Quantum Information and Computation, Vol. 1, No. 1 (2001) 45–75

DISTILLATION AND BOUND ENTANGLEMENT

PAWEŁ HORODECKI*
Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, Poland

RYSZARD HORODECKI †
Institute of Theoretical Physics and Astrophysics, University of Gdańsk, Poland

Received April 24, 2001
Revised May 31, 2001

Quantum entanglement has been known for over sixty years, however the full significance of it as a basic resource in quantum information theory is only being discovered. The fundamental problem is that the decoherence effect due to the environment converts the pure entangled states into a statistical mixture involving some residual noisy entanglement. This leads to an entanglement theory including a scheme of distillation of noisy entanglement within the quantum communication paradigm. This review provides a systematic description of the main (qualitative) results concerning entanglement theory in the context of the so called bound entanglement being a physical manifestation of basic limits for entanglement processing and quantum communication.

Keywords: Distillation, entanglement

1. Introduction

Quantum entanglement has been known since 1935 when EPR [1] and Schrödinger [2] investigated the counterintuitive properties of the quantum systems. The question of expected locality of the entangled quantum systems raised by EPR allowed Bell to discover his famous inequalities serving as a test and demonstration of strange properties of the simplest entangled wave function represented by a singlet state. Still one had to wait long for the proposals of practical applications of quantum entanglement. Nowadays we have such proposals which constitute two main branches of nonclassical information theory: quantum communication and quantum computing. The first comprises quantum cryptography [3], quantum dense coding [4] quantum teleportation [5], which developed into the quantum channels theory. The second is based on quantum algorithms [6] (for review see e. g. [7]) which have been shown to work better than their classical counterparts. The main obstacle against the physical realization of all those highly nonclassical and nontrivial phenomena is their sensitivity against quantum noise. This leads to the development of quantum error correction [8] and fault tolerant computing (see e. g. [7]) on the quantum

*E-mail address: pawel@mif.pg.gda.pl
†E-mail address: fizrh@univ.gda.pl

computing theory. This also lead to invention of *distillation of noisy entanglement* [9] within the quantum communication paradigm. Distillation of quantum entanglement has been introduced basically to allow for quantum teleportation in the presence of noise [9] and soon afterwards it has been applied for quantum privacy amplification [10] in context of a cryptographic scheme with entangled states [3]. So far theoretical development of quantum distillation idea has not been complemented by the experiment due to technical difficulties. However quite recently the first experimental demonstration of single copy distillation has been performed [11] and the experimentally feasible multicopy schemes has been proposed [12].

The aim of this present paper is to present an overview of that part of the quantum information theory which concerns entanglement distillation together with its limits symbolized by so called bound entanglement [13] which is still intensively investigated. The present approach is qualitative. For a quantitative analysis a reader is referred to the Ref.[14]. More extensive treating in the context of various aspect of quantum information theory can be found for instance in Ref. [15].

2. Quantum entanglement

Quantum entanglement is a phenomenon which has no counterpart in classical physics. We say that the wave function describing quantum system is *entangled* iff it cannot be written as a product states of subsystems. The simplest example is [16] the singlet state of two spin-$\frac{1}{2}$ particles

$$\psi_- = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) \,. \tag{1}$$

It can be proved that $\psi_- \neq |\psi\rangle|\phi\rangle$ for any $|\psi\rangle$, $|\phi\rangle$ describing subsystems and $|0\rangle$, ($|1\rangle$) standing for "spin-up" ("spin-down") state. The "nonfactorisability" of any bipartite pure state implies that its reduced density matrices are mixed. The above definition is naturally generalized to the entanglement of multiparticle pure state. The latter (i) represents entanglement iff is not product of n pure states (ii) represents generic m-particle entanglement iff its *any* reduced density matrix is mixed. The well-known example of satisfying not only (i) but also (ii) is represented by the three spin-$\frac{1}{2}$ state $|\psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle - |1\rangle|1\rangle|1\rangle)$ which is called GHZ state [17].

In subsequent section we shall provide a concise review of entanglement theory needed for distillation. In what follows we shall mainly restrict to finite-dimensional case. The case of continuous variables will be described in separate section.

2.1. *Quantum entanglement: bipartite case*

We shall deal with states on product space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Any system described by Hilbert space $\mathcal{H}_{AB}$ we shall call $n \otimes m$ system, where n and m are dimensions of the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively.

Definition 1 .- [18] *Let state ϱ be a density matrix on $\mathcal{H}_A \otimes \mathcal{H}_B$. One calls it separable* *iff it can be written as a convex combination :*

$$\varrho_{AB} = \sum_{i=1}^{k} p_i \varrho_A^i \otimes \varrho_B^i, \quad 0 \le p_i \le 1, \quad \sum_{i=1}^{k} p_i = 1. \tag{2}$$

or can be approximated in trace norm by states of the above form. Otherwise the state is called inseparable or entangled.

All separable states form in the set of states the proper subset $\mathcal{S}$ which is (i) closed (in trace norm) ‡(ii) convex and (iii) closed under so called *separable operations* [19]

$$\Lambda^{sep}(\sigma) = \sum_i A_i \otimes B_i \sigma \otimes A_i^\dagger \otimes B_i^\dagger / Tr(A_i \otimes B_i \sigma \otimes A_i^\dagger \otimes B_i^\dagger), \quad \sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i \le \mathbb{I} \tag{3}$$

Remarks .- Recall that for hermitian operators $Y \le Z$ means that $0 \le Y - X$ i. e. the operator $X \equiv Y - Z$ is positive (see Remarks after Prop. 2, sect. 2.3).

For $dim\mathcal{H} < \infty$ the above definition can be simplified: ϱ is separable iff it can be represented in the form (2) where the states $\{\varrho_A^i, \varrho_B^i\}$ can be taken to be pure and there exist the decomposition with $k \le (dim H_{AB})^2$. In general it is very hard to check separability of given state. If, however, $m \otimes n$ is pure then is separable iff its reduced density matrix is pure. This follows from the Schmidt decomposition

$$|\psi\rangle = \sum_{i=1}^{K} a_i |e_i\rangle |f_i\rangle, \; a_i \le 0, \; a_i \le a_{i+1} \; K = min[dim\mathcal{H}_A, dim\mathcal{H}_B] \tag{4}$$

which is always possible for some orthogonal bases $\{|e_i\rangle\}$, $\{|f_i\rangle\}$. It follows that pure state is separable iff has only one of a_i-s is nonzero i. e. $a_1 = 1$.

Definition 2.- *Bipartite pure state is called maximally entangled iff the reduced density matrices are* $\frac{P}{K}$, $K = min[n, m]$ *with* K*-dimensional projector* P.

Remarks .- Maximal entanglement defined above corresponds to $a_i = \frac{1}{\sqrt{K}}$ for first K coefficients in (4) with other coefficients vanishing. In symmetric $d \otimes d$ case the above holds iff the reduced matrix is maximally mixed. All maximally entangled states are equivalent up to product unitary transformation $U_1 \otimes U_2$ to the state

$$P_+ = |\psi_+\rangle\langle\psi_+|, \quad |\psi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle. \tag{5}$$

Both reduced density matrix of the pure states have the same spectrum and their von Neumann entropy $S(\varrho_A) = S(\varrho_B)$ represents a measure of entanglement of ψ which can be extended to so called entanglement of formation [20].

2.2. *Scalar separability criteria*

The scalar separability criteria are represented as some bounds on values of scalar functions of ϱ. There is natural characterization of separable states in terms of mean values of hermitian operators [21,22]

‡The trace norm is defined as $||A||_{Tr} \equiv Tr|A|$.

Proposition 1.- *The state ϱ is separable iff $Tr(\varrho W) \geq 0$ for all hermitian operators W called entanglement witnesses (EW) such that (i) $Tr(\sigma W) \geq 0$ for all separable σ (ii) there exists some (entangled) ϱ such that $Tr(W\varrho) < 0$.*

Remarks .- Any fixed entanglement witness W provides necessary condition for separability $Tr(W\varrho) \geq 0$. The theory of EW-s has been developed recently [22,24,25,26].

Examples .- The first explicit example of operator with properties (i) and (ii) above was provided in [18]. This was "flip operator" V defined for $d \otimes d$ systems as $V|\phi\rangle|\psi\rangle = |\psi\rangle|\phi\rangle$ for all $\phi, \psi \in \mathcal{C}^d$. It reveals entanglement of ψ_- as $Tr(V|\psi_-\rangle\langle\psi_-|) = -1 < 0$. Another very important physically examples of EW-s come from Bell inequalities [23] (see also [27]). They follow from the general separability condition which is existence of Local Hidden Variable (LHV) Model for general (sequential) local measurements [28] (for the case of single local measurements see the pioneering paper [18]). The possible equivalence of the model to separability is open (see, however,[29]). For details of LHV model and Bell inequalities the reader is referred to Ref. [30].

Another kind of scalar separability conditions are entropic inequalities:

$$S_\alpha(\varrho_{AB}) \leq S_\alpha(\varrho_X), \ X = A, B, \alpha \in \{0\} \cup [1,2] \cup \{\infty\} \tag{6}$$

satisfied for α-entropies or quantum Renyi entropies $S_\alpha(\sigma) = \frac{1}{1-\alpha} \ln[Tr(\varrho^\alpha)]$ with the boundary cases $S_0(\varrho) = -\ln r(\varrho)$ ($r(\varrho)$ is a rank of ϱ), $S_1(\varrho) = -Tr(\varrho \ln \varrho)$, $S_\infty(\varrho) = -ln||\varrho||$ ($||\varrho|| = max$ {eigenvalues of ϱ}). The inequalities (6) for $\alpha = 0$ [31], $\alpha = 1, 2$ [32] and $\alpha = \infty$ ([33,21]) is relatively easy to prove. General proof for $\alpha \in [1,2]$[34] requires operator function properties.

2.3. *Structural separability criteria*

In general structural separability criterion is any separability condition which involves more than scalar function of quantum state. Quantum entanglement theory is linked with the theory of positive maps [36,37,38,35] by the following structural separability criteria [21]:

Proposition 2.- *State ϱ defined on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable iff for all positive linear maps $\Lambda : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A)$ one has*

$$[\mathbb{I} \otimes \Lambda](\varrho) \geq 0 \tag{7}$$

Remarks .- In the above the positivity of Λ means that $\Lambda(X) \geq 0$ for any $X \geq 0$. Recall that one that X is positive (which is denoted by $X \geq 0$) iff $\langle\Psi|X|\Psi\rangle \geq 0$ for any vector Ψ. This is equivalent to the requirement that X is hermitian operator with nonnegative spectrum. There is one-to-one correspondence between dual separability conditions in terms of EW-s (Prop. 1, sect. 2.2) and positive maps (Prop. 2 above). Any EW W defines positive map Λ_W via the isomorphism [36]:

$$W = [\mathbb{I} \otimes \Lambda_W^\dagger](\tilde{P}_+), \quad \tilde{P}_+ = dP_+ \tag{8}$$

where $\Lambda_W^\dagger$ is the map conjugated to Λ_W and P_+ stands for state (5) with $d = dim\mathcal{H}_B$. The following structural criteria are particularly important:

Positive Partial Transposition (PPT) Criterion .- This is first criterion applying positive map in context of separability. Namely we have [39]

Proposition 3.-*If state ϱ is separable then the matrix $T_B(\varrho) \equiv \varrho^{T_B}$ is positive.* Here the *partial transposition map* T_B is defined *via* matrix elements $\langle m|\langle\mu|X|n\rangle|\nu\rangle = X_{m\mu,n\nu}$ in a fixed product basis $\{|n\rangle|\nu\rangle\}$ as follows: $[T_B(X)]_{m\mu,n\nu} \equiv [X^{T_B}]_{m\mu,n\nu} = X_{m\nu,n\mu}$. The positive matrix $X \geq 0$ is called PPT iff $X^{T_B} \geq 0$. The PPT property is independent on the choice of the product basis $\{|n\rangle|\nu\rangle\}$ defining X^{T_B}. For low dimensional the above condition is also sufficient [21]:

Proposition 4.- *For $2\otimes2$ and $2\otimes3$ systems ϱ is separable if and only if ϱ^{T_B} is positive.* Below we shall see that this is *not* however the case in general.

Range criterion .- Basing on analysis from Ref. [37] the necessary separability condition in terms of range $\mathcal{R}(\varrho)$ §of ϱ was formulated [40]:

Proposition 5 .- *If the state ϱ is separable then there exists set of product vectors $|e_i\rangle|f_i\rangle$ such that they span $\mathcal{R}(\varrho)$ and their partial complex conjugates $|e_i\rangle|f_i^*\rangle$ span $\mathcal{R}(\varrho^{T_B})$.*

Remarks .- The above criterion is useless if the matrix has full rank. However, in general it is independent on PPT one: some states violate the above criterion despite satisfying the PPT one. Such counterexamples were first explicitly provided in Ref. [40], though their prototypes existed in mathematical literature much earlier [38] (c.f.[37,35]). The example is a $2\otimes4$ mixture ϱ_b of the projections corresponding to the following vectors (with the corresponding eigenvalues): (i) $\psi_i = \frac{1}{\sqrt{2}}(|0\rangle|i-1\rangle+|1\rangle|i\rangle)$, $i=1,2,3$ ($\lambda_i = \frac{2b}{7b+1}$) (ii) $\psi_4 = |0\rangle|3\rangle$, ($\lambda_4 = \frac{b}{7b+1}$) (iii) $\psi_5 \equiv (\sqrt{\frac{1+b}{2}}|1\rangle|0\rangle + \sqrt{\frac{1-b}{2}}|1\rangle|2\rangle$ ($\lambda_5 = \frac{1}{7b+1}$) where $\{|i\rangle\}$ $0 \leq i \leq m-1$ is standard basis in $\mathcal{C}^n$. Such ϱ_b is PPT but violates the range criterion for the parameter $0 < b < 1$ [40]. There are many examples of PPT entangled states see [41,42,43,44,45]. Among them there are very important ones using the concept of unextendible product base (UPB) [41]. Consider projector P on $\mathcal{C}^3\otimes\mathcal{C}^3$ corresponding to the subspace spanned by set $S_{UPB} \equiv \{|0\rangle(|0\rangle+|1\rangle), (|0\rangle+|1\rangle)|2\rangle, |2\rangle(|1\rangle+|2\rangle)(|1\rangle+|2\rangle)|0\rangle, (|0\rangle-|1\rangle+|2\rangle)(|0\rangle-|1\rangle+|2\rangle)\}$. The latter is called UPB as there is no product vector orthogonal to any element of S_{UPB} [41]. Consequently the state $\varrho_{UPB} = \frac{1}{4}(I-P)$(which turns out to be PPT) violates range criterion for it has no product vector in its range. The state is important in context of irreversibility of entanglement manipulations due to bound entanglement (see sect. 7.1). The systematic way to construct UPB sets and EW detecting the corresponding states ϱ_{UPB} worked out in [42] and [22] respectively provides new tool in context of an open problem of characterization of *undecomposable positive maps* [37]. ¶ In general [24] EW detecting entanglement of PPT state provides via the isomorphism [36] such indecomposable map. Quite recently following [22] the general formalism was developed [24,25] characterizing all EW-s detecting PPT entangled states by some very special class of so called "edge states" [24], (c.f.[46,47,48]). The state δ is "edge" PPT state if it is PPT and violates extremally the range criterion (i. e. there is no $|e\rangle|f\rangle \in \mathcal{R}(\varrho)$ such that $|e\rangle|f^*\rangle \in \mathcal{R}(\varrho^{T_B})$). In particular

§Range of X is defined as $R(X) = \{\psi : \exists\phi, \psi = X\phi\}$. In case of states (which are hermitian) range is equal to support.

¶The map is *decomposable* iff it is of the form $\Lambda_{CP} + T\circ\Lambda'_{CP}$ for some completely positive Λ_{CP}, Λ'_{CP}. The map Λ_{CP} is completely positive iff $\mathbb{I}\otimes\Lambda_{CP}$ is positive (i. e. maps positive matrices into positive ones, see Remarks after the Prop. 2) for identity acting on arbitrary finite dimensional system.

both ϱ_b and ϱ_{UPB} have such edge property. The structure of any PPT entangled state ϱ_{PPT} is as follows [24,25]: $\varrho_{PPT} = (1-p)\varrho_{sep} + p\delta$ for some separable ϱ_{sep}, edge PPT δ and optimal $p > 0$ (i. e. the smallest p allowing for such decomposition, c.f.[48]).

For the following classes PPT property is equivalent to separability:

A. Werner $d \otimes d$ states [18] .- If $P^{(\pm)} = (\mathbb{I} \pm V)/2$ with identity $\mathbb{I}$, and "flip" operation V defined before then the $d \otimes d$ state

$$W(p) = (1-p)\frac{2}{d^2+d}P^{(+)} + p\frac{2}{d^2-d}P^{(-)}, \ 0 \leq p \leq 1 \tag{9}$$

is invariant under any $U \otimes U$ operation for unitary U. $W(p)$ is separable $\Leftrightarrow$ $W(p)$ is PPT $\Leftrightarrow 0 \leq p \leq \frac{1}{2}$.

B. Isotropic states [49] .- The $U \otimes U^*$ invariant (for any unitary U) $d \otimes d$ state

$$\varrho_F = \frac{1-F}{d^2-1}\mathbb{I} + \frac{Fd^2-1}{d^2-1}P_+, \ 0 \leq F \leq 1 \tag{10}$$

(with P_+ defined by (5)) is separable $\Leftrightarrow$ PPT $\Leftrightarrow 0 \leq F \leq \frac{1}{d}$. We have that $F(\varrho_F) = F$ with the general parameter of similarity

$$F(\varrho) \equiv Tr(\varrho P_+). \tag{11}$$

measuring similarity ϱ to P_+. One has $0 \leq F(\varrho) \leq 1$ and $F(\varrho) = 1$ iff $\varrho = P_+$.

C. "Low global rank class" .- One can consider the class [47] of all states which have global rank $r(\varrho_{AB}) \leq max[r(\varrho_A), r(\varrho_B)]$. Here again PPT is equivalent to separability. If $r(\varrho_{AB}) = r(\varrho_A) = r(\varrho_B)$ then PPT property of ϱ_{AB} implies separability [47]. If $r(\varrho_{AB}) < max[r(\varrho_A), r(\varrho_B)]$ (which corresponds to violation of 6 for $\alpha = \infty$) then PPT test is violated, because reduction criterion (see below) is weaker than PPT one [49] but stronger than S_∞ entropy one [31].

Reduction criterion .- Applying the Proposition 2 to the positive map $\Lambda(\sigma) = \mathbb{I}Tr(\sigma) - \sigma$ (with respect to the subsystems A and B) the following criterion was been provided [49,50].

Proposition 6.- *Any separable state ϱ satisfies $\varrho_A \otimes \mathbb{I} - \varrho \geq 0$, $\mathbb{I} \otimes \varrho_B - \varrho \geq 0$.*

Remarks .- The above condition is independent on range criterion as the latter fails for full rank states but is weaker than PPT one [49]. However, as we shall see further, it is important as its violation is *sufficient* condition for distillability of mixed-state entanglement. It also is stronger than all known entropic criteria ([49,31,50,34]).

Finally let us note that there is the structural criterion involving partial order structure [51] which is connected to general effects of state catalysis (for review see [52]).

3. Separability - multiparticle case

The basic notions of separability from sect. 2.1 can be easily generalized. The separability definition becomes m-separability one (see e. g. [53]) after the natural multi-product modification $\sum_{i=1}^k p_i \varrho_1^i \otimes \varrho_2^i \rightarrow \sum_{i=1}^k p_i \varrho_1^i \otimes ... \otimes \varrho_m^i$ in formula (2). In this case ϱ is defined on the m-particle Hilbert space $\mathcal{H} = \bigotimes_{l=1}^{m} \mathcal{H}_l$. Again for finite-dimensional case the product states in the convex combination can be taken to be pure and k can be chosen to be not greater than $dim\mathcal{H}$. Such defined set of m-separable states is (i) convex (ii) closed with respect to trace norm and (iii) invariant under m-separable operations which are immediate generalization of bipartite separable operations $\sum_i A_i^1 \otimes ... \otimes A_i^n \varrho (A_i^1 \otimes ... \otimes A_i^n)^\dagger / Tr(\sum_i A_i^1 \otimes ... \otimes A_i^n \varrho (A_i^1 \otimes ... \otimes A_i^n)^\dagger)$.

The notion of EW generalizes immediately. The characterization in terms of linear maps is formally similar but there is essential difference [54]: the (7) must be satisfied for all linear Λ-s acting from $\mathcal{B}(\mathcal{H}_2 \otimes ...\mathcal{H}_n)$ to $\mathcal{B}(\mathcal{H}_1)$ (still identity $\mathbb{I}$ acts on $\mathcal{B}(\mathcal{H}_1)$) and such that $\Lambda(|e_2\rangle...|e_n\rangle\langle e_2|...\langle e_n|) \geq 0$ for all $m-1$ particle product vectors $|e_2\rangle...|e_n\rangle$. The multiparticle form of isomorphism (8) still holds.

However in comparison to bipartite case there are complications even for pure states. The generalization of Schmidt decomposition (i. e. the form $\sum_i a_i |e_i^1\rangle...|e_i^n\rangle$) is only sometimes possible and those cases were characterized in [55,56]. Among states admitting such decomposition there are states which appear to be maximally entangled. Those are product of unitary transformations $U_1 \otimes ... \otimes U_n$ of generalized m-particle $d \otimes ... \otimes d$ state called GHZ state [17]

$$|GHZ\rangle_d^{(m)} = \frac{1}{\sqrt{d}}(|0\rangle|0\rangle...|0\rangle + |1\rangle|1\rangle...|1\rangle + |d-1\rangle|d-1\rangle...|d-1\rangle) \qquad (12)$$

(we shall omit the indices d, m). The above states represent m-particle entanglement which seems to be maximally entangled [57] and plays important role in multiparticle distillation (see sect. 8). For 3-qubit case detailed investigations showed [58] that apart from $|GHZ\rangle$ there is another state

$$|W\rangle = \frac{1}{\sqrt{3}}(|0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle) \qquad (13)$$

which is important in context of convertibility of multiparticle entanglement with help of local operations and classical communication (see sect. 8).

In the context of multiparticle separability other definitions are possible:

Definition .- *The m-partite ϱ is separable with respect to the partition $\{A_1, ..., A_k\}$ and A_i being disjoint subsets if the set of indices $I = \{1, ..., m\}$ $(\cup_{i=1}^k A_i = I)$ iff $\varrho = \sum_{i=1}^N p_i \varrho_1^i \otimes ... \otimes \varrho_k^i$ where ϱ_l^i is defined on tensor product of all elementary Hilbert spaces corresponding to indices belonging to set A_i. The state is called semiseparable iff it is separable with respect to all 1-to-(m-1) partitions: $A_k = \{k\}$, $A_k^\perp = \{1, ..., k-1, k+1, ..., m\}$, $1 \leq k \leq m$.* Below we shall single out some specific classes:

A. Examples of semiseparable states which are entangled .- The first example [42] was $2\otimes 2\otimes 2$ state generated by UPB set defined as $S_{\mathbf{Shift}} = |0\rangle|0\rangle|0\rangle, |+\rangle|1\rangle|-\rangle, |1\rangle|-\rangle|+\rangle, |-\rangle|+\rangle|1\rangle\}$, (with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$). There is again no 3-separable pure state orthogonal to all elements of S_{UPB} and the construction analogous to bipartite case (sect. 2.3) takes place resulting in curious entangled but semiseparable state $\varrho_{\mathbf{Shift}}$. Another important class is the set of $U\otimes U\otimes U$ invariant $d\otimes d\otimes d$ states which comprises semiseparable and 3-separable cases in one 5-parameter family of states [59]. Quite recently the general characterization of three qubit density matrices has been provided [60].

B. m-qubit family characterized by bipartite splittings.- Note that states $\varrho_{\mathbf{Shift}}$ satisfy PPT condition for all partitions but are still entangled (i. e. are not mixture of products of n states) However we shall recall special m-qubit family [61,62,63] where PPT condition applied to bipartite splittings does characterize all separability properties. Consider the state [61]

$$\varrho^{(m)} = \sum_{a=\pm} \lambda_0^a |\Psi_0^a\rangle\langle\Psi_0^a| + \sum_{k\neq 0} \lambda_k (|\Psi_k^+\rangle\langle\Psi_k^+| + |\Psi_k^-\rangle\langle\Psi_k^-|) \tag{14}$$

where $|\Psi_k^\pm\rangle = \frac{1}{\sqrt{2}}(|k_1\rangle|k_2\rangle...|k_{m-1}\rangle|0\rangle \pm |\overline{k}_1\rangle|\overline{k}_2\rangle...|\overline{k}_{m-1}\rangle|0\rangle$ with $k_i = 0,1$, $\overline{k}_i = k_i \oplus 1 \equiv (k_i+1)mod2$ and k being one of 2^{m-1} real numbers defined by binary sequence $k_1, ..., k_{m-1}$. Let $\Delta = \lambda_0^+ - \lambda_0^- \geq 0$ and let *bipartite splitting* into two disjoint parts $A(k) = \{$ subset with last (m-th) qubit $\}$, $B(k) = \{$ subset without last qubit $\}$ be defined by binary sequence k such that i-th qubit belongs to $A(k)$ (and not to $B(k)$) iff in the sequence $k_1, ..., k_{m-1}$ one has $k_i = 0$. Then (i) $\varrho^{(m)}$ is separable with respect to partition $\{A(k), B(k)\}$ (c.f.Definition 1) $\Leftrightarrow \lambda_k \geq \Delta_k/2 \Leftrightarrow \varrho^{T_B} \geq 0$ (ii) if $\varrho^{T_B} \geq 0$ for all bipartite splittings corresponding to $\mathcal{P}_k$ then $\varrho^{(m)}$ is fully separable. The state is invariant with respect to the random operation Λ_r composed of sequence of the following $n+1$ operations (each performed with probability $\frac{1}{2}$): (i) simultaneous spin flip at all m locations (ii) σ_z applied to both l-th and m-th particle (l runs from 1 to $m-1$ (iii) random phase shift $|0\rangle_i \to e^{i\phi_l}|0\rangle_i$ with $\sum_l \phi_l = 2\pi$.

4. Quantum communication and distant labs paradigm

Quantum teleportation [5] .- Suppose Alice and Bob stay in spatially separated labs and share two particles in maximally entangled state P_+. Then Alice can send Bob the unknown state ϕ of a given particle X_ϕ in the process called *quantum teleportation*, without transfer of any quantum system form Alice to Bob. The teleportation protocol consist of three steps: (i) on two particles (X_ϕ and one member of pair in state P_+) Alice performs jointly the measurement of some observable with maximally entangled eigenvectors. (ii) Alice communicates Bob the outcome of her measurement, (iii) Bob applies unitary operation, depending on the message he got, on his particle (former member of P_+). In the result the final state of Bob's particle is ϕ.

It is very important that if two ancillas X, Y are entangled and instead of X_ϕ Alice has access to, say ancilla X, then, because of linearity of quantum mechanics, she can entangle the other ancilla (Y) with Bob particle. This is achieved just by performing the above protocol with particle X instead of X_ϕ. In such cases one says that Alice teleports to Bob the member Y of entangled pair XY. The teleportation scheme was generalized to shared the pair in arbitrary quantum state instead of P_+ [64] and to arbitrary LOCC operations [65] (see below for definition of LOCC).

The paradigm .- Generally in quantum communication schemes (c.f. quantum cryptography with Bell states [3]) one deals with the paradigmatic situation similar to the above. The observers Alice and Bob are separated in distant labs sharing, (as an fixed input resource) some number of entangled pairs and are allowed to perform local operations (LO) on their particles (with possibly some ancillas) and use classical communication (CC) (to inform each other about their operations, make common decision on next step of the experiment depending on the results obtained so far etc.). Note that Alice and Bob can sometimes decide either to discard (or, mathematically, trace out over subsystem) some portion of the pairs they share. They can also add locally some ancillas which corresponds to embedding the Hilbert space of the system to a new larger one. Note that according to the paradigm the states of the ancillas must be prepared locally which implies that Alice ancillas can not be entangled with those of Bob. Summarizing, in the paradigm the observers are allowed to apply LOCC operations defined above. In particular *no* transfer of quantum system between the labs is allowed.

Probabilistic and deterministic LOCC schemes .- Any LOCC operation defined above is some completely positive (CP) map[‖] Λ_{LOCC} with, in general different domain and codomain. The dimension of LOCC codomain can have a probabilistic nature: starting from the same input Alice and Bob can end up with various finite number of particles depending on results of some intermediate measurements performed in course of LOCC action (called *protocol*). In practical analysis we shall be interested in average results of LOCC actions in the sense that the latter are performed many times on the same input and after that the corresponding mean value is calculated. However it has been proved rigorously [66] that in case of entanglement distillation (which is the subject of this review) one can restrict to so called deterministic protocols. This fact is important for quantitative analysis of distillation process (see [14]).

We shall call the CP map either *quantum operation* if we admit trace decrease, which would corresponds to performing the map only with some probability, or *superoperator* if it preserves the trace. The *distant labs paradigm* with the class of LOCC operations defined above can be extended immediately to multiparticle case (with Alice, Bob, Charlie etc.). It plays a fundamental role in quantum communication theory.

In bipartite case one defines the following classes of quantum operations

C1. LOCC operations with two-way classical communication (2-local operations) .- Here classical communication in both directions (from Alice to Bob and vice versa) is allowed. This class defined above has two subclasses well characterized:

C1a. LOCC operations with zero way classical communication (0-local operations). No classical communication is allowed. The operations must be superoperators as otherwise Bob could operate on member of pair Alice has already discarded. They can be written as $\Lambda_{LOCC}(\varrho) = [\Lambda_A \otimes \Lambda_B](\varrho)$ for some local superoperators Λ_A, Λ_B.

C1b. LOCC with one-way classical communication (1-local operations). Alice can only call to Bob[*] which leads to the form $\Lambda_{LOCC}(\varrho) = \sum_i V_i \otimes I[\mathbb{I} \otimes \Lambda_i](\varrho) V_i^\dagger \otimes \mathbb{I}$ for some tracepreserving Λ_i.

C2. Separable operations .- Those are operations defined before (see sect. 2.1).

C3. PPT operations .- Those are operations [72] Λ such that $T_2 \circ \Lambda \circ T_2$ is completely positive. The simplest example of such operation is $\varrho \to \varrho \otimes \varrho_{PPT}$ i. e. adding some PPT state. Those operations allowed to prove new bounds on entanglement of distillation [68,72,73]. In particular there exists a nice characterization of maximal F obtainable with help of PPT operations [73] (see also [74]).

‖The most general action one can perform in the lab corresponds to some CP map. It is known [67] that is always can be written as $\Lambda_{CP}(\varrho) = \sum_i V_i \varrho V_i^\dagger$.

*It can be defined alternatively if only Bob is allowed to call to Alice.

Remarks .- The above classes are closed under tensor product and composition. There is an order $C1a \subset C1b \subset C1 \subset C2 \subset C3$ with all the inclusions *strict*. In particular there is nontrivial nonequivalence $C1 \neq C2$ [75]. Namely there are separable superoperators (i. e tracepreserving operators) which can not be represented as LOCC ones. However any separable superoperator can be performed with some finite probability [76]. The classes $C1$, $C2$ immediately generalize to multiparticle case resulting in $C1$ class of *m-particle LOCC or (m-local operation)* and $C2$ class of *m-separable operation* with the strict inclusion $C1 \subset C2$. Below we shall provide several important examples of LOCC:

"Twirling" operations .- The random product unitary operations of the form (i) $\sigma \to \int U \otimes U^* \sigma (U \otimes U^*)^\dagger dU$ ($U \otimes U^*$ "twirling") or (ii) $\sigma \to \int U \otimes U \sigma (U \otimes U)^\dagger dU$ ($U \otimes U$ "twirling") are both 1-local superoperators [20]: Alice picks up U randomly, performs it and orders Bob to use U or U^* respectively. By the above transformations any state ϱ_{AB} is transformed to $W(p)$ (case (i)) or $\varrho(p)$ (case (ii)) with operation invariants $p = \frac{2}{d^2-d} Tr(P^{(-)})\sigma$ and $F = Tr(\varrho P_+)$ preserved.

Local filtering operation .- This is a 1-local probabilistic operation [77,84] of the form $\sigma \to V \otimes I \sigma V^\dagger \otimes \mathbb{I} / Tr(V \otimes \mathbb{I} \sigma V^\dagger)$. Alice performs the POVM $\{V_1 = V, V_2 = \sqrt{\mathbb{I} - V^\dagger V}\}$. If the event "one" ($V_1$) occurs she orders to Bob to keep his particle otherwise the decide both to discard their particles. The probability of success amounts to $Tr V^\dagger V \otimes \mathbb{I} \sigma$. If support of V contains range of reduced density matrix σ then the operation is *probabilistically reversible*: with help of new "filter" proportional to pseudoinverse V^{-1} of V Alice can get the initial state σ back.

m-local depolarization of qubits .- The sequence of $n+1$ random operations [61] under which state (14) is invariant form the m-local operation Λ_r. Again any n-qubit state ϱ can be transformed into the form (14) with all parameters λ_i^a being invariants as the corresponding matrix elements of the state in basis $\{|\Psi_k^\pm\rangle\}$.

Entanglement monotones .- There is a class [81] (see [14] for review) of the quantifying entanglement functions of a state which can not (on average) increase under separable superoperators (class $C2$ of sect. 4). They are called entanglement monotones (EM). Among them are fundamental entanglement measures - entanglement cost E_c [78] and distillable entanglement D [20] as well as Schmidt rank (SR) r_S defined for pure states as rank of reduced density matrix (or - equivalently - number of nonzero a_i-s in (4) which does not increase even under general separable superoperators [79]. The same holds for SR generalized to density matrices [80] as $r_S(\varrho) = min(\ max_i[r_S(\psi_i)])$ where minimum is taken over all decompositions $\varrho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. It turns out to be equivalent to one of entanglement monotones of Ref. [81]. It is easy to see that general separable superoperators can not increase it.

Sufficient condition for entanglement .- No m-separable operation can create m-particle entanglement (because of invariance properties of the set of separable states, see previous sections). Thus presence of entanglement after action of separable operation is sufficient condition for existence of entanglement before the action.

5. Towards general distillation scheme - improving entanglement of single copy

We shall consider the possibility of improving entanglement of *single copy* of a state. This includes, among others, the *single-copy distillation* i. e. LOCC conversion (with finite probability) of single copy of the state into the maximally entangled state. The pioneering step was done in Ref. [82] where it was proven that of states $W(p)$ which was shown to satisfy all Bell inequalities become to violate Bell inequality after action of simple LOCC action - bilocal projection of the state onto the four dimensional (isomorphic to $\mathcal{C}^2 \otimes \mathcal{C}^2$) subspace of $\mathcal{C}^d \otimes \mathcal{C}^d$. This effect was called the process of revealing "hidden nonlocality". Next similar single copy effect was reported [77] for mixed $2 \otimes 2$ state *via* filtering method (see previous section).

At the same time the latter was successfully applied for entanglement concentration in case of arbitrary pure states [84] and idea of entanglement distillation [9] involving many copies of given state was invented (see next section).

In the case of single copy of given entangled state one is interested in improving F (11) or its generalization F_{GHZ} for $d^{\otimes n}$ case defined as $F_{GHZ}(\varrho) = \langle GHZ|\varrho|GHZ\rangle)$ making it as close to 1 as possible by means of LOCC operations.

There is a general statement [83,58,65]

Proposition 7 .- *The m-particle state ϱ is LOCC convertible with nonzero probability into state σ iff $\sigma = A_1 \otimes ... \otimes A_m \varrho A_1^\dagger \otimes ... \otimes A_m^\dagger / Tr(A_1 \otimes ... \otimes A_m \varrho A_1^\dagger \otimes ... \otimes A_m^\dagger)$ for some matrices A_i).*

The above Proposition is immediate consequence of the fact that LOCC operation is separable, the fact that $\varrho = \varrho'$ iff $||\varrho - \varrho'|| = 0$ and the convexity of the norm.

Remarks .- The convertibility by means of operation Λ can be denoted by $\varrho \xrightarrow{\Lambda} \sigma$. The operation in Proposition 7 can be called multifiltering operation as it consists of the sequence of local filters defined by $V \otimes \mathbb{I} = A_i \otimes \mathbb{I}$ with operators A_i, $\mathbb{I}$ acting on i-th particle and all other particles respectively. The action is probabilistically reversible if the filtering reversibility condition (see sect. 4) applies to all filters $A_i \otimes \mathbb{I}$.

Pure states .- Any of entangled $n \otimes m$ pure state $\psi = \sum_{i,j} a_{ij} |i\rangle|j\rangle$ of Schmidt rank $r = r_S(\psi)$ (see previous section) can be 1-locally transformed with nonzero probability into $\psi' = \frac{1}{\sqrt{r}} \sum_{i=1}^{r} |i\rangle|i\rangle$ which is maximally entangled state with the same SR. As SR can not be increased this gives maximal output parameter $F_{max} = F(\psi') = r/d$, $d = min[n,m]$. Thus only ψ-s with maximal SR can be 2-locally transformed into maximally entangled state P_+ (5) with $d = min[n,m]$. Here optimal F is achieved by the Procrustean method [84,77] namely the one applying filtering operation $V' \otimes I$ with $V' = \sqrt{X/||X^\dagger X||}$ and $X = A_\psi^{-1}$ being a left pseudoinverse of the $n \times m$ A_ψ matrix with elements $\langle i|A_\psi|j\rangle = \sqrt{d} a_{ij}$. Note that one has

$$|\psi\rangle = A_\psi \otimes \mathbb{I}|\psi_+\rangle. \tag{15}$$

which means that for 2-particle finite-dimensional case any pure state can be produced by LOCC action from only one state ψ_+ which, in that sense, plays the role of" maximal element". Such property does not take place in general multiparticle case: for 3 qubits there are two "generating" (in the above sense) states $|GHZ\rangle$, $|W\rangle$ and neither of them is "maximal" as [58] any other state can be LOCC created only from one of them.

In particular $|GHZ\rangle$, $|W\rangle$ are 3-locally inconvertible to each other [58] and this follows from simple observation that any bipartite reductions of $|GHZ\rangle$ have two product states in their rank while in those of $|W\rangle$ only one product state is contained. Now because of Proposition 7 $|GHZ\rangle \stackrel{LOCC}{\longrightarrow} |W\rangle$ implies $|GHZ\rangle \stackrel{A\otimes B\otimes C}{\longrightarrow} |W\rangle$ for local filtering operations defined by A, B, C matrices which must be nonsingular to preserve three particle entanglement. The corresponding (i) probabilistically convertible and (ii) preserves the number of product states in ranges of reduced density matrices so $|GHZ\rangle \stackrel{LOCC}{\longleftrightarrow} |W\rangle$ is impossible. For optimal conversion of 3-qubit single copy state into $|GHZ\rangle$ see [85].

Mixed states .- Consider mixed $d \otimes d$ states. It is impossible to convert any of them into P_+ with finite probability. Sometimes no separable superoperator can improve F (see [83] for $2 \otimes 2$ Werner states and [86] for more general case). On the other hand, sometimes Alice can improve F even by 0-local (hence tracepreserving) action [87]. There are quite curious examples [65,88] (see also [89]) of state (for instance $pP_+ + (1-p)|0\rangle|1\rangle\langle 1|\langle 0|$ for which it is possible to achieve F arbitrary close to 1 but with the probability $p(F) \to 0$ as $F \to 1$. However this effect called *quasidistillation* always requires two-way classical communication, not tracepreserving operation and singularity of input matrix [90]. Still there are matrices of small rank for which this is impossible (i. e. threshold for F attainable by LOCC operations exists) and the example is [65]

$$\varrho_{FE} = pP_+ + \frac{(1-p)}{3}(|0\rangle|1\rangle\langle 0|\langle 1| + |1\rangle|2\rangle\langle 1|\langle 2| + |2\rangle|0\rangle\langle 2|\langle 0|) \tag{16}$$

For asymmetric case $n \otimes m$, $n \neq m$ sometimes one can even achieve $F = 1$ with probability one [90].

Experimental realisation .- Quite recently an experiment has been performed [11] in which the entanglement of single copy was improved by means of Procrustean method [77,84] and the effect of revealing "hidden nonlocality" according to Ref. [77] was reported. This is remarkable fact as it is the first time when entanglement distillation ideas (though in single copy regime) has been confirmed experimentally.

6. Entanglement distillation - bipartite case

Let Alice and Bob share a large number n of qubit pairs, each in the same mixed noisy state ϱ. Suppose that Alice needs to teleport some number of qubit states to Bob. Then she needs $2 \otimes 2$ maximally entangled states ψ_+ (or any $U_1 \otimes U_2$ transformation of it). There is a process called *entanglement distillation* [20,9]: by means of LOCC operations Alice and Bob can get less $k(n) < n$ pairs which are almost in states ψ_+ (or in singlet states (1), which is equivalent). Maximal rate $k(n)/n$ in the limit of large n under condition of convergence of output pairs to states ψ_+ is called *entanglement of distillation* and denoted by $D(\varrho)$. This is always less than or equal to entanglement cost $E_c(\varrho)$ [78]. The latter (see [14]) is, in a sense, the quantity dual to D. It is defined as minimal asymptotic rate of $k'(n)/n$ where $k'(n)$ is a number of input ψ_+ states needed to prepare n copies of ϱ by means of LOCC operations. Recently it has been shown [78] that $E_c(\varrho) = lim_n E_f(\varrho^{\otimes n})/n$ with *entanglement of formation* $E_f(\varrho) = min \sum_i p_i S(\varrho_A^i)$ where minimum is taken over all possible decompositions $\varrho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and $\varrho_A^i = Tr_B(|\psi_i\rangle\langle\psi_i|)$.

6.1. *Distillation of qubit states*

BBPSSW reccurence protocol .- The following reccurrence protocol [9] is still the most transparent protocol of entanglement distillation. It works for $2 \otimes 2$ states with $F > \frac{1}{2}$. Given $\varrho^{\otimes n}$ Alice and Bob perform $U \otimes U^*$ twirling to get n copies of $2 \otimes 2$ isotropic state ϱ_F still with $F > \frac{1}{2}$. Then on each two pairs XOR operations

$$U_{XOR}|a\rangle|b\rangle = |a\rangle|(b+a) mod 2\rangle \tag{17}$$

are locally performed by Alice and Bob. In (17) first (second) particle is called source (target). During the last process they take as source (target) particles from the first (second) of two pairs. This leads to many copies of four-qubit state symbolized by $\varrho' = (U_{XOR})_{Alice} \otimes (U_{XOR})_{Bob} \varrho_F \otimes \varrho_F (U_{XOR})^{\dagger}_{Alice} \otimes (U_{XOR})_{Bob})^{\dagger}$. Now for each of the four-qubit group observers measure target qubits locally in basis $|0\rangle$, $|1\rangle$ each, discard them and communicate results of the measurements classically. If the results agree they keep the remaining pair formed by source particles and "twirl" it, otherwise discard it too. The process leads to some number of survived pairs with the new fidelity

$$F'(F) = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}. \tag{18}$$

Since the function $F(F')$ is continuous, $F'(F) > F$ for $F > \frac{1}{2}$ and $F'(1) = 1$, iterating the procedure Alice and Bob can obtain state with arbitrarily high F. Of course, the larger F is required the more pairs must be sacrificed, and the less the probability p of the success (going to zero in the limit $F \to 1$). However, if F is high enough to ensure $1 - S > 0$ ($S \equiv S_1(\varrho_F)$ stands here for von Neumann entropy) then there exists a complicated so called hashing protocol [20], that gives asymptotically nonzero distillation rate providing $k = (1-S)n > 0$ maximally entangled pairs from any n pairs of ϱ_F with required $1 - S > 0$. Thus for large numbers state with $F > \frac{1}{2}$ Alice and Bob can start by the recurrence method to obtain $1 - S > 0$, and then apply the hashing protocol providing on average nonzero rate $k/n = \frac{p}{2^l}(1-S) > 0$ where both numbers (i) the probability p of getting $1 - S > 0$, (ii) the number l of bilocal XOR protocol iteration achieving $1 - S > 0$ will depend on initial F. All this means that any state with $F > 1/2$ has nonzero entanglement of distillation and allows to recover maximal entanglement from mixed input states within LOCC paradigm.

Basing on the above result another protocol was invented and applied to Quantum Privacy Amplification (QPA) [10] with analytic proof of convergence [91]. The effectiveness of both protocols (BBPSSW and QPA distillation part) in case of perfect and unperfect Alice and Bob operations was also analyzed showing that the convergence and rate can be significantly improved [93] and that protocols with errors of order 1% are well tolerated [92]. The experimental application is not easy because of difficulty with implementation of XOR gate. However recent attempts in this direction are promising [12].

6.2. *All entangled two-qubit states are distillable*

Below we shall recall the proof that *any* two-qubit entanglement is always distillable [94]. Consider an arbitrary $2 \otimes 2$ entangled state. As PPT criterion is necessary and sufficient for separability there exists $|\psi\rangle$ such that

$$\langle\psi|\varrho^{T_B}|\psi\rangle < 0 \,. \tag{19}$$

Using the identity (15) we rewrite that in the form $Tr[(A_\psi^\dagger \otimes \mathbb{I}\varrho A_\psi \otimes \mathbb{I})^{T_B} P_+] < 0$. Form $Tr A^{T_B} B = Tr A B^{T_B}$ (valid for any A, B and the fact that $P_+^{T_B} = \frac{1}{d}V$ (with "flip" operator V) we obtain $Tr[(A_\psi^\dagger \otimes \mathbb{I}\varrho A_\psi \otimes \mathbb{I}), V] < 0$. This implies that $A_\psi^\dagger \otimes \mathbb{I}\varrho A_\psi \otimes \mathbb{I}$ cannot be equal to null operator and that we have the following state

$$\tilde{\varrho} = \frac{A_\psi^\dagger \otimes \mathbb{I}\varrho A_\psi \otimes \mathbb{I}}{Tr(A_\psi^\dagger \otimes \mathbb{I}\varrho A_\psi \otimes \mathbb{I})} \tag{20}$$

with $Tr(\tilde{\varrho}V) < 0$. Then one has $F(\tilde{\varrho}') > \frac{1}{2}$ for new state $\tilde{\varrho}' = \sigma_y \otimes \mathbb{I}\tilde{\varrho}\sigma_y \otimes \mathbb{I}$ where σ_y is Pauli matrix. Thus by means of sequence of two 1-local filtering operations $A_\psi \otimes \mathbb{I}$, $\sigma_y \otimes \mathbb{I}$ any entangled two qubit state can be transformed with nonzero probability $q = Tr A_\psi \otimes \mathbb{I}\varrho A_\psi^\dagger \otimes \mathbb{I} > 0$ to the state with $F > \frac{1}{2}$. Performing this filtering on each member of supply $\varrho^{\otimes n}$ gives on average nq pairs with $F > \frac{1}{2}$. Combination of this with BBPSSW protocol proves immediately the nonzero distillation rate $k/n = q\frac{p}{2^l}(1-S) > 0$. Hence we have proved the important property [94]

Proposition 8.-*Any entangled two-qubit state is distillable.*

The general 2-qubit distillation protocol [94] recalled above can be also shown to work for any $2 \otimes 3$ entangled state [33] or, in general, for any $2 \otimes n$ state violating PPT criterion [46]. Note that we assumed Alice and Bob know the initial state of the pairs. If they do not know, they still can do the job sacrifying $\sqrt{n}$ of pairs to estimate the state (see [95] for generalization of BBPSSW protocol and [90] for general case).

Example .- The following example [15] illustrates the above scheme. The state $\varrho = \overline{p}|\psi_-\rangle\langle\psi_-| + (1-\overline{p})|0\rangle|0\rangle\langle 00|$ violates PPT criterion (and hence is entangled, see sect. 2.3) iff $\overline{p} > 0$. The negative eigenvalue of ϱ^{T_B} is $\lambda_- = \frac{1}{2}\left(1 - \overline{p} - \sqrt{(1-\overline{p})^2 + \overline{p}^2}\right)$ with the eigenvector $\phi = C(\lambda_-|0\rangle|0\rangle - \frac{\overline{p}}{2}|1\rangle|1\rangle)$ where $C = \frac{1}{\lambda_-^2 + \overline{p}^2/4}$. The corresponding filter $A_\phi = C\mathrm{diag}[\lambda_-, -\frac{\overline{p}}{2}]$ leads to new state

$$\tilde{\varrho} = \frac{1}{N}\begin{bmatrix} \lambda_-^2(1-\overline{p}) & 0 & 0 & 0 \\ 0 & \frac{\overline{p}^3}{8} & \frac{\overline{p}^2}{4}\lambda_- & 0 \\ 0 & \frac{\overline{p}^2}{4}\lambda_- & \frac{\overline{p}}{2}\lambda_-^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{21}$$

where $N = \lambda_-^2(1-\overline{p}) + \overline{p}^2/8 + \lambda_-^2\overline{p}/2$. Now $\langle\psi_-|\tilde{\varrho}|\psi_-\rangle = (\overline{p}^3/8 + \lambda^2\overline{p}/2 - \lambda\overline{p}^2/2)/N$ is greater than $1/2$ if only $\overline{p} > 0$ and then the state $\tilde{\varrho}$ can be successfully subjected to the BBPSSW reccurence protocol (see previous section).

Remarks .- Note that the protocol described in this section is *the only* one which is known to be universal for two qubits i.e. which allows to distill entanglement from any entangled two-qubit state. The whole protocol (including BBPSSW stage) requires two basic ingredients: (i) local filters (ii) XOR gates. Remarkably the first of the latter has been experimentally implemented quite recently [11] while the second has been proven to be available in a probabilistic manner within the current linear optics technology [12]) (in particular see Ref. [76] where general theorems about possibility of probabilistic implementation of any quantum LOCC operation were first provided).

6.3. *Distillation of higher dimensional systems*

There was a natural question: when the given state ϱ is distillable i. e. when maximal entanglement can be distilled from ϱ ? Basing on previous results the necessary and sufficient condition to distill nonzero amount of $2 \otimes 2$ ψ_+ states (or any other $n' \otimes k'$ maximally entangled states, see sect. 7.4) from any $n \otimes m$ state was derived:

Proposition 9.- *A bipartite state ϱ on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ is distillable if and only if for some two-dimensional projectors P, Q and for some number n, the "two-qubit-like"state $\varrho_n'(\varrho) = P \otimes Q \varrho^{\otimes n} P \otimes Q / Tr[P \otimes Q \varrho^{\otimes n} P \otimes Q]$ is entangled.*

Remarks .- (i) It is remarkable fact that state ϱ_n' is effectively two-qubit: it has support in $C^2 \otimes C^2$ subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$ due to character of P, Q. In this sense the distillable entanglement is two-qubit entanglement. (ii) The property "$\varrho_n'(\varrho)$ entangled" is called *n-copy pseudo-distillability of ϱ* [96,97]. It is not known whether one can relax the conditions putting $n = 1$ (or $n \leq n_0$ for some bound n_0 depending on $dim\mathcal{H}_A$,$dim\mathcal{H}_B$) in the above proposition. (iii) One can see that the latter is compatible with the fact [84] that any pure state can be distilled. (iv) From the above it can be seen that the set of $n \otimes m$ distillable states is closed [98].

Distillation and reduction criterion .- We have [49]

Proposition 10 .- *Any state violating reduction criterion is distillable. In particular any entangled isotropic state is distillable.*

This can be shown as follows [49]: without loss of generality we can assume $\langle\psi|\varrho_A \otimes \mathbb{I} - \varrho|\psi\rangle < 0$. Then applying $A_\psi \otimes \mathbb{I}$ (15) one obtains state with $F > \frac{1}{d}$. Now, $U \otimes U^*$ twirling will convert it into isotropic state with the same F. Then both Alice and Bob apply the projector $P = |0\rangle\langle 0| + |1\rangle\langle 1|$ with $|0\rangle$, $|1\rangle$ local basis elements corresponding to the composition of two local filtering operations $P \otimes \mathbb{I}$ and $\mathbb{I} \otimes P$). This converts the state with $F > \frac{1}{d}$ into two-qubit isotropic state with $F > \frac{1}{2}$ which can be distilled by BBPSSW protocol. Applications of generalized XOR gates was presented in [49,99]. There is an interesting application of Proposition 10 to Gaussian states [100] (see sect. 9).

7. Bound entanglement - bipartite case

7.1. *Bound entanglement phenomenon*

One of the basic questions was "are all entangled states distillable ?". Surprisingly the answer is "not". Indeed, one has [13] the following

Proposition 11.- *Entanglement of $n \otimes m$ PPT state cannot be distilled.*

Now, as we know, many PPT entangled states exist (see sect. 2.3) providing explicit examples of nondistillable entanglement.

Proof .- To prove the above result [13] we shall show that the set of PPT states is (i) closed under LOCC operations [13] and (ii) satisfies $F \leq \frac{1}{d}$, $d = min[n,m]$ [101,72]. Then, since $(\varrho^{\otimes n})^{T_B} = (\varrho^{T_B})^{\otimes n}$ [39] we obtain the theorem. Now (i) follows easily from the property $(A \otimes B \varrho C \otimes D)^{T_B} = A \otimes D^T \varrho^{T_B} C \otimes B^T$ valid for any operators A, B, C, D and the fact that any LOCC operation represent some separable operation which is completely positive. To prove (ii) consider a PPT state ϱ of a $d \otimes d$ system. We obtain $F = Tr(\varrho P_+) = Tr(\varrho^{T_B} P_+^{T_B}) = Tr(\varrho^{T_B} \frac{1}{d} V)$ with known hermitian "flip" operator V. Since ϱ is PPT the matrix ϱ^{T_B} is a legitimate state. Then, as V has spectrum ± 1, the upper bound $\frac{1}{d}$ on F easily follows. For general $n \otimes m$ systems the proof easily generalizes. Now for any PPT ϱ the state $\varrho^{\otimes n}$ is PPT [39]. Since any LOCC action keeps the PPT property (see (i)) then application of (ii) for $d = 2$ implies impossibility of obtaining even single $2 \otimes 2$ copy with $F > \frac{1}{2}$ hence PPT state ϱ is not distillable.

Bound entanglement phenomenon .- We know already that there exist entangled states with PPT property. From the above it follows that they contain nondistillable entanglement called *bound entanglement* (BE) [13] which have $D = 0$. Similarly one calls distillable states *free entangled* (FE).

Existence of BE is rather curious phenomenon. Recently, using the range properties of ϱ_{UPB} (see sect. 2.3) it was proved [102] that the entanglement cost $E_c(\varrho_{UPB})$ is strictly positive. This means that in asymptotic preparation of PPT entangled states ϱ_{UPB} the entanglement is *irreversibly lost*: it can not be distilled back because of $D(\varrho_{UPB}) = 0$ (see earlier analysis in [103,104]). The BE has the interesting properties and its existence raised new important questions concerning the possible *nonadditivity of quantum resources* [44], the physical sense of PPT test etc. In particular there is a conjecture [69] that PPT BE states satisfiy all the Bell inequalities and it has already partially confirmed [70,30]. The question of nonadditivity will be discussed subsequently (sects 7.2, 7.3 and 8.3).

7.2. *Activation of bound entanglement and nonadditivity of quantum resources*

Bound entanglement and teleportation .- It can be shown [65] that BE, if used alone is useless for teleportation (this was proved first [105] for special family of PPT states from [40]). To prove that in general [65] suppose, to the contrary, that we could teleport any state with quantum fidelity f (i. e. strictly greater than the classical value [65] $f_{cl} = \frac{2}{d+1}$) . Then it can be checked that teleporting half of maximally entangled state would produce the new state with $F > \frac{1}{d}$. But, because any teleportation scheme is an LOCC operation itself, this means that we would be able 2-locally transform PPT state into the state with $F > \frac{1}{2}$ which is an expected contradiction. Thus BE can not be useful for teleportation *if used alone*. Remarkable that recently it has been shown that BE is also useless for quantum dense coding [71]. Surprisingly, as we shall see below, the bipartite BE can be helpful in teleportation process in a subtle way. (c.f. sect. 8.3 for multiparticle case)

Single copy activation of bipartite bound entanglement .- Consider the state (16) ϱ_{FE}. This state *free entangled* (FE) being single copy pseudodistillable with $P = Q = |0\rangle\langle 0| +$

$|1\rangle\langle 1|$. However we know that there is threshold value $F_0 < 1$ for F obtainable by LOCC. Now the following state [44] $\sigma_\alpha = \frac{2}{7}|\psi_+\rangle\langle\psi_+| + \frac{\alpha}{7}\sigma_+ + \frac{5-\alpha}{7}\sigma_-$ with $\sigma_+ = |0\rangle|1\rangle\langle 0|\langle 1| + |1\rangle|2\rangle\langle 1|\langle 2| + |2\rangle 0\rangle\langle 2|\langle 0|)$, $\sigma_- = V\sigma_+ V$ is PPT entangled hence BE for any $\alpha \in (3,4]$. It can be shown that the protocol similar to BBPSSW with generalized XOR gate [49] results in quasidistillation of ϱ_{FE} i. e. the threshold F_0 vanishes and F arbitrary close to unity can be achieved with finite probability. This effect of vanishing threshold has been called *activation of bound entanglement* in analogy to chemical processes.

The above single copy activation can be useful [44] in so called *conclusive teleportation* i. e. probabilistic teleportation conditioned by the success of some previous operations. It was shown that maximal value F_{max} of (11) determines maximal teleportation fidelity via the state in any (hence conclusive) teleportation according to the formula $f_{max} = \frac{F_{max}d+1}{d+1}$. Thus threshold F_0 implies the unconditional threshold f_0 in teleportation via ϱ_{FE} alone. Now if instead of the latter Alice and Bob have large supply of BE states σ_α, then they can obtain arbitrary good teleportation with nonzero probability which was impossible without the supply.

Nonadditivity of quantum resources and the paradigm of entanglement enchanced operations .- The activation effect above reveals *nonadditivity of quantum resources* within the distant labs paradigm. Indeed single pair in the state ϱ_{FE} does not allow for arbitrary good (conclusive) teleportation. Similarly, the latter is impossible for any supply of BE states which is represented here by $\varrho_\alpha^{\otimes n}$. However, the two resources jointly (represented by joint state $\varrho_{FE} \otimes \varrho_\alpha^{\otimes n}$) do allow to teleport (conclusively) arbitrary well. The activation effect led to the conjectures about asymptotic nonadditivity of quantum resources [44]: it was conjectured that distillable entanglement D as well as capacities of quantum channel are nonadditive. Those possible effects (with some restrictions [42,68]) are strongly related to the existence of so called NPT bound entanglement (see sects 7.3, 10). For multiparticle case such interesting effects of both in single-copy and asymptotic regime have already been proven (sect. 8.3).

Following the activation effect it was suggested [44] that it is interesting to consider new class of operations: LOCC operations with a supply of BE states (LOCC+BE). This is an element of wider paradigm of entanglement enchanced LOCC operations (c.f. [15]). Within this paradigm a beautiful effect of *entanglement catalysis* has been revealed (see [52] for review) displaying again the nonadditivity of quantum resources.

7.3. *Is there NPT bound entanglement?*

All examples of bipartite BE which have been known so far correspond to PPT entanglement. It has turned out to be hard nut to crack to answer the question whether there exist a state which is BE and does not have positive partial transpose (this is called NPT property).

Remark .- In $2 \otimes n$ NPT property is equivalent to distillability so that there are no NPT BE states of $2 \otimes n$ type [97]. It is also known that no rank two BE exists [31] and it can be concluded that if rank three BE exists it must be NPT [47]. In [49] it was pointed out that the following statements are equivalent: (i) Any NPT state is distillable (ii) Any entangled

Werner state (eq. 9) is distillable. This significantly reduces the problem. Recently it has been proved [96,97] that some NPT Werner states are not single copy pseudodistillable. Moreover it has been also shown [96] that the distillability of the states is at least very hard if number of state copies increases and local minimum argument for nondistillability of two copies case has been provided [107]. However there is still no a full proof of existence of NPT BE. The problem corresponds to the following conjecture [96,97]:

Conjecture .- *The Werner states for $p \in (\frac{1}{2}, \frac{3(d-1)}{2(2d-1)})$ (which are entangled and NPT) are not distillable.*

Recently it has been proved [108] that if the above were true it would have a highly nontrivial and far-reaching implications: nonadditivity and nonconvexity of D. Namely it was shown that $D(W(p_*) \otimes \varrho_{\mathbf{Pent}}) > 0$ for some values of p_* from the interval $(\frac{1}{2}, \frac{3(d-1)}{2(2d-1)})$ and BE PPT state denoted by $\varrho_{\mathbf{Pent}}$. Since $D(\varrho_{\mathbf{Pent}}) = 0$ this implies immediately that from the validity of the conjecture $(D(W(p_*)) = 0)$ follows nonadditivity of distillable entanglement D (which was conjectured in ([44])). Similarly it was shown [108] that D would not be convex. The idea of the proof is to take $2n$ copies of biased mixtures of two BE composed states $W(p_*) \otimes |0\rangle\langle 0|$, $\varrho_{\mathbf{Pent}} \otimes |1\rangle\langle 1|$ where the ancilla is on the Alice side. After Alice measurement both Alice and Bob can produce n copies of $\varrho_{\mathbf{Pent}} \otimes W(p_*)$ which concludes the proof. The third important implication of the above Conjecture is nonadditivity of quantum channels capacities (see sect. 10).

Quite recently the result of the paper [108] was significantly extended . Namely following the characterization of the PPT superoperators [73] it was shown [74] that any NPT entanglement can be distilled with help of PPT operations. But this is not conclusive for the conjecture: there are PPT operations which are not LOCC. For instance adding PPT entangled state is not LOCC because no entanglement can be created by means of LOCC operations). For restrictions on distillation with help of PPT operators see [42,68].

7.4. *Reversibility question, entanglement concentration and thermodynamical analogies*

Entanglement concentration and reversibility question .- It has been shown [84] that for bipartite pure states entanglement of distillation equal to entanglement of formation i .e. that $D(|\psi\rangle) = E_f(|\psi\rangle)$. The corresponding distillation protocol called *entanglement concentration* can be done in 0-local way. This means, following the recent result [78] about entanglement cost $E_c = \lim_n \frac{E_f(\varrho^n)}{n}$ that for pure states asymptotic manipulation of pure entanglement is fully reversible i. e. $D = E_c$. Some of mixed states posses such property too. Those are so called mixtures of locally orthogonal pure states[††]The equality $D = E_f$ for such states was pointed out in Ref. [109]. The nontrivial examples of the states can be found in ([110]). Here the reversibility holds because the pure members of the mixture are locally distinguishable and after distinguishing them one can distill them reversibly. For mixed states it has been conjectured for a long time that $D < E_c$ and this property (representing irreversibility of asymptotic entanglement manipulations) has been proven

[††]Two states are locally orthogonal [109] if supports of reduced density matrices on at least one of sides are disjoint.

recently in Ref. [102] as explained before in sect. 7.1 (c.f. sect. 8.3 for multiparticle systems).

In Ref. [110] it was shown that, for a class of ensembles $\{p_i, \varrho_i\}$, in the process of mixing the amount of information lost is no less than the loss of distillable entanglement D, and it was conjectured to hold in general. The loss of information is quantified by average increase of entropy, so the conjecture takes the form

$$\sum_i p_i D(\varrho_i) - D(\varrho) \leq S(\varrho) - \sum_i p_i S(\varrho_i). \tag{22}$$

This will be discussed subsequently in sect. 10.

Thermodynamical analogies .- Possible irreversibility of the entanglement distillation process has been pointed out first in Refs [20,84]. Further the analogy between distillation-formation of pure entangled states and Carnot cycle as well as extensivity of entanglement was pointed out [111]. In particular the counterpart of second principle of thermodynamics has been proposed: "*Entanglement cannot increase under local quantum operations and classical communication*". Detailed analysis of the principle resulted in some (although not complete) analogy between efficiency of distillation and efficiency of Carnot cycle [103].

In Refs [112,109] entanglement-energy analogy has been developed. In particular it was argued that sending of (entangled or not) qubits corresponds to different types of work [109]. The conservation of information in closed quantum systems has been postulated as analogous to the first principle of thermodynamics: *Entanglement of compound system does not change under unitary processes on one of the subsystems* [112].

Recently basing on the analogies between (i) entanglement and energy, as well as (ii) the work and the process of sending qubits it has been shown that the information in bipartite systems satisfying distant labs paradigm is conserved [113].

8. Distillation and bound entanglement in multiparticle case

8.1. *General properties and protocols*

As in bipartite case the aim is to distill nonzero amount k/n of maximally entangled pairs of m-particle states. The role of maximally entangled states appears to be played by $|GHZ\rangle$ state (which has already been particularly well justified for multiqubit case see [57]). In particular it allows to create $d \otimes d$ maximally entangled ψ_+ state between fixed party and any $m-1$ parties with certainty. This is achieved by LOCC action involving sequence of $m-2$ measurements each in basis $\{|0\rangle ..., |d-1\rangle\}$ rotated by Hadamard transform (see e. g. [15]). One has the following [114,61,62,63]):

Observation 1.- *From given m-particle state ϱ it is possible to distill $|GHZ\rangle$ iff it is possible to distill nonzero amount of maximally entangled states P_+ between each of $m-1$ pairs connecting one particle with all $m-1$ ones.*

Here the "if" part of the proof is trivial because of property of $|GHZ\rangle$ mentioned above. The converse follows from the fact that given ψ_+ among any of two parties one can product GHZ state in one location and then distribute its $m-1$ parts among the remaining locations with help of teleportation via the corresponding ψ_+-s (see discussion in sect. 4). The above Observation states that both sets: (i) one member set formed by GHZ state (ii) the set of mentioned $m-1$ parts of ψ_+ are entanglement generating sets (EGS). For qubits it was shown [115] that the role of $|GHZ\rangle$ can play an arbitrary pure state which has mixed reduced density matrices over all partitions (c. f. definitions of multiparticle separability). Note that bipartite entanglement is convertible into $2 \otimes 2$ ψ_+ states (see sect. 7.4) for which hashing method providing nonzero distillation rate exists (see sect. 6.1).

The condition about $m-1$ copies of ψ_+ from the Observation 1 easily implies that the possibility of *distillation* of m-particle entanglement is equivalent to possibility of *probabilistic LOCC creation of the m-particle state arbitrary close to* $|GHZ\rangle$ state (or its equivalence in sense of EGS). In what follows we shall briefly recall some of the multiparticle distillation protocols that have been invented so far. According to discussion above we can focus on the possibility of making $F_{GHZ}(\varrho) = \langle\psi_{GHZ}|\varrho|\psi_{GHZ}\rangle$ arbitrary close to unity with help of LOCC.

In the first [114], applied to the generalization of isotropic state

$$\varrho_x = x|\psi_{GHZ}\rangle\langle\psi_{GHZ}| + (1-x)\frac{\mathbb{I}}{2^n}, \quad 0 \leq x \leq 1, \tag{23}$$

some indirect (via $m-1$ bipartite distillation protocols) and direct (keeping multiparticle entanglement at each step) methods were compared. It turned out that for fixed m the second protocol worked for larger range of parameters.

Analogs of entanglement of distillation and protocols in m-particle case .- As we shall see in sect. 8.2 there is no uniquely defined distillable entanglement in multiparticle case. Subsequently we shall only use the following notions. For the m-particle system in state ϱ the ψ-entanglement of distillation $D^s_\psi(\varrho)$ with respect to the s-particle subsystem $\tilde{A}$ and is called maximal rate of s-particle state ψ which can distilled from the subsystem $\tilde{A}$. If we only know that such system exists then we simply say that $D^s_\psi(\varrho) > 0$. We can also write $D^s_{|GHZ\rangle} \equiv D^s$. The Observation 1 implies that if $D^s(\varrho) = 0$ for all subsystems with $s \geq 2$ then *no* pure entanglement can be distilled which one can denote traditionally by $D(\varrho) = 0$.

From the Observation 1 one also has $D^k > 0 \Rightarrow D^{k'} > 0$ for all $k' \leq k$. But $D^{k'} > 0$ does not imply $D^k > 0$ with $k > k'$. For example 3-qubit state $|\psi_-\rangle_{AB}|0\rangle_C$ has $D^2 > 0$ but $D^3 = 0$ because of separability with respect to the biparticle partition $\{(AB), C\}$ and the fact that LOCC operation can not create entanglement between the subsystems (AB) and C. In Ref. [61] various distillability properties of the states (14) were provided. In particular we have [62]:

Proposition 12 .- *The state (14) has* $D^s > 0$ *with respect to subsystem* $\tilde{A}$ *iff it generates NPT state with respect to any bipartite partition such that the members of subsystem* $\tilde{A}$ *are not at the same side.*

The corresponding distillation protocol is not direct - it relies on amplification of bipartite parameter F for given pair of subsystems from $\tilde{A}$, but works for 3-particle states (23) in larger range of the parameter x then other protocols. Finally, the 3-particle protocol basing on Procrustean method [84] (c.f. [77]) was invented [116] resulting in fast convergence of F_{GHZ} to unity.

8.2. *Asymptotic nonequivalence of pure multiparticle entanglement*

There is a fundamental difference [115,117] on the level of multiparticle pure state entanglement if compared with bipartite case. For the latter *minimal reversible entanglement generating set (MREGS)* [115] consists of one element ψ_+ (or its equivalence 2-qubit state ψ_-). This is because $E_c = D$ which implies that any pure entanglement can be asymptotically reversibly converted into ψ_+ states of $2 \otimes 2$ type. For tripartite case it is not the case. For example the expected asymptotic equivalence $2n|\psi_{GHZ} \sim 3n|\psi_-\rangle$ (with each trio of $|\psi_-\rangle$-s located to connect all three parties) is not the case [117]. For extensive analysis see [115,117]. It should be noted that for nonasymptotic regime we already have two nonequivalent classes of pure states (see sect. 5).

The basic consequence of the fact that MREGS has more then one element is that in general *distillable entanglement can no longer be a number like in bipartite case.* It must be rather a (in general nonuniquely defined) vector [115] constituted by distillation rates $\{D_{\psi_1}, D_{\psi_2}, ...\}$ (c.f. sect. 8.1) of several elements $\{\psi_1, \psi_2, ...\}$ of MRGES.

8.3. *Multiparticle bound entanglement and associated effects*

Semiseparable states .- Immediate example of multiparticle bound entangled (BE) states is $\varrho_{\mathbf{Schift}}$ (see sect. 3) which is semiseparable but not separable [41]. They do not allow for distillation of any pure entanglement. Indeed suppose that it is possible to distill pure entanglement between Alice and Bob $A-B$ (suppose we have three parties Alice, Bob and Charlie) then it would be, in particular, entanglement symbolized by $A-(BC)$ i. e. the one between Alice and two other parties treated as one system. But semiseparability implies separability with respect to the partition $A-(BC)$. Thus no LOCC can create entanglement between A and (BC) which is an expected contradiction. Suppose that it is possible to distill any m-particle pure state entanglement. Then by the very definition we would have violation of PPT criterion with respect to all partial transpositions. This is again impossible because of semiseparability.

Below we shall describe three effects of the nonadditivity of quantum resources due to the existence of bound entanglement in the multiparticle case.

Three qubit asymmetric states and asymptotic activation .- There is another kind of tripartite bound entanglement with the corresponding BE activation effect [61] (c.f. BE activation for single copy case in sect. 7.2). This is due to the state ϱ_{asym} being an example of special 3-qubit state (14) parameters adjusted so that $\varrho_{asym}^{T_A} \geq 0$, $\varrho_{asym}^{T_B} \geq 0$, but $\varrho_{asym}^{T_C}$ is not positive. Let us recall that any m-particle FE can be distilled to the corresponding GHZ state [58]. From that one can show that no pure entanglement can be distilled from ϱ_{asym} unless one admits some kind of interaction between A and B. But the latter can be achieved by using some supply of pure states $|\psi_+\rangle_{AB}|0\rangle_C$. Indeed, then one can teleport part of ϱ_{asym} form B to A (or vice versa) producing $2 \otimes 4$ NPT entanglement between A and C (or B and C) sites. But NPT $2 \otimes N$ state can be easily shown to be distillable [46]. So we can produce $m-1 = 3-1 = 2$ maximally entangled states which is equivalent to distillability of GHZ state (see sect. 8.1).

The above analysis performed in Ref. [61] has provided an example of *asymptotic activation* (c.f. single copy activation in sect. 7.2). To write this more formally we use the notation of sect. 8.1. One has $D(\varrho_{asym}) = 0$ and $D^2(\sigma) > 0$ but $D^3(\sigma) = 0$. However $D^3(\varrho_{asym} \otimes \sigma) > 0$ so 3-particle BE was activated by biparticle FE contained in σ.

Unlockable state and superactivation of BE.- Third interesting example of multiparticle BE entanglement in literature was provided in [118]. Namely there exist "unlockable " 4-qubit state: $\varrho_{unloc} = \frac{1}{4}\sum_{i=1}^{4} |\Phi_i\rangle\langle\Phi_i| \otimes |\Phi_i\rangle\langle\Phi_i|$ where $\{|\Phi_i\rangle\}$ stands for four Bell states $\{\frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle\}$. This state can be shown to be BE [118] but has "unlockability" property - it becomes FE if only join operation for any two out of four qubits is allowed (note that the same property but with respect to distinguished pair of qubits has state ϱ_{asym} discussed above).

Using the state ϱ_{unloc} the following effect called *superactivation of BE* has been discovered in Ref. [119] which reveals strong nonadditivity of entanglement of distillation for multiparticle case. Consider 5-particle state $\varrho^{ABCDE} \equiv \sigma^A \otimes \varrho^{BCDE}_{unloc}$ and all four states obtained form it via cyclic permutation of the systems i. e. ϱ^{EABCD}, ϱ^{DEABC}, ϱ^{CDEAB},ϱ^{BCDEA}. Any of those states is still BE. But it can be shown that from $M^{ABCDE}_{symm} \equiv \varrho^{ABCDE} \otimes \varrho^{EABCD} \otimes \varrho^{DEABC} \otimes \varrho^{CDEAB} \otimes \varrho^{BCDEA}$ maximally entangled state P_+ between any two of the parties can be created. Thus, following the Observation 1 (sect. 8.1) one has $D^5(M^{ABCDE}_{symm}) > 0$. This is most striking violation of additivity as each summand has $D = 0$ but the result of summing provides $D > 0$. This is the reason why this effect was called superactivation. Note that here asymptotic regime (in a sense of number of iterations [44] or number of particles [61]) is unnecessary - any four copies of M^{ABCDE}_{symm} give maximally entangled 5-particle state with probability one.

Quantum information concentrated remotely with help of BE .- This nice effect reported in [120] uses BE of ϱ_{unloc} [118] to concentrate quantum information of one qubit spread over three spatially separated locations. Suppose Alice, Bob and Charlie share 3-particle state $\psi_{ABC}(\phi)$ being an output of quantum cloning machine (see in this context [121]). The initial information about cloned qubit ϕ is delocalised and they can not concentrate it back with help of LOCC. But the situation changes when each of them has in addition one particle of the 4-particle system in state ϱ_{unloc} with remaining fourth particle handed to another party (David). Then by means of simple LOCC action Alice, Bob, Charlie can "concentrate" the state ϕ back remotely at David site.

9. Aspects of separability and distillation for continuous variables

Separability and distillability - concepts.- One has to deal with continuous variables (CV) if the dimension of the Hilbert space is infinite. The CV attracted increasing attention recently. There were many interesting analysis concerning experimental aspects of CV for pure states [122]. We shall focus on quantum properties of mixed states which are closer to distillation domain. It is known that in case of CV there are qualitative changes in comparison with finite dimensional case. For example volume of separable states becomes zero [123]. There is a problem what kind of CV entanglement should be treat as generic in case of mixtures. One possibility [45] is to require that arbitrary finite dimensional density matrix of arbitrary Schmidt rank can be created by means of LOCC from ϱ. This is reasonable requirement as it excludes possibility of the states of type $\tilde{\sigma} = \bigoplus_{n=1}^{\infty} p_n \sigma_n$ with σ_n of fixed Schmidt rank (SR). On the other hand the requirement allow SR of σ_n in $\tilde{\sigma}$ above to be still finite but converging to infinity which can happen only in case of CV being then "generic" in some sense. The stronger definition [124] would impose infinite SR on at least one pure state ψ_{i_0} in *any* decomposition of the state $\varrho = \sum_i |\psi_i\rangle\langle\psi_i|$. Concerning distillability there are two natural possibilities (i) to require [100] possibility of quasidistillation (i.e. distillation in single copy sense) of pure state with arbitrary large finite SR (ii) to require the same for infinite SR. We shall focus on (i) as it was analyzed in present literature. For bipartite states again as in the finite-dimensional case the PPT property is necessary condition for separability and implies nondistillability of the state (see [45]).

Bound entanglement and CV.- There exist some PPT entangled states hence one has bound entanglement in CV case [45]. The following example was built [45] basing on elements of matrices structure from Ref. [38]: consider the pure state $|\psi\rangle = \sum_{n=1}^{\infty} a_n |n\rangle|n\rangle$ with $||\psi||^2 = \sum_{n=1}^{\infty} a_n^2 = q < \infty$, and the family of states $|\psi_{mn}\rangle = c_m a_n |n\rangle|m\rangle + (c_m)^{-1} a_m |m\rangle|n\rangle$ $n = 1, 2, ..., m > n, 0 < c_{n+1} < c_n < 1$. The $\sum_{n=1}^{\infty} \sum_{m>n}^{\infty} ||\psi_{mn}||^2$ can be made finite by setting, for instance, $a_n = a^n$, $c_n = c^n$ for some $0 < a < c < 1$. Then it can be shown [45] that the following state

$$\varrho = \frac{1}{A}(|\psi\rangle\langle\psi| + \sum_{n=1}^{\infty} \sum_{m>n}^{\infty} |\psi_{mn}\rangle\langle\psi_{mn}|), \tag{24}$$

is PPT entangled and hence bound entangled. The state can be, in principle, realized experimentally [45]. More elegant BE states for CV were obtained on the ground on Gaussian states theory (see below). There is a conjecture that the volume of BE states is also zero for CV case [124]. There is also strong evidence that for PPT states either the state or its partial transpose has very small SR (as it holds for finite-dimensional systems) [124].

Gaussian states and separability/distillability problem.- The separability of well defined family of *Gaussian states* was considered. The states describe k distinguishable quantum systems ("modes") defined by infinite-dimensional Hilbert space $L^2(R)$ each. In the case of bipartite so called $n \times m$ systems the first n modes are on Alice side, and the rest m on Bob one. Gaussian states are completely characterized by their characteristic function $\kappa(x) = exp(-\frac{1}{4}x^T \gamma x - i d^T x)$ with $x = (p, q), p, q \in R^{m+n}$,the $2(m+n) \times 2(m+n)$ covariance matrix γ and mean (or displacement) d of the matrix. The displacement d can be make zero by unitary transformations applied to individual modes (those unitaries can be made within current technology). The symplectic matrix $J = J_A \oplus J_B$ with $J_A = \oplus_{i=1}^{m} J_i$, $J_A = \oplus_{i=1}^{n} J_i$, with one mode symplectic matrices $J_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. The necessary and sufficient condition for positivity of state is $\gamma + iJ \geq 0$. PPT condition (with respect to Alice side) is equivalent to $\gamma + i\tilde{J} \geq 0$ with $\tilde{J} = -J_A \oplus J_B$. Several results have been proved recently. One of them is [127]

Proposition 13.- Bipartite Gaussian state with variance γ is separable iff $\gamma \geq \gamma_A \oplus \gamma_B$

for some Gaussian variances γ_A, γ_B of Alice and Bob modes respectively.

This implies the following property (see [126,125] for 1×1 and[127] for general case):

Proposition 14.- *For $1 \times n$ Gaussian states PPT is necessary and sufficient condition of separability.*

It is not true in general: using the Proposition 13 the PPT entangled (hence bound entangled) 2×2 Gaussian was provided [127] defined by the covariance

$$\gamma = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 2 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 4 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 2 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}. \tag{25}$$

which was obtained applying to variances the technique similar to that from [48]. Then Proposition 13 was generalized to 3-partite case and for 3-mode $1 \times 1 \times 1$ Gaussians the separability has been fully including semiseparable states characterized [128]. The distillability properties of Gaussians has been investigated [100] showing, in particular, distillability for any entanglement of $1 \times N$ case and nonexistence NPT BE for general $n \times m$ case. Remarkable that the latter property makes Gaussians similar to $2 \otimes N$ spin systems. For distillability proofs of Gaussians the reduction criterion [49] was used in a form generalized to CV case.

There were interesting distillation schemes for CV states [129,130]. For interesting aspect of other quantum CV states in context of entanglement distillation see Refs. [131,132]. However practical distillation protocol remains in this context still open question.

10. Entanglement distillation and quantum channels theory

Quantum states and quantum channels .- There is a connection between quantum states and quantum channels [133] which was developed in context of distillation and quantum error correcting codes in seminal Ref. [20]. The simplest physical case is just the teleportation via bipartite state ϱ (see sect. 4) as there the shared particles serves just as quantum channel $\mathcal{T}_\varrho$ for sending unknown state ϕ (or entangle Bob with some other ancilla). In general *quantum channel* [20] Λ is a tracepreserving completely positive map (superoperator) with its usual origin in environment. There is the notion of *quantum channel capacity* $Q_C = Q_C(\Lambda)$ [20]. This is the maximal possible rate k/n such that k qubits states (or their equivalents embedded in higher Hilbert space) can be reliably sent to Bob down the new channel $\Lambda^{\otimes n}$ (composed of n copies of the original channel) with help of classical resource C. Here $C = \leftrightarrow, \leftarrow, \rightarrow, \emptyset$ corresponding to two-way, one way forward, one-way backward and zero-way classical communication from Alice to Bob. One of basic results is that $Q_0 = Q_\rightarrow$ [134,20] while any protocol corresponding to Q_0 represents some error correcting code.

The quantity Q_C resembles the entanglement of distillation D in bipartite case. In fact one can immediately classify entanglement of distillation D as D_C. Now if we define isomorphism between subset of bipartite states and quantum channels: $\varrho(\Lambda) = [I \otimes \Lambda](P_+)$ (see [15]). Note that the left reduced density matrix of $\varrho(\Lambda)$ is maximally chaotic. There is a basic inequality [20] $D_C(\varrho(\Lambda)) \leq Q_C(\Lambda)$. Similarly, it $\mathcal{T}_\varrho$ stands for the channel obtained by teleportation *via* ϱ then $Q_C(\mathcal{T}_\varrho) \leq D_C(\varrho)$.

An important example is *quantum depolarizing channel* $\tilde{\Lambda}$ acting on d-level systems: $\varrho \to \tilde{\Lambda}(\varrho) = p\varrho + (1-p)\frac{\mathbb{I}}{d}$. The corresponding state is $\varrho(\tilde{\Lambda}) = \varrho_F$ with $F = [p(d^2-1)+1]/d^2$. For this channel one has [20,65] $\mathcal{T}_{\varrho(\tilde{\Lambda})} = \tilde{\Lambda}$.

Quantum distillation as counterfactual error correction.- In the above context quantum distillation can be interpreted as counterfactual error correction [15]. The original direct error correction [8,20,134] is achieved by coding: the input k qubits of information is encoded into a larger number of n qubits. Such a package is sent via the noisy channel. Now error correction via entanglement distillation works as follows [20]. Suppose we deal with qubit channels (like depolarizing one) then Alice (the sender) instead of the qubits, sends to Bob members of entangled pairs (in state ψ_-), keeping another member of each pair. If the channel is memoryless then, turning any state into mixture, it produces the global state $\varrho^{\otimes n}$. Finally Alice and Bob distill the pairs (with resource C) and after that Alice can teleport quantum states via distilled pairs. This idea was fruitfully applied on the ground of quantum photonic channels [135] and so called quantum repeaters [136] allowing for quantum communication over long distances.

In all the effects the error correction process can be called counterfactual [15] as errors are corrected (in distillation) before the message *via* teleportation is send .

Towards quantum noisy coding theorem - distillation approach .- The above paradigm was applied fruitfully to achieve unified upper bounds on quantum capacities [137] worked earlier in [134] for special case. Namely

$$Q_C \leq I_C \tag{26}$$

where I_C is maximal asymptotic rate of coherent information $I(\varrho) = max[0, S(\varrho_B) - S(\varrho_{AB})]$ obtained *via* optimizing over the process of sending states down $\Lambda^{\otimes n}$ and increasing I with help of resource C. In this context the possibility of following conjecture

$$I(\varrho) \leq D_{\rightarrow}(\varrho) \tag{27}$$

called hashing inequality was considered [137]. If it held then one would have equality in (26) [137]. The quantity $D_{\rightarrow}$ is very difficult to calculate. Quite recently it has been calculated for some special states [72]. It is worth to note that one could change the criterion requiring (27) to hold only for some tensor products $\sigma^{\otimes k}$ defined by arbitrary σ with some k depending on σ. Such modified form would still imply the equality in (26). Another interesting implication following from the above conjecture is that it implies inequality (22) for pure state ensembles i. e. for ϱ_i pure [137].

Binding entanglement channels and NPT BE conjecture.- It was shown [138,42] that any BE state ϱ_{BE} represents some *binding entanglement (BE) channel* i. e. such a channel such that no free entanglement can come out of it, but sometimes it transforms FE into BE instead of destroying it completely. Physically it can be achieved in an elegant way by performing the quantum teleportation of half of maximally entangled system via ϱ_{BE} [42]. Mathematically one can construct another BE channel Λ_{BE} knowing that it is uniquely determined by the following relation [138]:

$$[\mathbb{I} \otimes \Lambda_{BE}](P_+) = \sqrt{\varrho_1^{-1}} \otimes \mathbb{I} \varrho_{BE} \sqrt{\varrho_1^{-1}} \otimes \mathbb{I} \tag{28}$$

where ϱ^{-1} is a pseudoinverse of the partial trace ϱ_1 of the state ϱ_{BE}. Any BE channel has all quantum capacities zero: $Q_{\leftrightarrow} = Q_{\rightarrow} = Q_{\emptyset} = Q_{\leftarrow} = 0$ [138]. Note that applying (28) *mutatis mutandis* one can derive some quantum channel for arbitrary quantum state [15].

Now recall that it was shown (see sect. 7.3) that if NPT BE of some Wener states existed then $D_{\leftrightarrow}$ is nonadditive. This result has an important implication on quantum channels theory: basing on it one can show [90] that the nonadditivity of quantum capacity $Q_{\leftrightarrow}$ (conjectured [44,138]) follows from the conjecture about NPT bound entanglement of some Werner states.

Quantum privacy amplification (QPA).- The idea of distillation was applied to quantum privacy amplification (QPA). Suppose Alice and Bob share entangled pairs and want to produce quantum cryptographic key with help of local measurements like in [3]. In some cases eavesdropper (Eve) could get entangled with the particles getting then some information about the produced key in this way. However subjecting the pairs to a distillation protocol before production of the key leads to disentanglement of Eve ancilla from the Alice and Bob pair. So finally Eve has no access to results of further Alice and Bob actions. This nice effect was further shown to work unconditionally in case of unperfect Alice and Bob operations [139] (c.f.[140]).

Question of existence of bound information .- Recently [141] the classical probability distributions coming from BE states were carefully analyzed from the informational point of view. An interesting question about existence "bound information" with subtle kind of correlations expected was raised.

11. Concluding remarks

Distant labs paradigm with LOCC class of operations allowed to invent new quantum effects like teleportation or quantum cryptography with Bell theorem. However the original effects were based on pure maximal entanglement. The idea of entanglement distillation is a successful method to make the effects possible in the presence of noise: in many cases given noisy entangled states one can distill an amount of maximal entanglement and then proceed with effects. The example of enormous power of entanglement distillation in quantum information theory is unconditional security of QPA cryptographic scheme.

The entanglement which is distillable has (in the case of discrete variable systems) 2-qubit character: any 2-qubit entanglement is distillable and any distillable entanglement of $n \otimes m$ has the 2-qubit form in the well defined sense i. e. *via* possibility of local projection of some number of copies onto 2-qubit entangled state. Moreover for $n \otimes m$ biparticle $n \cdot m > 6$ and for all multiparticle cases there exist nondistillable or bound entanglement. The latter involves a genuine irreversibility in asymptotic manipulations of entanglement. Its existence resulted in conjectures about nonadditivity of entanglement distillation and capacities of quantum channels. Bipartite bound entanglement is useless for teleportation if it is the only resource. However if in addition FE is available BE leads to subtle nonadditivity effect - activation of BE on single copy - which can be applied in case of so called conclusive teleportation. In this way existence BE resulted in nonadditivity of quantum resources in distant labs regime. This have led to the paradigm of entanglement enhanced LOCC operations. Any bound entanglement known so far satisfies PPT separability test. But there is well justified conjecture that NPT bound entanglement exists and it was shown that this would imply expected nonadditivites together with nonconvexity of distillable entanglement.

There is a general significant connection of bipartite entanglement distillation theory and quantum channels theory. In particular distillation can serve as counterfactual error correction. The conjectured hashing inequality concerning one-way entanglement distillation $D_{\rightarrow}$ implies the Shannon formula for capacity of noisy quantum channels. In general in entanglement distillation theory of bipartite systems some natural thermodynamical analogies occur. In particular the process of sending qubits corresponds to work and conservation of information in some bipartite LOCC systems can be shown.

The idea of entanglement distillation can be generalized to the multiparticle case. However there is ambiguity in definition of entanglement distillation which can not be a number in the case of more than two particles. So far the only known way to get nonzero asymptotic rate one it the indirect multiparticle distillation step distilling entanglement bipartite between different parties of m-particle system, followed by distribution of m particle entanglement by teleportation. However the direct multiparticle distillation procedures serving as initial on intermediate steps have been found. The existence of multiparticle bound entanglement allowed for revealing the most striking nonadditivity of quantum resources: asymptotic activation and superactivation. It also allows for remote concentration of quantum information within LOCC paradigm.

Finally it follows under the consideration that within the framework of quantum information theory there are many open problems concerning entanglement distillation and bound entanglement. Some of them are

(i) The NPT bound entanglement problem - it is important because of potential implications on entanglement measures and quantum channels theory. The related problem is to fully characterize the set of BE states;

(ii) The hashing inequality question - if the inequality were true we would have Shannon noisy coding formula. It would also prove the inequality between entanglement of distillation and information losses in the case of pure states ensembles;

(iii) Calculation explicitly D for mixed states. This is a very difficult technical question but important for practical reasons;

(iv) Find relation between entanglement distillation (and, in particular bound entanglement) to nonlocality and Bell inequalities.

There are many questions about distillation of entanglement in CV domain like the need of quantifying entanglement which is distilled. In general finding of practical, efficient distillation scheme in either of CV or discrete systems is one of the fundamental open questions. In particular the further research towards efficient experimental implementation of those parts of an entanglement distillation protocol which involve gates operating on more than one system (like XOR gate) seems to be desirable. In fact the only distillation protocol which is known to be universal for two qubit case involves just (i) XOR gate and (ii) local filtering operation. Both recent experiment implementing local filtering method in single copy distillation and the proposal of feasible implementation of XOR gate with help of linear quantum optics allow to hope for further experimental development of entanglement distillation idea.

The work is supported by European Comission, contract No. IST-1999-11053 (EQUIP) and by Polish Committee for Scientific Research, contract No. 2 P03B 103 16.

1. A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
2. E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935).
3. A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, (1992) 2881.
5. C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
6. P. Shor, *Proc. 35th Annual Aymp. on Foundation of Computer Science* 1994 (Santa Fe, NM: IEEE Computer Society Press),
7. A. Steane, Rep. Prog. Phys. **61**, 117 (1998).
8. P. Shor, Phys. Rev. A, **52**, 2439 (1995); A. Steane, Phys. Rev. Lett. **77**, 793 (1996).
9. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
10. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
11. P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, N. Gisin, Nature **409**, 1014 (2001).
12. J. W. Pan, C. Simon, C. Brukner, A. Zeilinger, Nature **410**, 1067 (2001).
13. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
14. M. Horodecki, "Entanglement measures", present issue.
15. A. Albert, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, *Quantum information: An Introduction to Basic Concepts and Experiments* (Springer, Berlin 2001).
16. D. Bohm, *Quantum theory* (Prentice-Hall, Englewood Cliffs, N. J., 1951).
17. D. M. Greenberger, M. Horne, and A. Zeilinger, *Bell's theorem*, edited by M. Kafatos (Kluwer, Dordrecht,1989), p. 69.
18. R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
19. V. Vedral, M. B. Plenio, M. A. Rippin and P. L. Knight, Phys. Rev. Lett. **78**, (1997) 2275.
20. C. H. Bennett, D. P. Di Vincenzo, J. Smolin and W. K. Wootters, Phys. Rev. A **54**, 3814 (1997).
21. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
22. B. Terhal, Lin. Algebr. Appl. **323**, 61 (2000).
23. B. M. Terhal, Phys. Lett. A **271**, 319 (2000).
24. M. Lewenstein, B. Kraus, J. I. Cirac, P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
25. M. Lewenstein, B. Kraus, P. Horodecki, and J. I. Cirac, **63**, 044304 (2001).
26. A. Sanpera, D. Bruss, M. Lewenstein, quant-ph/0009109.
27. S. M. Barnett and S. J. D. Phoenix, Phys. Lett. A **167**, 233 (1992).
28. S. Teufel, K. Brendl, D. Dürr, S. Goldstein, N. Zanghí, Phys. Rev. A **46**, 1217 (1997).
29. D. Kaszlikowski, P. Gnacinski, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **86**, 3658 (2001).
30. R. Werner, present issue.

31. P. Horodecki, J. Smolin, B. Terhal, A. Thaplyial, Theor. Comp. Sci. (accepted), quant-ph/9910122.
32. R. Horodecki, P. Horodecki and M. Horodecki, Phys. Lett. A **210**, 377 (1996)
33. P. Horodecki, PhD thesis, Politechnika Gdańska, Gdańsk 1999.
34. B. Terhal, quant-ph/0101032.
35. E. Störmer, Acta Math. **110**, 233 (1963), E. Störmer, Proc. Amer. Math. Soc. **86**, 402 (1982).
36. A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
37. S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).
38. M. D. Choi, Proc. Sympos. Pure Math **38**, 583 (1982).
39. A. Peres, Phys. Rev. Lett. **77**, 1413 (1996);
40. P. Horodecki, Phys. Lett. A, **232**, 333 (1997).
41. C. H. Bennett, D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999);
42. D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B. M. Terhal, Commun. Math. Phys. (accepted), quant-ph/9908070,
43. D. Bruß and A. Peres, Phys. Rev. A **61** 30301(R) (2000).
44. P. Horodecki, M. Horodecki and R. Horodecki, Phys. Rev. Lett. **82**, 1046 (1999).
45. P. Horodecki, M. Lewenstein, Phys. Rev. Lett. **85**, 2657 (2000).
46. B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein Phys. Rev. A **61**, 062302 (2000).
47. P. Horodecki, M. Lewenstein, G. Vidal, I. Cirac, Phys. Rev. A **62**, 032310 (2000).
48. M. Lewenstein, A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
49. M. Horodecki, P. Horodecki, Phys. Rev. A **59**, 4026 (1999).
50. N. Cerf, C. Adami, and R. M. Gingrich, Phys. Rev. **60**, 898 (1999).
51. J. K. Nielsen, J. Kempe, quant-ph/0011117.
52. M. A. Nielsen, G. Vidal, present issue.
53. K. Życzkowski, P. Horodecki, A. Sanpera and M. Lewenstein, Phys. Rev. A **58** 833 (1998), K. Życzkowski, Phys. Rev. A **60**, 3496 (1999).
54. M. Horodecki, P. Horodecki, R. Horodecki, Phys. Lett. A, **283**, 1 (2001).
55. A. Peres, Phys. Lett. A **202**, 16 (1995).
56. A. V. Thaplyial, Phys. Rev. A **59**, 3336 (1999).
57. N. Gisin, H. Beschmann-Pasquinuici, Phys. Lett. A, **246**, 1 (1998).
58. W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
59. T. Eggeling and R. F. Werner, Phys. Rev. A, **63**, 042111 (2001).
60. A. Acin, D. Bruß, M. Lewenstein, and A. Sanpera, quant-ph/0103025.
61. W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
62. W. Dür and J. I. Cirac, Phys. Rev. A **61**, 042314 (2000).
63. W. Dür and J. I. Cirec, Phys. Rev. A **62**, 022302 (2000).
64. S. Popescu, Phys. Rev. Lett. **72**, 797 (1994).
65. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).
66. E. Rains, Phys. Rev. A **60**, 173 (1999).
67. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Wiley, New York, 1991).
68. V. Vedral, Phys. Lett. A **262**, 121 (1999).
69. A. Peres, Found. Phys. **29**, 589 (1999).
70. R. F. Werner, M. M. Wolf, Phys. Rev. A **61**, 062102 (2000).
71. C. H. Bennett, M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. M. Terhal, in preparation.
72. E. M. Rains, Phys. Rev. A **60**, 179 (1999), *ibid.* **63**, 019901(E) (2001).
73. E. Rains, quant-ph/0008047.
74. T. Eggeling, G. K. H. Vollbrecht, R. F. Werner, M. M. Wolf, quant-ph/0104095.

75. C. H. Bennett, D. DiVincenzo, Ch. Fuchs, T. Mor, E. Rains, P. Shor, J. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
76. J. I. Cirac, W. Dür, B. Kraus, M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
77. N. Gisin, Phys. Lett. A **210**, 151 (1996).
78. P. Hayden, M. Horodecki and B. Terhal, quant-ph/0008134.
79. H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
80. B. M. Terhal, P. Horodecki, Phys. Rev. A **61**, 040301(R) (2000).
81. G. Vidal, J. Mod. Opt. **47**, 355 (2000).
82. S. Popescu, Phys. Rev. Lett. **74**, 2619 (1995).
83. N. Linden, S. Massar and S. Popescu, Phys. Rev. Lett. **81**, 3279 (1998)
84. C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
85. A. Acin, E. Jané, W. Dür, and G. Vidal, Phys. Rev. Lett. **85**, 4811 (2000).
86. A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).
87. P. Badziąg, M. Horodecki, R. Horodecki and P. Horodecki, Phys. Rev. A **62**, 012311 (2000).
88. T. Mor, P. Horodecki quant-ph/9906039.
89. F. Verstraete, J. Dehaene, B. D. Moor, quant-ph/ 0011111.
90. P. Horodecki, unpublished.
91. C. Machiavello, Phys. Lett. A **246**, 385 (1998).
92. G. Giedke, H. J. Briegel, J. I. Cirac, P. Zoller, Phys. Rev. A **59**, 2641 (1999).
93. T. Opatrny, G. Kurizki, Phys. Rev. A **60**, 167 (2000).
94. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).
95. T. V. Brun, C. M. Caves, R. Schack, Phys. Rev. A **63**, 042309 (2001).
96. D.P. DiVincenzo, P. W. Shor, J. A. Smolin, B. Terhal and A. Thapliyal, Phys. Rev. A, **61** 062312 (2000).
97. D. Dür, J. I. Cirac, M. Lewenstein and D. Bruss, Phys. Rev. A **61**, 062313 (2000).
98. P. Horodecki: presented on Workshop "Alghoritms in Quantum Information Processing", (Chicago, 1999).
99. G. Alber, A. Delgado, N. Gisin, I. Jex quant-ph/0008022; G. Alber, A. Delgado, N. Gisin, I. Jex, quant-ph/0102035.
100. G. Giedke, Lu-Ming Duan, J. I. Cirac, J. I. Zoller, quant-ph/0104072.
101. M. Horodecki: presented on Dagstuhl Seminar *Quantum Algorithms* (Dagstuhl, 1998).
102. G. Vidal and J. I. Cirac, quant-ph/0102037.
103. V. Vedral and M. Plenio, Phys. Rev. A **57**, 1619 (1998).
104. E. Rains, quant-ph/9704042.
105. N. Linden, S. Popescu, Phys. Rev. A **59**, 137 (1999).
106. S. Braunstein, C. M. Caves, R. Jozsa, N. Lindena and S. Popescu, Phys. Rev. Lett. **83**, 1054 (1999).
107. M. Lewenstein, D. Bruß J. I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera and R. Tarrach, J. Mod. Opt. **47**, 2481 (2000).
108. P. W. Shor, J. A. Smolin and B. M. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
109. P. Horodecki, M. Horodecki and R. Horodecki, Acta Phys. Slov. **48**, 141 (1998).
110. J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio and M. Wilkens, Phys. Rev. Lett. **84**, 1611 (2000).
111. S. Popescu and D. Rohlich, Phys. Rev. A, **57**, 1619 (1997).
112. M. Horodecki and R. Horodecki, Phys. Lett. A **244**, 473 (1998).
113. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. A, **63**, 022310 (2001).
114. M. Murao, M. B. Plenio, S. Popescu, V. Vedral and P. L. Knight, Phys. Rev. A **57**, 4075 (1998).
115. C. H. Bennett, S. Popescu, D. Rohlich, J. A. Smolin, A. V. Thaplyial, Phys. Rev. A **63**, 012307 (2000).

116. O. Cohen and T. A. Brun, Phys. Rev. Lett. **84**, 5908 (2000).
117. N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, quant-ph/9912039.
118. J. A. Smolin, Phys. Rev. A **63**, 032306 (2001).
119. P. W. Shor, J. A. Smolin, A. V. Thaplyial, quant-ph/0005117.
120. M. Murao and V. Vedral, Phys. Rev. Lett. **86**, 352 (2001).
121. V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
122. S. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998). A. Furosawa *et al.* Science **282**, 706 (1998).
123. R. Clifton, H. Halvorson, Physical Review A **61**, 012108 (2000).
124. P. Horodecki, M. Lewenstein, quant-ph 0103076.
125. L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
126. R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
127. R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001),
128. G. Giedke, B. Kraus, J. I. Cirac, M. Lewenstein, quant-ph/0103137.
129. T. Opatrny, G. Kurizki, and D.-G. Welsch, Phys. Rev. A, **61**, 032302 (1999)
130. L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. A **62**, 032304 (2000).
131. S. Parker, S. Bose, and M. B. Plenio, Phys. Rev. A **61**, 032305 (2000).
132. B. Reznik, quant-ph/0008006.
133. B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).
134. H. Barnum, E. Knill and M. Nielsen, IEEE T. Inform. Theory **46** 1317 (2000).
135. S. J. van Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).
136. H.- J. Briegel, W. Dür J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
137. M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **82**, 433 (2000).
138. P. Horodecki, M. Horodecki and R. Horodecki, J. Mod. Opt. **47**, 347 (2000).
139. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
140. H. Aschauer, H. J. Briegel, quant-ph/0008051.
141. N. Gisin, S. Wolf, quant-ph/0005042.