\mathscr{H}^1\otimes\mathscr{H}^1$. Here the Hermitian conjugate of $\mathscr{L}$, $\mathscr{L}^\dagger$ is defined by the relation $\operatorname{Tr}A^\dagger\mathscr{L}(B)=\operatorname{Tr}\mathscr{L}^\dagger(A^\dagger)B$.

In Ref. [34] a family of multiqubit entanglement witnesses was presented. For an n-partite qubitsystem the authors introduce an averaging observable $\bar{a}=1/n\sum_{i=1}^n a_i$ where a_i is an observable acting on the ith factor in $\mathscr{H}^1\otimes\mathscr{H}^2\otimes\cdots\otimes\mathscr{H}^n$. The operators a_i are bounded in their norm, $\|a_i\|\leqslant 1$ (here $\|\cdot\|$ is the standard operator norm). The operator $\bar{a}$ could, for example, be a sum of Pauli operators Z_i, measuring a mean magnetic field in the z-direction. It is proved in Ref. [34] that for separable density matrices ρ the expectation of the commutator

$$|\operatorname{Tr}\rho[\bar{a},c]| \leqslant \frac{2}{\sqrt{n}} \tag{29}$$

for any averaging observable $\bar{a}$ and $c=c^\dagger$ with $\|c\|\leqslant 1$. An expectation value such as Eq. (29) can appear in a perturbative expansion in linear response theory (see for example Section IV in Ref. [54]). The operator c will then be a nonlocal time-dependent observable, the operator $\bar{a}$ some local mean field observable and ρ can be the equilibrium state of a physical system. For entangled states the expectation value of the commutator in Eq. (29) can be of order 1 as was shown in Ref. [34]. A consequence is that for such entangled states the region of validity of the perturbation theory is much smaller than for separable states. Let us translate the result in the language of entanglement witnesses. The observable

$$H = \frac{2}{\sqrt{n}}\mathbf{1} - i[\bar{a},c] \tag{30}$$

is a witness in the sense that Eq. (26) holds. This witness can detect the entanglement in superpositions of macroscopically distinct states, such as the cat $|GHZ_n\rangle$ state. For example (see Ref. [34]) when we choose the operators $a_i=|1\rangle\langle 1|_i$ and $c=i[|0^{\otimes n}\rangle\langle 1^{\otimes n}|-|1^{\otimes n}\rangle\langle 0^{\otimes n}|]$, we obtain a witness which has

$$\langle GHZ_n|H|GHZ_n\rangle = \frac{2}{\sqrt{n}} - 1, \tag{31}$$

which is negative when $n>2$.

3.3. Incomparable forms of pure state entanglement

The possibility for extraction of bipartite pure state entanglement from mixed state entanglement by LOCC is captured by the notion of distillation, which we discussed in Section 2.3. The definition of bipartite distillation does not depend on the form—maximally or partially entangled states—of the final pure state entanglement, since the *Asymptotic Interconversion Theorem* for bipartite entanglement [4] says that all bipartite pure state entanglement is interconvertible by LOCC in the asymptotic limit (when we have many copies of a state). For multipartite entanglement no such theorem exists. The exploration of interconvertibility of multipartite entanglement was initiated in Ref. [8]. It was found for example that 3 EPR pairs $(|00\rangle + |11\rangle)^{\otimes 3}$ shared among three parties were not exactly convertible by LOCC to 2 GHZ states $(|000\rangle + |111\rangle)^{\otimes 2}$. In Ref. [39] this result was considerably strengthened by showing that $3n$ EPR pairs are not interconvertible to $2n$ GHZ states even in the asymptotic limit $n \to \infty$. As such these states form the building blocks of an MREGS, a Minimal Reversible Entanglement Generating Set [8], with which all tripartite entanglement can reversibly be created. It is an open question whether a third type of state, the W-state $|001\rangle + |010\rangle + |100\rangle$ should be added to the tripartite MREGS, in other words whether the W-state is asymptotically interconvertible to a supply of EPR pairs and GHZ states (see Refs. [19] and [20] for indications that this may not be the case). These results show that intrinsically *multipartite* forms of pure state entanglement exist.

3.4. Bound entanglement

One of the best illustrations of the phenomenon of intrinsic mixed state 'multipartiteness' was given in Ref. [6]. It is an example of a tripartite mixed state in $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$ which is separable over all bipartite cuts of the three parties, while at the same time the state is entangled. Let $|v_1\rangle = |000\rangle$, $|v_2\rangle = |-+1\rangle$, $|v_3\rangle = |+1-\rangle$ and $|v_4\rangle = |1-+\rangle$, where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$. The state is

$$\rho_{\text{Shifts}} = \mathbf{1} - \sum_{i=1}^{4} |v_i\rangle\langle v_i|. \tag{32}$$

No product state exists in the range of ρ_{Shifts}, since the vectors $\{|v_1\rangle, |v_2\rangle, |v_3\rangle, |v_4\rangle\}$ form an unextendible product basis [6]. At the same time, the product basis can be completed with vectors which are separable over a bipartite cut, which results in ρ being separable over this cut. The density matrix ρ_{Shifts} in Eq. (32) is also an example of a *bound entangled* state in the multipartite setting; if entanglement could be distilled from $\rho_{\text{Shifts}}^{\otimes n}$ by local actions and classical communications of the three parties, then entanglement would be created over some bipartite cut, which is forbidden since ρ is separable over all cuts.

The phenomenon of multipartite bound entanglement is more general than this. It can be argued [49] that any multipartite density matrix ρ for parties $A_1, \ldots, A_k$ is bound entangled when for all pairs of parties (A_i, A_j) there exists a cut (a bipartition) where A_i and A_j are in different sets of parties, such that ρ is either separable or PPT

over this cut. This follows from the fact that these separability and PTT properties are preserved under LOCC and the fact that any multipartite pure entangled state is entangled over some bipartition. In Ref. [16] and Ref. [49] multiqubit examples of such bound entangled states were presented. Moreover in Ref. [49] it was shown that two 4-party bound entangled states both distributed among 5 parties, can be distillable. The state ρ^{ACBD} is a mixture of Bell states; with probability $1/4$, A and C share one of the 4 Bell states and B and D share *the same* Bell state. The state is symmetric under permutation of parties. Furthermore it is separable over any bipartition into $(2,2)$, but it is entangled for any bipartition into $(3,1)$. The other state ρ^{ABCE} is identical, except that now it is shared among A, B, C and E. The essential feature of these two states taken together, is that there exists no bipartition over which $\rho^{ACBD} \otimes \rho^{ABCE}$ is separable such that the parties D and E belong to different sets. This fact makes it possible for entanglement to be distilled between D and E and the authors of Ref. [49] show that 1 singlet (1 ebit) can be obtained from the two bound entangled states.

4. Experimental issues: detecting quantum entanglement

In this section, we consider how the criteria that we have discussed in the previous sections enable us to decide by physical experiment whether the physical state of a given quantum state is entangled. The capacity to build certain entangled states is one of the basic requirements for making a quantum computer and is often used as a benchmark test for the amount of control and coherence in a particular quantum system, see for example the creation of the cat state $|0^{\otimes 7}\rangle + |1^{\otimes 7}\rangle$ in the NMR experiment in Ref. [36].

It is desirable that the verification of the entanglement take place with a minimal number of measurements and operations. The first, but inefficient option would be to perform full quantum tomography on the state ρ, i.e. determine all the matrix elements ρ_{ij}, after which we may analyze the state on paper using the various separability criteria. If no prior knowledge exists about the state, then it appears that there is no shortcut to such a quantum tomography experiment.[1] In the more common situation in which we expect to have created a certain state ρ, more efficient methods exist. A traditional method for detecting entanglement (employed for example in Ref. [9]) is to test for a violation of a Bell type inequality. We have indicated in this review that these tests are part of a larger framework of entanglement witnesses which exists both in the bipartite as well as in the multipartite setting. In Ref. [37] the notion of an optimal entanglement witness was introduced; an entanglement witness H is *optimal* if there exists no other witness H' which detects the same entanglement (the same states) as H *and more*. These optimal witnesses are the ones that will be useful in detecting quantum entanglement. We will need the following additional definition:

Definition 4. A ρ-optimal witness H_* for an entangled state ρ is an optimal entanglement witness according to the definition in Ref. [37] and among the optimal normalized

[1] A 'shortcut' was found after completion of this paper, see the method in Ref. [4].

witnesses, it is the best in detecting the entanglement of ρ, i.e.

$$\operatorname{Tr} H_*\rho = \min_{\text{optimal } H} \operatorname{Tr} H\rho, \tag{33}$$

with H normalized as

$$\operatorname{Tr} H = 1. \tag{34}$$

In the next sections, we will consider the optimal ψ-witness for pure states $|\psi\rangle$ and small systems, for mixed states in larger systems and for multipartite entangled states. In Section 4.4, we consider how well these entanglement witnesses detect entanglement in the vicinity of the desired entangled state.

4.1. (Multipartite) pure states, small bipartite mixed states

Let us assume that we believe that the state of our multi- or bi-partite quantum system is an entangled state $|\psi\rangle$ and let us assume that we are interested in detecting the entanglement of $|\psi\rangle$ over some bipartite A–B cut $\mathscr{H}_A \otimes \mathscr{H}_B$. For pure states, there always exists a witness H of the form

$$H = aP + (1-a)(\mathbf{1}\otimes T)(Q), \tag{35}$$

where $P \geqslant 0$ and $Q \geqslant 0$, see Section 2.2. An optimal witness (see Theorem 2, Ref. [37]) in this class[2] has $a = 0$ and has the property that the operator Q has no product states in its range. To optimize with respect to the state $|\psi\rangle$ we choose $Q = |\psi_{\mu_{\min}}\rangle\langle\psi_{\mu_{\min}}|$ where $|\psi_{\mu_{\min}}\rangle$ is the eigenvector of $(\mathbf{1}\otimes T)(|\psi\rangle\langle\psi|)$ which has the smallest eigenvalue (which is negative). Such a witness is optimal in the sense of Ref. [37]. The optimality of this choice with respect to $|\psi\rangle$ follows from

$$\operatorname{Tr}(\mathbf{1}\otimes T)(Q)|\psi\rangle\langle\psi| = \operatorname{Tr} Q\,(\mathbf{1}\otimes T)(|\psi\rangle\langle\psi|) \geqslant \lambda_{\min}, \tag{36}$$

since $Q \geqslant 0$ and $\operatorname{Tr} Q = 1$ due to normalization.

To see the explicit form of such a witness, we write $|\psi\rangle$ in the Schmidt decomposition $|\psi\rangle = \sum_i \sqrt{\lambda_i}|a_i\rangle \otimes |b_i\rangle$ and take the partial transpose in a fixed basis $|0\rangle, |1\rangle, \ldots$. We have

$$(\mathbf{1}\otimes T)\left(\sum_{i,j} \sqrt{\lambda_i\lambda_j}|a_i\rangle\langle a_j| \otimes |b_i\rangle\langle b_j|\right) = \sum_{i,j} \sqrt{\lambda_i\lambda_j}|a_i\rangle\langle a_j| \otimes |b_j^*\rangle\langle b_i^*|, \tag{37}$$

which has eigenvectors and corresponding eigenvalues $\{|a_i, b_i^*\rangle, \lambda_i\}$ and for $i \neq j$,

$$\left\{\frac{1}{\sqrt{2}}(|a_i\rangle \otimes |b_j^*\rangle \pm |a_j\rangle \otimes |b_i^*\rangle),\ \pm\sqrt{\lambda_i\lambda_j}\right\}. \tag{38}$$

[2] We will only be optimizing amongst the decomposable witnesses to keep things as simple as possible.

We choose the eigenvector with the most negative of the eigenvalues, let us call it $\mu_{\min} = -\max_{i\neq j} \sqrt{\lambda_i \lambda_j}$. The optimal ψ-witness is equal to

$$H_* = \tfrac{1}{2}\left(|a_i,b_j\rangle\langle a_i,b_j| + |a_j,b_i\rangle\langle a_j,b_i| - |a_i,b_i\rangle\langle a_j,b_j| - |a_j,b_j\rangle\langle a_i,b_i|\right) \tag{39}$$

for the pair (i,j) corresponding to $\mu_{\min}$. Let us take a simple example.

Example 5. For the state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$, the optimal witness is

$$H_* = \tfrac{1}{2}(|0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0| - |0,0\rangle\langle 1,1| - |1,1\rangle\langle 0,0|) \tag{40}$$

and $\mu_{\min} = -\sqrt{\cos\theta \sin\theta}$.

For bipartite quantum systems consisting of 2 qubits or 1 qutrit + 1 qubit, the entanglement witness is always decomposable, i.e. of the form $H = aP + (1-a)(\mathbf{1}\otimes T)(Q)$ (see Section 2.2). As for pure states, the witness is optimal when $a = 0$ and Q has no product states in its range. To optimize for ρ among such witnesses, we find the eigenvector $|\psi_{\mu_{\min}}\rangle$ [3] of $(\mathbf{1}\otimes T)(\rho)$ with the smallest eigenvalue $\mu_{\min}$ and we choose

$$H_* = (\mathbf{1}\otimes T)(|\psi_{\mu_{\min}}\rangle\langle\psi_{\mu_{\min}}|). \tag{41}$$

4.2. Mixed state entanglement in higher dimensions

Let ρ be a (multipartite) mixed state in dimensions more than $\mathcal{H}_2\otimes\mathcal{H}_2$ or $\mathcal{H}_2\otimes\mathcal{H}_3$ whose entanglement we wish to detect over a bipartite cut A–B. If ρ violates the Peres–Horodecki criterion then the methods in the previous Section can be applied to determine an optimal entanglement witness. When ρ has the PPT property and is believed to be entangled, then ρ has bound entanglement and we will need an indecomposable entanglement witness for ρ (see Section 2.2). In Ref. [37] a method was developed to optimize a given indecomposable entanglement witness. The problem is a lot harder than for decomposable witnesses: a generic form for an optimal witness is not known. Nonetheless we can sketch a procedure for finding an optimal indecomposable witness which detects ρ:

(1) Find a decomposable witness H, Eq. (10), for which $\mathrm{Tr}\, H\rho = 0$ with $\mathrm{Tr}\, H = 1$.
(2) Choose as a starting point the indecomposable witness $H' = (H - \varepsilon\mathbf{1})/(1-\varepsilon d)$ where $\varepsilon = \inf_{\psi_1,\psi_2}\langle\psi_1,\psi_2|\, H\, |\psi_1,\psi_2\rangle$ which ensures that H' is a (normalized) witness. Here d is the total dimension of the quantum system.
(3) Optimize H' to H_* with the methods in Ref. [37], taking into account the optimality with respect to ρ, see Definition 4. The optimized witness relates to H' as

$$H_* = (H' - \lambda_* D_*)/(1-\lambda_*), \tag{42}$$

[3] This eigenvector is always entangled, since for all product states $|\psi_A,\psi_B\rangle$, $\langle\psi_A,\psi_B|\,(\mathbf{1}\otimes T)(\rho)\,|\psi_A,\psi_B\rangle = \mathrm{Tr}\,\rho\,(\mathbf{1}\otimes T)(|\psi_A,\psi_B\rangle\langle\psi_A,\psi_B|) \geqslant 0$.

where λ_* is a constant depending on D_* and H' (see Eq. (13) in Ref. [37]) and where D_* is a normalized decomposable witness, Eq. (35), with the property that for all product states $|\psi_1,\psi_2\rangle$ such that (1) $\langle\psi_1,\psi_2|H'|\psi_1,\psi_2\rangle = 0$ we have $\langle\psi_1,\psi_2|D_*|\psi_1,\psi_2\rangle = 0$, (2) λ_* and D_* are such that H_* is an optimal indecomposable entanglement witness (no more decomposable witnesses can be subtracted from it) and (3) when under constraints (1) and (2) there is still freedom of choice in λ_* and D_*, we choose an H_* which is optimal with respect to ρ, i.e. $\mathrm{Tr}\, H_*\rho$ is minimal.

It is not guaranteed that this procedure will lead to a ρ-optimal indecomposable witness according to Definition 4. The method does however ensure that the witness is optimal as well as detecting the entanglement of ρ.

4.3. Multipartite (Bound) entanglement

The entanglement witness framework carries over to multipartite states. This framework is particularly useful when entanglement is to be detected in a bound entangled state such as the first example ρ_{Shifts}, Eq. (32), in Section 3.4 which is separable over all bipartitions. For this state an entanglement witness was found in Ref. [26], in analogy to the construction in Ref. [52]. Even though various Bell inequalities and entanglement witnesses exist for multipartite entanglement (Sections 3.1 and 3.2), a more elaborate theory as in the bipartite case is still lacking. We would also like to refer the reader to Ref. [17] for alternative ideas on the experimental detection of entanglement in multiqubit states.

4.4. The vicinity of the trial state

Often the quantum system under consideration will not exactly be in the desired state ρ. It is therefore essential that the entanglement witness that we chose is robust, in the sense that it detects as much entanglement as possible in the neighborhood of ρ (provided that the neighborhood is entangled). This property is guaranteed in the following manner. Let ρ' be all states in the 'vicinity' of ρ, namely for a given ε, $\Delta = \rho' - \rho$

$$\|\Delta\|_1 \leqslant \varepsilon, \tag{43}$$

where $\|\cdot\|_1$ is the tracenorm, i.e. $\|A\|_1 = \mathrm{Tr}\sqrt{A^\dagger A}$. Letting H_* be the optimal ρ-witness, we have

$$\mathrm{Tr}\, H_*\rho' = \mathrm{Tr}\, H_*\rho + \mathrm{Tr}\, H_*\Delta. \tag{44}$$

The last quantity can be bounded, using the Schwarz inequality $|\mathrm{Tr}\, A^\dagger B| \leqslant \sqrt{\mathrm{Tr}\, A^\dagger A}\,\sqrt{\mathrm{Tr}\, B^\dagger B}$ and also $\sqrt{\mathrm{Tr}\, A^\dagger A} \leqslant \mathrm{Tr}\sqrt{A^\dagger A}$. This gives

$$\mathrm{Tr}\, H_*\rho - \varepsilon\sqrt{\mathrm{Tr}\, H_*^2} \leqslant \mathrm{Tr}\, H_*\rho' \leqslant \mathrm{Tr}\, H_*\rho + \varepsilon\sqrt{\mathrm{Tr}\, H_*^2}. \tag{45}$$

For the optimal decomposable entanglement witnesses given in Section 4.1 we have $\sqrt{\mathrm{Tr}\, H_*^2} = 1$, irrespective of the dimension of the system. Thus when ρ' is close to the state ρ, the optimal witness H_* for ρ will also detect the entanglement in ρ'. We will now consider a specific example in which all states in a certain class are detected by one entanglement witness:

Example 6. Let $|\Psi\rangle$ be any maximally entangled pure state in a bipartite space of total dimension d. Instead of $|\Psi\rangle$ the physical state of our quantum system is

$$\rho_p = p|\Psi\rangle\langle\Psi| + \frac{1-p}{d}\mathbf{1}. \tag{46}$$

As long as $(\mathbf{1}\otimes T)(\rho_p) \not\geqslant 0$, the optimal Ψ-witness $H_* = (\mathbf{1}\otimes T)(|\psi_{\mu_{\min}}\rangle\langle\psi_{\mu_{\min}}|)$ will detect the entanglement of ρ_p. The eigenvector with the minimal eigenvalue of $(\mathbf{1}\otimes T)(\rho_p)$ is the same for all $p\in[0,1]$. Furthermore the density matrix ρ_p has the property that it is separable *if and only if* it satisfies the Peres–Horodecki criterion [25]. Therefore the entanglement in all (entangled) ρ_p is witnessed by H_*, since $\mathrm{Tr}\, H_*\rho_p$ is negative as long as ρ_p violates the Peres–Horodecki criterion.

4.5. Measurement of the witness

In principle, the entanglement witness method has the advantage that only one observable, the entanglement witness, needs to be measured. In practice, the measurement of this observable may be done by a series of local measurements. Consider for example the entanglement witness of Example 5, in terms of the Pauli-matrices it reads

$$H_* = \tfrac{1}{4}(I\otimes I + Y\otimes Y - X\otimes X - Z\otimes Z). \tag{47}$$

A measurement of all the Pauli matrices on both sides is needed to measure this observable by local measurements. At this point the advantage over basic state tomography becomes somewhat questionable. The entanglement witness will in general be a nonlocal observable. But if we allow for nonlocal measurements, or rotate the state by a nonlocal rotation U prior to testing such that $UH_*U^\dagger$ is local, there exists a real advantage over state tomography. A CNOT gate where the first qubit is the control and the second is the target, will rotate H_* in Eq. (47) to a product of operators

$$\mathrm{CNOT}_{A\to B}\, H_*\, \mathrm{CNOT}^\dagger_{A\to B} = \tfrac{1}{4}(\mathbf{1}-X)\otimes(\mathbf{1}-Z)). \tag{48}$$

Thus some quantum computation power is needed to measure the entanglement witness efficiently. For large systems one may ask whether such quantum computation can be performed efficiently, in polynomial time in the number of qubits, for states which can be built efficiently. With this open question we will conclude our review.

Acknowledgements

Thanks to Patrick Hayden for suggesting an improved counterexample in Section 2.4, to Michał and Paweł Horodecki for discussions on the entropic inequalities, to Daniel

Gottesman for discussions on homomorphisms and positive maps and to David DiVincenzo for reading through this manuscript.

Appendix A. Indecomposable positive linear maps and Hilbert's 17th problem

In Ref. [11] it was shown how certain indecomposable positive linear maps present answers (in the negative) to Hilbert's 17th problem. Hilbert's 17th problem asks whether all positive semidefinite homogeneous polynomials are sums of squares of homogeneous polynomials (see Ref. [47] for some history on the problem). Indecomposable positive maps with real coefficients present counterexamples for polynomials which are real biquadratic forms. The construction is the following.

Given is a positive indecomposable map $\mathscr{L}: B(\mathscr{H}_n) \to B(\mathscr{H}_m)$ which is known not to be completely positive. Furthermore, the coefficients of $\mathscr{L}$ in some fixed basis $\{|i\rangle\}$ are real and therefore $\mathscr{L}$ maps real (symmetric) matrices in $B(\mathscr{H}_n)$ onto real symmetric matrices in $B(\mathscr{H}_m)$. Note that matrix transposition acts as the identity on real symmetric matrices and therefore we restrict ourselves to indecomposable maps.

We define a positive semidefinite symmetric biquadratic form in the following way:

$$F(x_1,\ldots,x_n;y_1,\ldots,y_m) = \langle y|\,(\mathscr{L}(|x\rangle\langle x|)\,|y\rangle, \tag{A.1}$$

where $|x\rangle$ and $|y\rangle$ are unnormalized vectors with coefficients $|x\rangle = \sum_i x_i|i\rangle$ and $|y\rangle = \sum_i y_i|i\rangle$, $x_i \in \mathbf{R}$ and $y_i \in \mathbf{R}$. The positivity of the map $\mathscr{L}$ guarantees the positive semidefiniteness of $F(x_1,\ldots,x_n;y_1,\ldots,y_m)$ for all $x_1,\ldots,x_n,y_1,\ldots,y_m$, or

$$F(x_1,\ldots,x_n;y_1,\ldots,y_m) = \sum_{i,j,k,l} \mathscr{L}_{ij,kl} x_i x_j y_k y_l \geqslant 0. \tag{A.2}$$

Now we pose Hilbert's question: is every positive semidefinite symmetric biquadratic form a sum of squares, i.e.

$$F(x_1,\ldots,x_n;y_1,\ldots,y_m) \stackrel{?}{=} \sum_t (G_t(x_1,\ldots,x_n;y_1,\ldots,y_m))^2, \tag{A.3}$$

where $G_t(x_1,\ldots,x_n;y_1,\ldots,y_m)$ is a symmetric bilinear form, i.e.

$$G_t(x_1,\ldots,x_n;y_1,\ldots,y_m) = \sum_{i,j} g^t_{ij} x_i y_j. \tag{A.4}$$

Assume that the equality in Eq. (A.3) holds. We define a set of real operation elements A_t with

$$\langle j|\,A_t\,|i\rangle = g^t_{ij}, \tag{A.5}$$

so that

$$\sum_t (G_t(x_1,\ldots,x_n;y_1,\ldots,y_m))^2 = \sum_t \langle y|\,A_t|x\rangle\langle x|A_t^{\mathrm{T}}\,|y\rangle. \tag{A.6}$$

This would imply that the map $\mathscr{L}$ has a decomposition in terms of the operation elements A_t and therefore $\mathscr{L}$ is a completely positive map. Conversely, when a map $\mathscr{L}$ is completely positive, the corresponding positive semidefinite symmetric biquadratic form is a sum of squares. Instead of the positive indecomposable map $\mathscr{L}$, we could have defined the biquadratic form in terms of an (indecomposable) entanglement witness H with real coefficients:

$$F(x_1,\ldots,x_n;y_1,\ldots,y_m) = \langle y,x|\, H\,|y,x\rangle \geqslant 0 \tag{A.7}$$

for all real vectors $|y,x\rangle$. It was shown how to construct (real-valued) entanglement witnesses for every (real) unextendible product bases (UPB) in Ref. [52]; furthermore the graph-theoretic UPB construction in Ref. [1] always has a realization with real vectors.

References

[1] N. Alon, L. Lovász, Unextendible product bases, J. Combin. Theory, Ser. A 95 (1) (2001) 169–179.
[2] T. Ando, Majorizations and inequalities in matrix theory, Linear Algebra Appl. 199 (1994) 17–67.
[3] J.S. Bell, On the Einstein–Podolsky–Rosen paradox, Physics 1 (1964) 195–200.
[4] C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A 53 (1996) 2046–2052.
[5] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels, Phys. Rev. Lett. 70 (1993) 1895–1899.
[6] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, B.M. Terhal, Unextendible product bases and bound entanglement, Phys. Rev. Lett. 82 (1999) 5385–5388, quant-ph/9808030.
[7] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W.K. Wootters, Mixed state entanglement and quantum error correction, Phys. Rev. A 54 (1996) 3824–3851, quant-ph/9604024.
[8] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin, A.V. Thapliyal, Exact and asymptotic measures of multipartite pure state entanglement, Phys. Rev. A 63 (2000) 012307, quant-ph/9908073.
[9] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, A. Zeilinger, Observation of three-photon Greenberger–Horne–Zeilinger entanglement, Phys. Rev. Lett. 82 (1999) 1345–1349, quant-ph/9810035.
[10] N.J. Cerf, C. Adami, R.M. Gingrich, Quantum conditional operator and a criterion for separability, Phys. Rev. A 60 (1999) 893–898, quant-ph/9710001.
[11] M.-D. Choi, Positive semidefinite biquadratic forms, Linear Algebra Appl. 12 (1975) 95–100.
[12] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. 23 (1969) 880.
[13] D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, B.M. Terhal, Unextendible product bases, uncompletable product bases and bound entanglement, Comm. Math. Phys., submitted for publication, quant-ph/9908070.
[14] D.P. DiVincenzo, A. Peres, Quantum codewords contradict local realism, Phys. Rev. A 55 (1997) 4089–4092, quant-ph/9611011.
[15] D.P. DiVincenzo, P.W. Shor, J.A. Smolin, B.M. Terhal, A.V. Thapliyal, Evidence for bound entangled states with negative partial transpose, Phys. Rev. A 61 (2000) 062312/1–13, quant-ph/9910026.
[16] W. Dür, J.I. Cirac, Classification of multi-qubit mixed states: separability and distillability properties, Phys. Rev. A 61 (2000) 042314, quant-ph/9911044.
[17] W. Dür, J.I. Cirac, Multiparticle entanglement and its experimental detection, J. Phys. A 34(35) (2001) 6837–6850, quant-ph/0011025.
[18] W. Dür, J.I. Cirac, M. Lewenstein, D. Bruss, Distillability and partial transposition in bipartite systems, Phys. Rev. A 61 (2000) 062313, quant-ph/9910022.

[19] W. Dür, G. Vidal, J.I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A 62 (2000) 062314, quant-ph/0005115.
[20] E.F. Galvao, M.B. Plenio, S. Virmani, Tripartite entanglement and quantum relative entropy, J. Phys. A 33 (2000) 8809, quant-ph/0008089.
[21] N. Gisin, H. Bechmann-Pasquinucci, Bell inequality, Bell states and maximally entangled states for *n* qubits, Phys. Lett. A 246 (1998) 1–6.
[22] D. Gottesman, I. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single qubit operations, Nature 402 (6760) (1999) 390–393, quant-ph/9908010.
[23] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, Phys. Lett. A 232 (1997) 333–339, quant-ph/9703004.
[24] M. Horodecki, P. Horodecki, Private communication.
[25] M. Horodecki, P. Horodecki, Reduction criterion of separability and limits for a class of distillation protocols, Phys. Rev. A 59 (1999) 4206–4216, quant-ph/9708015.
[26] M. Horodecki, P. Horodecki, R. Horodecki, Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps, Phys. Lett. A 283 1–7 quant-ph/0006071.
[27] M. Horodecki, P. Horodecki, R. Horodecki, Separability of mixed states: necessary and sufficient conditions, Phys. Lett. A 223 (1996) 1–8, quant-ph/9605038.
[28] M. Horodecki, P. Horodecki, R. Horodecki, Inseparable two spin 1/2 density matrices can be distilled to a singlet form, Phys. Rev. Lett. 78 (1997) 574–577, quant-ph/9607009.
[29] M. Horodecki, P. Horodecki, R. Horodecki, Mixed state entanglement and distillation: is there a 'bound' entanglement in nature?, Phys. Rev. Lett. 80 (1998) 5239–5242, quant-ph/9801069.
[30] M. Horodecki, P. Horodecki, R. Horodecki, in: G. Alber, M. Weiner (Eds.), Mixed-state Entanglement and Quantum Communication in Quantum Information—Basic Concepts and Experiments, Springer, Berlin, 2000.
[31] P. Horodecki, M. Lewenstein, G. Vidal, I. Cirac, Operational criterion and constructive checks for the separability of low rank density matrices, Phys. Rev. A 62 (2000) 032310, quant-ph/0002089.
[32] P. Horodecki, J.A. Smolin, B.M. Terhal, A.V. Thapliyal, Rank two bound entangled states do not exist, quant-ph/9910122.
[33] A. Jamiołkowski, Linear transformations which preserve trace and positive semidefiniteness of operators, Rev. Mod. Phys. 3 (1972) 275–278.
[34] D. Janzing, Th. Beth, Fragility of a class of highly entangled states with n qubits, Phys. Rev. A 61 (2000) 052308, quant-ph/9907042.
[35] E. Knill, R. Laflamme, R. Martinez, C.-H. Tseng, An algorithmic benchmark for quantum information processing, Nature 404 (2000) 368–370, quant-ph/9908051.
[36] E. Knill, R. Laflamme, G. Milburn, Efficient linear optics quantum computation, Nature 409 (2001) 46–52, quant-ph/0006088.
[37] M. Lewenstein, B. Kraus, J.I. Cirac, P. Horodecki, Optimization of entanglement witnesses, Phys. Rev. A 62, 052310/1–6, quant-ph/0005014.
[38] M. Lewenstein, B. Kraus, P. Horodecki, J.I. Cirac, Characterization of separable states and entanglement witnesses, Phys. Rev. A 63, 044304/1–4, quant-ph/0005112.
[39] N. Linden, S. Popescu, B. Schumacher, M. Westmoreland, Reversibility of local transformations of multiparticle entanglement, quant-ph/9912039.
[40] N.D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states, Phys. Rev. Lett. 65 (1990) 1838–1840.
[41] N.D. Mermin, Quantum mysteries revisited, Am. J. Phys. 58 (1990) 731–734.
[42] M.A. Nielsen, J. Kempe. Separable states are more disordered globally than locally, Phys. Rev. Lett. (86) 5184–5187 quant-ph/0011117.
[43] A. Peres, Quantum Theory: Concepts and Methods, Kluwer Academic Publishers, Dordrechet, 1993.
[44] A. Peres, Separability criterion for density matrices, Phys. Rev. Lett. 77 (1996) 1413–1415.
[45] E.M. Rains, A rigorous treatment of distillable entanglement, Phys. Rev. A 60 (1999) 173–178.
[46] R. Raussendorf, H. Briegel, Quantum computing via measurements only, quant-ph/0010033.
[47] B. Reznick, http://www.math.uiuc.edu/Reports/reznick/98-002.html.
[48] J. Schliemann, J.I. Cirac, M. Kuś, M. Lewenstein, D. Loss, Quantum correlations in two-fermion systems, Phys. Rev. A 64 (2001) 022303, quant-ph/0012094.

[49] P.W. Shor, J.A. Smolin, B.M. Terhal, Evidence for Nonadditivity of bipartite distillable entanglement follows from conjecture on bound entangled werner states, Phys. Rev. Lett. 86 (2001) 2681–2684, quant-ph/0010054.
[50] P.W. Shor, J.A. Smolin, A.V. Thapliyal, Superactivation of bound entanglement, quant-ph/0005117.
[51] J.A. Smolin, A four-party unlockable bound-entangled state, Phys. Rev. A 63 (2001) 032306/1–4, quant-ph/0001001.
[52] B.M. Terhal, A family of indecomposable positive linear maps based on entangled quantum states, Linear Algebra and its Appl. 323 (2000) 61–73, quant-ph/9810091.
[53] B.M. Terhal, Bell inequalities and the separability criterion, Phys. Lett. A 271 (2000) 319–326, quant-ph/9911057.
[54] B.M. Terhal, D. DiVincenzo, Problem of equilibration and the computation of correlation functions on a quantum computer, Phys.Rev. A 61 (2000) 22301, quant-ph/9810063.
[55] A. Wehrl, General properties of entropy, Rev. Mod. Phys. 50 (1978) 221–260.
[56] R.F. Werner, Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model, Phys. Rev. A 40 (1989) 4277–4281.
[57] R.F. Werner, M.M. Wolf, Bell's inequalities for states with positive partial transpose, Phys. Rev. A 61 (2000) 062102.
[58] S.L. Woronowicz, Positive maps of low dimensional matrix algebras, Rep. Math. Phys. 10 (1976) 165–183.