Proceedings of the International Conference "Quantum Optics V", Kościelisko, Poland, 2001

On Mixed States Entanglement and Quantum Communication: Aspects of Quantum Channels Theory

P. Horodecki

Faculty of Applied Physics and Mathematics, Technical University of Gdańsk
Narutowicza 11/12, 80-952 Gdańsk, Poland

Basic aspects of quantum communication based on quantum channels theory are reviewed together with suitable examples. The key notion of quantum channel capacity is discussed. The role of mixed states entanglement as a practical tool in quantum channels theory is explained in detail. Application of recent results on non-positive partial transpose bound entanglement conjecture to binding entanglement channels shows that validity of the conjecture for some states implies *nonadditivity* of two-way quantum channel capacity. Some aspects of robustness of entanglement in context of positive maps theory are also discussed.

PACS numbers: 03.67.–a, 03.65.Ca, 03.67.Hk

1. Introduction

Quantum communication is an important part of quantum information theory (see [1] and references therein). There are two basis fields of quantum communication theory. The first develops applications of quantum mechanics to communication of classical bits. This involves in particular very important quantum cryptography area. The importance of these issues is undisputable for practical reasons. The second field involves investigations of how to use quantum mechanics to improve and optimise quantum states transfer. This is "fully" quantum part of quantum communication and we would like to focus on that. It is natural to ask why this part is interesting or important. There are many reasons of more or less practical reasons for that:

— For example it allows to study fascinating quantum effect called quantum teleportation even if we have real physical scenario with presence of noise. This is because of so-called distillation [2] of quantum entanglement. Recently it has been

shown that quantum teleportation not only can be viewed as quantum computing primitive [3] but also allows to overcome well-known linear optics problem in quantum computer theory [4].

— Some versions of quantum cryptography (so-called BB84 scheme [5]) involve explicitly physical transfer of classical information encoded in quantum systems that have to be physically transmitted.

— Other cryptographic methods (Ekert scheme) [6] use quantum states transfer implicitly (so-called shared entanglement that has to be distributed first).

— Quantum computing — intensively investigated since well-known Shor's discovery [7] — turns out to require so-called quantum error correction [8, 9] that can be translated into problem of reliable transmission via quantum channel and in some cases both the description and the solution achieved by entanglement distillation idea are simplified (see [10]).

— One of main tools to treat many issues of quantum communication is distillation of quantum entanglement that allows for nontrivial cryptographic scheme called quantum privacy amplification (QPA) [11].

— If one would like to distribute processing of quantum algorithm among several quantum computers in nontrivial way then it must be done with help of "fully" quantum communication. Otherwise we could not utilise quantum coherence that is absolutely crucial for the algorithm.

All the above is enough to justify an interest in "fully"quantum communication and related topics.

Before discussing quantum communication let us recall fundamental concepts of quantum information theory. There are two basic concepts used in the theory. The first is a unit of quantum information. This is *qubit* or quantum bit — an extension of notion of bit from classical information theory. This is a physical system described by *two-dimensional* Hilbert space or the state of such system. It can be state of elementary spin, two-level atom or photon polarisation state. It has two basic states $|0\rangle$, $|1\rangle$ corresponding to eigenstates of observable corresponding to natural setting of our measuring apparatus. The state $|0\rangle$, $|1\rangle$ can play the same role as "states" of classical bit 0, 1. The fundamental difference is that unlike in classical theory quantum information can be processed qubits that are superpositions

$$|\phi\rangle = a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1. \tag{1}$$

The second basic notion of quantum information theory is *quantum entanglement*. This is the property that can have quantum system AB composed of two elementary subsystems (A and B). Namely, in same cases the whole system is in the pure state while subsystems are not

$$|\Phi_{AB}\rangle \neq |\phi_A\rangle|\phi_B\rangle. \tag{2}$$

An elementary example of such state is the singlet state describing spin degrees of freedom two spin-$\frac{1}{2}$ particles

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \tag{3}$$

Here vector $|0\rangle$ ($|1\rangle$) corresponds to "spin-up" ("spin-down") state of the system.

The state (3) (or any of its transformation by product $\sigma_i \otimes \sigma_j$ of the Pauli matrices acting on elementary spins) serves as a unit of quantum entanglement called e-bit or entanglement bit.

The essence of quantum information theory is that, speaking very roughly, initial quantum (classical) information written in qubits (bits) can be encoded into entanglement, that is counted in e-bits, and processed only in that form. This serves either to *paralelise* the process of computing or to *delocalise* transferred information or both.

The main problem is that we usually have uncontrolled action of environment (like thermal bath) on our system and neither of two basic quantum informational units (1), (3) can survive in pure form. They are turned into mixture called density matrix. The action of environment is modelled by what one calls quantum channel. The question how to encode qubit so that its information is retained in the resulting density matrix is a subject of *quantum error correction theory* which surprisingly can be viewed either as a part of quantum communication or as a part of quantum computer theory ([10], see below). The question whether any entanglement is retained in a given mixed state and, if so, how much of that we have there is a subject of *quantum entanglement theory*. The two above theories (devoted to error correction and entanglement) have been linked within *quantum channels theory* in seminal work [10] where mixed states entanglement was one of central notions.

Werner [12] first pointed out that it makes sense to speak about entanglement in case of mixed states. For systems with corresponding Hilbert spaces of finite dimension the original definition [12] can be simplified as follows (see [13, 14]): Consider the so-called $d_A \otimes d_B$ state ϱ. This is density matrix of bipartite system defined on Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim\mathcal{H}_A = d_A$, $\dim\mathcal{H}_B = d_B$. We say that ϱ is *entangled* (respectively *separable*) if can (cannot) be written in the form

$$\varrho_{AB} = \sum_{i=1}^{k} p_i |\psi_A^i\rangle|\psi_B^i\rangle\langle\psi_A^i|\langle\psi_B^i| \tag{4}$$

for some set of pure states $|\psi_A^i\rangle$, $|\psi_B^i\rangle$ and probabilities p_i.

The state ϱ defined on finite dimensional Hilbert space is called *maximally entangled* if it is pure and has one of its reduced density matrices maximally mixed. In the present paper we shall discuss and apply *qualitative* aspects of mixed states entanglement defined above. Quantitative aspects within so-called entanglement measures theory [14–16] are reviewed in [17].

The notion of mixed states entanglement first considered in context of quantum nonlocality has turned out to be important in context of quantum communication, especially quantum channels capacities.

In this paper we shall focus on some of those quantum channels properties that are connected to density matrices and their entanglement. We shall review some basic notions of the quantum channels theory and show how they are related to quantum mixed states. We shall also review some aspects of mixed states entanglement that are important for quantum channels. We explain simply the idea of distillation of quantum entanglement [2]. Then we shall present bound entanglement (BE) phenomenon [18] and recall non-positive partial transpose (NPT) bound entanglement conjecture [19, 20] having far reaching consequences [21]. We shall apply concept of binding entanglement channels [22, 23] to show that the result of Ref. [21] implies serious direct consequence for quantum communication — nonadditivity of quantum capacities conjectured in [24, 22]. Finally, we shall discuss briefly question of robustness of entanglement in context of positive maps (cf. [25]).

2. Preliminaria — quantum channels and quantum operations

Let us consider density matrix ϱ defined on Hilbert space $\mathcal{H}_A$, $\dim\mathcal{H}_A = d_A$, endowed with standard d_A-element basis $\{|i\rangle\}_{i=0}^{d_A-1}$. The most general physically feasible quantum operation on ϱ is

$$\varrho \to \varrho' \equiv \Lambda(\varrho)/\mathrm{Tr}[\Lambda(\varrho)], \tag{5}$$

where ϱ' is defined on $\mathcal{H}_B$ ($\dim\mathcal{H}_B = d_B$), where Λ is of so-called *completely positive** form

$$\Lambda(\varrho) = \sum_{k=1}^{m} V_k \varrho V_k^\dagger, \tag{6}$$

with operators V_k: $\mathcal{H}_A \to \mathcal{H}_B$ satisfying additional condition

$$C \equiv \sum_{k=1}^{m} V_k^\dagger V_k \leq I_B \tag{7}$$

and I_B is identity matrix. The notation $X \leq Y$ is used for hermitian X, Y operators and it means that for any Ψ one has $\langle\Psi|X|\Psi\rangle \leq \langle\Psi|Y|\Psi\rangle$.

In the above ϱ, ϱ' represents input and output *quantum states* (or density matrices) respectively. They describe different physical systems when $\mathcal{H}_A \neq \mathcal{H}_B$. This happens for instance when we perform partial trace: at the beginning we have

*This is, in a sense, operational definition of completely positive map. Original (equivalent) mathematical definition is: linear map Λ_{CP} on $\mathcal{B}(\mathcal{H})$ (bounded operators) is *completely positive* if for any natural n the new (extended) map $\mathcal{I}_n \otimes \Lambda_{CP}$ defined on $M_n(\mathcal{C}) \otimes \mathcal{B}(\mathcal{H})$ is positive. Here $M_n(\mathcal{C})$ stands for $n \times n$ complex matrices. Let us recall that linear map Θ is positive if for any hermitian A with nonnegative spectrum $\Theta(A)$ has nonnegative spectrum as well.

compound physical system in global state ϱ_{12}, so $\mathcal{H}_A = \mathcal{H}_1 \otimes \mathcal{H}_2$. After performing partial trace the reduced density matrix ϱ_1 (ϱ_2) describes subsystems so one has $\mathcal{H}_B = \mathcal{H}_1$ ($\mathcal{H}_B = \mathcal{H}_2$) after tracing out second (respectively first) subsystem.

The so-called completely positive map Λ (6) is *trace preserving* if for any ϱ one has $\mathrm{Tr}[\Lambda(\varrho)] = 1$. This happens if and only if we have equality in (7) i.e. $C = I_B$. Then denominator in (5) is trivially equal to 1. Trace preserving quantum operation is called *quantum channel* or *quantum operation without postselection* and plays fundamental role in quantum communication theory. If in addition the channel Λ preserves identity $\Lambda(I_A) = I_B$ then we say that it is *bistochastic*.

The map Λ is called *probabilistic quantum operation* or *quantum operation with postselection* if $A < I_B$ in (7). For any ϱ it can be performed in the lab with probability $p = \mathrm{Tr}[\Lambda(\varrho)]$. However, we can add the operator $V_0 \equiv \sqrt{I - A}$ to the set of operators $\{V_k\}_{k=0}^m$ defining Λ and then the new map

$$\Lambda'(\varrho) = \sum_{i=0}^{m} V_i \varrho V_i^\dagger = \Lambda(\varrho) + V_m \varrho V_m^\dagger \tag{8}$$

is trace preserving and serves as implementation of Λ (see Appendix A). Here we discuss special classes of quantum operations.

Von Neumann measurement without postselection. Then $V_i = P_i$ are projections that sum up to identity. Then Λ is trace preserving and has interpretation: we have performed measurement of some quantum observable (hermitian operator) of the form $A = \sum_{i=1}^{l} \lambda_i P_i$ (λ_i real) but we have not read the result. If we read the classical results during the von Neumann measurement of observable A, then we would get some of the results $i = 1, \ldots, m$ with probability $p_i = \mathrm{Tr}[P_i \varrho P_i]$. Only *after* getting i_0-th result we would know that the initial state ϱ had been subjected to the transformation $\varrho \to \varrho'_{i_0} = P_{i_0} \varrho P_{i_0} / \mathrm{Tr}[P_{i_0} \varrho P_{i_0}]$.

Von Neumann measurement with postselection. We can decide that we are only interested in cases when single chosen result i_0 takes place. This generates single operation

$$\varrho \to \varrho'_{i_0} = P_{i_0} \varrho P_{i_0} / \mathrm{Tr}[P_{i_0} \varrho P_{i_0}] \tag{9}$$

that can be performed and probabilistically (with probability $p = P_{i_0} \varrho P_{i_0} / \mathrm{Tr}[P_{i_0} \varrho P_{i_0}]$). We simply "discard" our system unless the result of the previous measurement is "satisfactory" i.e. $i = i_0$. Analogous protocol can be performed with subset J of "satisfactory" results $i \in J$ leading to $\varrho \to \varrho'_J = \sum_{i \in J} P_i \varrho P_i / \mathrm{Tr}[P_i \varrho P_i]$.

Obvious examples of quantum channels are von Neumann measurement without postselection and partial trace. Probabilistic operation is just von Neumann measurement with postselection. Below we present other interesting examples.

Example 1. *Filtering operation* [26, 27]. This is the most simple quantum operation of the form (5) i.e.

$$\Lambda_{\mathrm{filter}}(\varrho) = V_1 \varrho V_1^\dagger / \mathrm{Tr}[V_1 \varrho V_1^\dagger]. \tag{10}$$

This is, in general, probabilistic operation. According to (8) it can be interpreted as one of two outputs of trace preserving operation. The probability that (10) is performed is $p = \mathrm{Tr}(V_1 \varrho V_1^\dagger)$. The special (nonprobabilistic) case of filtering operation is *unitary operation* where V_1 is equal to some unitary matrix U.

Example 2. *Depolarising channel* [10]. The most popular quantum channel modelling the noise in quantum computer is *depolarising channel* mapping states on $\mathcal{H}_A$ onto the states onto the same space

$$\Lambda(\varrho) = pI_A/d_A + (1-p)\varrho. \tag{11}$$

This channel is also *bistochastic*. It does nothing to the state with probability $(1-p)$ and turns it into completely chaotic mixture I_A/d_A with probability p. For qubit case $d_A = 2$ we can reproduce the form (6) with $V_1 = \frac{\sqrt{1+3p}}{2} I$, $V_i = \frac{\sqrt{1-p}}{2}\sigma_{i-1}$, $i = 2, 3, 4$ where σ_k, $k = 1, 2, 3$ are usual Pauli matrices.

Example 3. *Erasure channel* [28]. This is the simple channel

$$\Lambda(\varrho)p|0\rangle\langle 0| + (1-p)\varrho. \tag{12}$$

The channel simulates losses of particles in the process of transfer:[†] when particle is lost we can produce its duplicate but only in some fixed blank state $|0\rangle\langle 0|$ because the state of the lost particle cannot be reconstructed.

3. Quantum channels capacities

3.1. Distant labs paradigm

Let us consider the distant labs paradigm (see [30]) in which two observers Alice and Bob stay in two spatially separated laboratories. Each of them is allowed to perform local operations (LO) on quantum system in the corresponding lab. They are also allowed to communicate classically (CC) exchanging classical bits. All operations allowed in this paradigm are called LOCC operations. In usual LOCC regime these are all operations Alice and Bob are allowed to perform. However, to make the whole game interesting they are given some additional resource. Usually it is one of two:

(i) quantum channel connecting each other,

(ii) shared[‡] quantum entanglement.

Below we shall focus on case (i). Now let us suppose that *apart from* LOCC operations the labs are connected by quantum channel (it could be optical fiber) and they are allowed to exchange quantum particles (for instance photons with given initial polarisation) sending it down the channel.[§]

[†] This interpretation is due to Professor Robert Alicki [29].

[‡] One says that Alice and Bob *share* quantum entanglement or entangled quantum state if there is a bipartite quantum system in an entangled state such that Alice (Bob) has access only to the first (the second) of its subsystems.

[§] Let us note that quantum channel has two meanings here: (a) physical "channel" transmitting physically given particle, (b) quantum trace preserving operation Λ that affects the state of the particle during the transmission.

3.2. Single copy regime and transfer fidelity

Let us suppose that Alice wants to transfer *quantum state* ϕ belonging to *known* Hilbert space $\mathcal{H}_A$ to Bob sending the particle in the state ϕ down the channel Λ connecting two labs. Usually it is impossible to do that reliably — during the transmission the density matrix of *pure state* $|\phi\rangle\langle\phi|$ is transformed into a *mixed state* $\varrho = \Lambda(|\phi\rangle\langle\phi|)$. The corresponding *fidelity* of the transmission

$$f(\phi) = \langle\phi|\varrho|\phi\rangle = \langle\phi|\Lambda(|\phi\rangle\langle\phi|)|\phi\rangle \tag{13}$$

is usually poor. This is always when the channel Λ is *noisy*, i.e. represents action of environment that destroys some part of quantum information. One defines also *average fidelity* [31] $\overline{f} = \int f(\phi)\mathrm{d}M(\phi)$ where we integrate over uniform measure $\mathrm{d}M(\phi)$ on set of all normalised pure states $\phi \in \mathcal{H}$.

Examples: *fidelities in ideal and von Neumann measurement channel.* We can consider *ideal channel* $\varrho \to \mathcal{I}(\varrho) = \varrho$ that does nothing to the state during transmission. This is special case of unitary channel with $U = I_A$. Clearly the transmission is completely faithful as in this case transmission fidelity (13) is equal to unity for any normalised vector $|\phi\rangle$.

On the other hand, let us consider one qubit channel

$$\varrho \to \Lambda(\varrho) = P_{|0\rangle}\varrho P_{|0\rangle} + P_{|1\rangle}\varrho P_{|1\rangle}, \tag{14}$$

which is evidently defined by von Neumann measurement. Here ϱ is one qubit state describing spin-$\frac{1}{2}$ and we use the notation

$$P_\Psi \equiv |\Psi\rangle\langle\Psi|. \tag{15}$$

Let us suppose now that the transmitted state is pure: $\varrho = P_\phi = |\phi\rangle\langle\phi|$ where ϕ is given by (1). The output state is mixed and the corresponding fidelity $f = |a|^4 + |b|^4$ is evidently not ideal unless $|\phi\rangle$ is equal either to $|0\rangle$ or $|1\rangle$. The average fidelity can be calculated to be [31] $\overline{f} = 2/3$.

3.3. Asymptotical regime and quantum capacities

In general one considers the transmission in asymptotical regime. We shall briefly describe the notion of *quantum capacity* introduced in Ref. [10] (for alternative, equivalent definition see [32]).

Let us consider a new (composed) channel $\Lambda^{\otimes n} = \Lambda \otimes \ldots \otimes \Lambda$ composed of n channels Λ. Let us suppose that Alice has arbitrary state Ψ^k of k-qubits (it can be entangled). She can perform some encoding operation D (acting on her k qubits) that gives the new state denoted by $\Lambda_D(|\Psi^k\rangle\langle\Psi^k|)$ and send it down the channel $\Lambda^{\otimes n}$.

In this process action of the global channel is composed of that of decoding operation so the resulting state on Bob side is $[\Lambda^{\otimes n} \circ \Lambda_D](|\Psi^k\rangle\langle\Psi^k|)$. The latter can be subjected to further Bob's decoding operation Λ_E getting finally $\varrho'_n = [\Lambda_E \circ \Lambda \circ \Lambda_D](|\Psi^k\rangle\langle\Psi^k|)$. This can be schematically written as follows:

$$|\Psi^k\rangle\langle\Psi^k| \xrightarrow{\Lambda_D} \Lambda_D(|\Psi^k\rangle\langle\Psi^k|) \xrightarrow{\Lambda^{\otimes n}} [\Lambda^{\otimes n} \circ \Lambda_D](|\Psi^k\rangle\langle\Psi^k|)$$

$$\xrightarrow{\Lambda_E} \varrho'_n = [\Lambda_E \circ \Lambda^{\otimes n} \circ \Lambda_D](|\Psi^k\rangle\langle\Psi^k|). \tag{16}$$

For many channels one can arrange the above process so that the transmission is *asymptotically reliable* in the sense of transmission fidelity (13) i.e. that

$$\min_{\Psi_k} f_n(\Psi_k) \overset{n\to\infty}{\longrightarrow} 1, \quad f_n(\Psi_k) \equiv \langle\Psi^k|\varrho'_n|\Psi^k\rangle$$

for any k-qubit state $|\Psi_k\rangle$. One can maximise the rate k/n in the limit of large n over all possible encoding, decoding operations (Λ_E, Λ_D) and under *classical resource* $C = \rightarrow, \leftarrow, \leftrightarrow, \phi$ that corresponds to sending classical communication (CC, see above) in one of the following regimes:

(i) "one way" — CC restricted to sending bits *only* from one experimentalist to another i.e. either form Alice to Bob ($C = \rightarrow$) or from Bob to Alice ($C = \leftarrow$),

(ii) "two way" — both from Alice to Bob and *vice versa* ($C = \leftrightarrow$),

(iii) "zero way" — no[¶] classical communication between Alice and Bob allowed ($C = \phi$).

Remark 1. *Important observation* [10]. Let us note that instead of being physically connected by n channels forming $\Lambda^{\otimes n}$ Alice and Bob can use *one* channel many times sending many particles one after another. This is why the quantities defined below are viewed as capacities of *single* channel Λ. This translation of the problem from "spatial" to "time" regime was utilised in an interesting way in case of photonic channels [33].

The rate k/n of the process (16) maximised under encoding, decoding and one of the above classical resource C is called *quantum capacity of channel* Λ and denoted by $Q_C(\Lambda)$ with $C = \rightarrow, \leftarrow, \leftrightarrow, \phi$ ([10, 32], for recent results see [34]). It is obvious that $Q_{\leftrightarrow}$ is not smaller than any other of remaining three capacities because they utilise classical resources that are weaker than two-way resource $C = \leftrightarrow$. One of basic results is that $Q_\phi = Q_\rightarrow$ [32, 10] while any protocol corresponding to Q_ϕ represents some so-called quantum error correcting code.

The physical meaning of quantum capacity is the *speed* of reliable quantum information transfer. In other words it says how many times we must use the channel per one qubit of reliably sent quantum information.[‖] This can be expressed as follows:

Using quantum channels n times (for large n) Alice can send reliably $k \sim nQ_C(\Lambda)$ quantum bits to Bob down the channel $\Lambda^{\otimes n}$ with help of classical communication resource C.

[¶]More precisely we allow for *asymptotically vanishing* rate (in the limit of large number of uses of channels n) of classical bits to the number of reliably sent quantum bits.

[‖]Readers familiar with quantum version of first Shannon theorem [35] must notice that here we do not assume any statistics on Alice's signals. They can be interpreted as pure states coming from a source described by maximal entropy. We shall not discuss quantum version of first Shannon theorem here recommending comprehensive review [36].

Remark 2. Typically in quantum communication the operation Λ_E encodes qubits into entangled states in order to *delocalise* transferred quantum information. This hides it from environment that acts *locally* because of tensor product structure of $\Lambda^{\otimes n}$.

Remark 3. There is interpretation [10] of the quantum capacity in sense of "reliably transmitted Hilbert subspace". The global channel transmits states defined on global Hilbert space of $\mathcal{H}_n = \mathcal{H}_A^{\otimes n}$ dimension $(d_A)^n$. The maximal number of qubits transferred reliably can be associated with 2^k-dimensional subspace of $\mathcal{H}_k \subset \mathcal{H}_n$ with $n = \log \dim \mathcal{H}_n$, $k = \log \dim \mathcal{H}_k$.

Fundamental questions. For given quantum channel Λ the very fundamental questions are: (i) is the quantity Q_C nonzero? (ii) what are lower and upper bounds on Q_C? (iii) what is its value? Usually (iii) is extremally hard problem and (ii) becomes important. One of main unsolved problems is *whether Q_C is additive or not*? There is one natural bound: capacity of the channel Λ mapping states in $\mathcal{H}_A$ into states on $\mathcal{H}_B$ cannot be greater than $\log d_B$, $d_B = \dim \mathcal{H}_B$:

$$Q_C(\Lambda) \leq \log_2 d_B. \tag{17}$$

For $d_A = d_B$ this bound is saturated by ideal channel (see Sec. 3.2).

Example 1. *Class with zero capacity*: *separable channels*. There is natural class of quantum channels with capacity zero — those are *separable channels* [37]. These are those channels that have *one rank* operators V_k in decomposition (6). From elementary algebra we know then that $V_k = |\phi_k\rangle\langle\tilde{\phi}_k|$ for vectors $|\phi_k\rangle$, $|\tilde{\phi}_k\rangle$ uniquely defining V_k. There is physically justified interpretation of such channel — namely it is simulated by simple protocol performed by external observer: (i) perform general measurement $\varrho \to \sum_k V_k \varrho V_k^\dagger$ on the system, (ii) read the result, say k_0, (iii) prepare the system in the state $|\phi_{k_0}\rangle$. Step (i) destroys quantum information completely. This is expressed in general property: *separable channels have all capacities Q_C zero*. Surprisingly the statement is not "if and only if": there are so-called binding entanglement channels [22, 23] (see Sec. 6.3) that have $Q_C = 0$ though they are not separable.

Example 2. *Class with maximal capacity*: *unitary channels*. Let us suppose that Alice and Bob are connected by simple unitary channel $\varrho \to \Lambda^U(\varrho) = U\varrho U^\dagger$ where U is unitary operation. For one qubit U can be the Pauli matrix. This channel transforms any qubit state into another qubit state. Fidelity of the transmission without encoding or decoding can be poor. Indeed for two qubit case we put U equal to the Pauli matrix σ_x then if Alice sends either of states $|0\rangle$, $|1\rangle$ the fidelity is even zero. However, on each pair Bob can perform encoding operation $\Lambda'(\cdot) = U^\dagger(\cdot)U$ "cancelling" the action of the channel and then transmission is ideal. This is because operation $U^\dagger$ is an inverse of U. Thus for global channel $\Lambda_U^{\otimes n}$ acting on many copies no encoding operation is needed and decoding operation $\Lambda_D = \Lambda'^{\otimes n}$ is enough to transmit ideally *one* qubit per one usage of channel. This gives all capacities $Q_C(\Lambda)$ equal to unity because of the bound (17) and $d_A = d_B = 2$ here. We must stress again that usually encoding and decoding

operations do not have tensor structure unlike $\Lambda_D = \Lambda'^{\otimes n}$ above. Typically they would *entangle* possible input (respectively output) product states.

4. Quantum states and quantum channels: connections

4.1. Mathematical isomorphism and its physical interpretation

Let us consider bipartite state ϱ defined on Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ and assume that $\varrho_A = I/d_A$ ($d_X = \dim \mathcal{H}_X$, $X = A, B$). The latter means that left reduced density matrix is maximally mixed. There is one to one correspondence between bipartite states with the latter property and quantum channels Λ transforming states on $\mathcal{H}_A$ into states on $\mathcal{H}_B$. This correspondence is given by the formula [10, 35]

$$\varrho = [\mathcal{I} \otimes \Lambda](P_+) \tag{18}$$

with pure state

$$P_+ = |\Psi_+\rangle\langle\Psi_+|, \quad \text{with} \quad |\Psi_+\rangle = \frac{1}{\sqrt{d_A}} \sum_{k=0}^{d_A-1} |k\rangle|k\rangle \tag{19}$$

defined on "symmetric" Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_A$. As in Ref. [38] let us consider the spectral decomposition of the state ϱ:

$$\varrho = \sum_{k=1}^{d_A d_B} p_k |\psi_k\rangle\langle\psi_k|, \tag{20}$$

where $|\psi_k\rangle = \sum_{i=0}^{d_A-1} \sum_{j=0}^{d_B-1} c_{ij}^k |i\rangle|j\rangle$. The operators V_k are defined by their matrix elements $\langle i|V_k|j\rangle = \sqrt{d_A} c_{ij}^k$ and the corresponding map

$$\Lambda(\sigma) = \sum_{k=0}^{d_A d_B - 1} p_k V_k \sigma V_k^\dagger \tag{21}$$

on arbitrary state σ on Hilbert space $\mathcal{H}_A$.

The following physical interpretation of Eq. (18) within distant labs paradigm (Sec. 3.1) was provided in Ref. [35]. Let us suppose that Alice and Bob are connected by channel Λ and suppose that Alice prepares in her lab a pair of quantum systems or "particles" in joint maximally entangled state $|\Psi_+\rangle$ defined on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_A$ (both subsystems have the same degrees of freedom). If she sends *one* of "particles" to Bob down the channel then the final joint state ϱ (18) shared by Alice and Bob contains all information about the channel. Let us note that separable channels (Sec. 3) correspond to separable states while bistochastic channels correspond to states with *both* reduced density matrices of state (18) maximally mixed [39].

Example. The following so-called isotropic state (see [40])

$$\varrho_p = p \frac{I_A \otimes I_A}{d_A^2} + (1-p) P_+ \tag{22}$$

corresponds to depolarising channel (11) via the isomorphism (18).

4.2. Quantum teleportation channel

Here we shall consider the class of quantum channels based on *quantum teleportation* discovery [41] (extended to shared mixed states case in Ref. [31]). Let us suppose that Alice and Bob stay in spatially separated labs and they share bipartite state ϱ defined on the space $\mathcal{H}_A \otimes \mathcal{H}_B$. Let us suppose that Alice has third particle defined also with help of space $\mathcal{H}_{A'}$ in unknown state $|\phi\rangle$. Let us suppose that $\mathcal{H}_A \sim \mathcal{H}_B \sim \mathcal{H}_{A'} = \mathcal{H}$ i.e. for observers all the particles are of the same physical kind (like three d_A-level atoms etc.). There is the following protocol:

(i) Alice performs joint measurement on both her particles (the one in unknown state and the member of pair in state ϱ). The measurement can correspond to *any* observable of nondegenerate spectrum with eigenvectors being maximally entangled pure states, i.e. states that have both reduced density matrices maximally mixed. Let us note that such measurement has d_A^2 outcomes (see example below);

(ii) after the measurement Alice sends the result of her measurement to Bob;

(iii) Bob performs some special operation (depending on Alice's result) on his particle (his member of pair in joint state ϱ).

The above quantum operation can be viewed as *quantum channel* transmitting with some reliability unknown state ϕ to Bob. It has been shown [41] that if two conditions are satisfied: (a) Alice and Bob share initially pure state maximally entangled (it can be $|\Psi_+\rangle$ defined by (3)) in place of ϱ (b) Bob's actions are some specific unitary operations then the transmission of $|\psi\rangle$ is *ideal*. This means that then after protocol consisting of three steps above Bob gets his particle to be just in (still unknown)** state $|\phi\rangle$ despite the fact that *no* quantum system has been sent from Alice to Bob. Moreover, no information about the state ϕ has been gained during the game — neither Bob nor Alice knows anything about it. This surprising phenomenon called quantum teleportation has many unusual applications in quantum information theory. It can be generalised to include more complicated Alice and Bob actions. Then the general bound on teleportation with help of separable states shared is $\overline{f} \leq 2/(d_A + 1)$ [38].

Example. One qubit teleportation [41]. Let us suppose that Alice and Bob are in distant labs each and suppose that they share maximally entangled singlet state $\psi_0 = \psi_- = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$. Let us note that this state belongs to four vector family called *Bell basis* with other three vectors of the form $\psi_1 = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, $\psi_2 = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, $\psi_3 = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$. Let us suppose now that Alice has unknown spin-$\frac{1}{2}$ particle in one qubit state $|\phi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$. The three particles $A'AB$ (two first $A'A$ belonging to Alice, the third B to Bob) are in a pure state $[|\Phi\rangle\langle\Phi|]_{A'AB}$ defined by

**This is related to so-called no-cloning theorem [42, 43] — it can be shown that despite Alice's measurement destroys completely state $|\phi\rangle$ on her side she still cannot learn anything about the state from results of the measurement.

$$|\Phi\rangle_{A'AB} = |\phi\rangle_{A'}|\psi_0\rangle_{AB}. \tag{23}$$

The essence of the teleportation idea lies in the fact that $\varrho_{A'AB}$ can rewrite the whole vector in the form

$$|\Phi\rangle_{A'AB} = |\psi_0\rangle_{A'A}(-\sigma_0|\phi\rangle_B) + |\psi_1\rangle_{A'A}(\sigma_1|\phi\rangle_B)$$

$$+|\psi_2\rangle_{A'A}(\sigma_2|\phi\rangle_B) + |\psi_3\rangle_{A'A}(\sigma_3|\phi\rangle_B) \tag{24}$$

with $\sigma_0 = I$ and Pauli matrices $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, $\sigma_3 = \sigma_z$. Now protocol goes as follows: Alice performs measurement of observable diagonal in Bell basis $|\psi_i\rangle_{A'A}$, $i = 0, 1, 2, 3$ on her particles $A'A$. Let us suppose that she gets result i_0. Then after her measurement the global state corresponds to

$$|\psi_{i_0}\rangle_{A'A}(\sigma_{i_0}|\phi\rangle_B). \tag{25}$$

Let us note that unlike before the experiment Bob's particle is now completely uncorrelated with any of Alice's particles. Then if only Alice calls to Bob and says that she has got i_0 he knows that the joint state of three particles corresponds to (25) and it is enough for him to apply the transformation σ_{i_0} to his particle B to reproduce $|\phi\rangle$ at his site. The latter is justified because one has $\sigma_{i_0}^2 = I$ independently of i_0. The corresponding fidelity is ideal. It can be drastically reduced if in the above protocol instead of maximally entangled state Alice and Bob share mixed state [31].

Summarising, it is important that if Alice and Bob share maximally entangled state the transmission is ideal. If they share mixed state then fidelity of the transmission is usually poor (see [38] for details). To avoid, at least partially, the latter disadvantage the new idea of *entanglement distillation* has been introduced in [2]. We shall describe it subsequently.

4.3. Distillation of quantum entanglement

Let Alice and Bob share a large number n of pairs of state, each in the some *mixed* state ϱ that is weakly entangled. Let us suppose that Alice needs to teleport some number of unknown qubit states to Bob. Then they both need to share two-qubit maximally entangled states like singlets ψ_-. However, they are given only mixed weakly entangled pairs. How to use them? For some states ϱ there is a process called *entanglement distillation* [10, 2]: by means of LOCC operations (Sec. 3.1) Alice and Bob can get k pairs which are almost in states ψ_-. Maximal rate k/n in the limit of large n and under condition of convergence of output pairs to states Ψ_+ is called *entanglement of distillation* and denoted by $D_C(\varrho)$ with C standing again for special classical resource. One says that $D_C(\varrho)$ is amount of entanglement one can distil from the state ϱ.

This nontrivial protocol was originally discovered for two-qubit Werner states [12] equivalent to states (22) with $d_A = 2$ and $p < 2/3$.

It must be stressed that during entanglement distillation *no* physical transmission of quantum particles from Alice to Bob is allowed. They can only use pairs

they share performing local quantum operation (like interactions among particles located in one lab) and send classical bits according to resource C.

In case of two-qubit ϱ the process can be viewed as, in a sense, concentrating entanglement from large number of mixed pairs to smaller number of pure states with additional process of removal of noise represented by mixed character of initial pairs. Entanglement distillation has various interesting aspects — readers are referred to review paper [30].

Summarising, within distant labs paradigm, using LOCC operations (with resource C) and large number n of shared pairs in mixed (but entangled) state ϱ Alice and Bob can achieve approximately $k = nD(\varrho)$ pairs in maximally entangled two-qubit states.

However, for some states ϱ one has $D_C(\varrho) = 0$. Then no entanglement can be distilled and ϱ is called nondistillable. It has been obvious that all separable states (see Introduction) have that property. This is, roughly speaking, because of general physical law saying that *LOCC action cannot create entanglement "at a distance"*. The question was whether there are any entangled states that are nondistillable. A surprising answer will be given in one of next subsections.

Example [27] (cf. [26]). We shall briefly describe the simplest distillation protocol. Let us suppose that Alice and Bob share n two-qubit pairs in state $|\Phi\rangle = \alpha|0\rangle|1\rangle - \beta|1\rangle|0\rangle$ with real parameters $\alpha > \beta > 0, \alpha^2 + \beta^2 = 1$. Then Alice performs local filtering operation (see Sec. 2) with $V_1 = \mathrm{diag}[\beta/\alpha, 1]$. Applying the formula (10) we see that such operation gives singlet state ψ_- with probability $p = 2\beta^2$. Thus given any pair from set of given n ones Alice performs local filtering operation on her particle and calls to Bob informing whether the operation succeeded (this happens with probability p) or not. If it succeeded then they keep the pair, otherwise the pair is discarded. Following binary Bernoulli distribution properties for large n this gives $k = pn = 2\beta^2$ pairs in maximally entangled state ψ_-. Let us note that because only Alice used phone, the communication was one-way. Thus we have got lower bound for one-way distillable entanglement

$$D_{\rightarrow}(P_\Phi) \geq 2\beta^2, \quad P_\Phi = |\Phi\rangle\langle\Phi|. \tag{26}$$

The above bound and the corresponding protocol can be shown to be not optimal. Indeed it can be shown that $D_{\rightarrow}(P_\Phi), D_{\leftarrow}(P_\Phi), D_{\leftrightarrow}(P_\Phi), D_{\phi}(P_\Phi)$ have *the same* value of the von Neumann entropy of partially reduced state $\mathrm{Tr}_B(P_\Phi)$ (see [27]).

5. Applications to quantum channels

It has been realised first in Ref. [10] that entanglement distillation can serve as an important tool for quantum channels theory. The trick was to *combine all three ideas* described above in Secs. 4.1, 4.2, 4.3 as follows. Let us suppose that Alice and Bob are just in the situation from Sec. 3: they are connected by n quantum channels Λ that are noisy, n is large enough and they are allowed to use resource $C = \rightarrow, \leftarrow, \leftrightarrow$. They can proceed as follows: instead of sending qubits

directly (that would be harmful to them) Alice and Bob can *prepare* new channel with help of Λ. Alice can prepare n pairs in maximally entangled state P_+ each. Then she can send "half" of any of them (one after another) down the same channel Λ. According to remark 1 of Sec. 3 the effect is as if we had many channels $\Lambda^{\otimes n}$ and sent one "half" of P_+ down any of them. Thus, as a result, Alice and Bob share n *quantum states* each of the form (18). If the latter is distillable (which can happen quite often) then they can apply the idea of Sec. 4.3 and distil $k = nD(\varrho)$ two-qubit maximally entangled states. Finally, Alice can *teleport* reliably (see Sec. 4.2) to Bob any k unknown qubits.

As a result almost ideal (for large n) transmission of k qubits from Alice to Bob took place. The idea was to turn global noisy channel $\Lambda^{\otimes n}$ into almost ideal *teleportation channel* and use the latter to send qubits. Highly nontrivial aspect of the above procedure can be revealed by some simple analysis showing that here errors that channel would have introduced to transmitted quantum information have been corrected virtually *before* the information was sent. This is interpreted as *counterfactual error correction* (see [1]): we "correct" errors *before* they happen.

Realising that the whole process used only resources allowed to achieve Q_C (that is local operations and classical communication resource C) and that it may be not optimal one gets lower bounds for quantum capacities [10]:

$$D_C \leq Q_C, \qquad C = \rightarrow, \leftrightarrow, \leftarrow \tag{27}$$

and, because of $Q_\phi = Q_\leftarrow$, also $D_\leftarrow \leq Q_\phi$.[††]

Other powerful application of distillation idea to quantum capacities can be found in [34] where results towards quantum version of second Shannon theorem has been provided. In particular nontrivial implications of the following conjecture:

$$D_\rightarrow \geq S(\varrho_B) - S(\varrho) \tag{28}$$

called "hashing inequality" (cf. [2]) have been proved. In the above ϱ_B is Bob reduced density matrix of shared state ϱ and S stands for von Neumann entropy.

6. Surprising phenomena and related issues

6.1. Bound entanglement phenomenon

The very natural question was: which states are distillable? As we mentioned above separable states are not because *no quantum correlations can be created with help of classical phone*. As for nonseparable (entangled) states the expected answer was — they should be all distillable. It even has been indeed shown that:

Any entangled two-qubit (or qubit–qutrit)[‡‡] *state is two-way distillable* [44, 40].

The result required prior research [45, 46] providing efficient criterion deciding whether given state is separable or not. This highly nontrivial problem focusing much attention is outlined in Appendix B. At the moment only few issues are im-

[††] The quantity D_ϕ is exception [34]. We shall not discuss it here.

[‡‡] Qubit–qutrit system is just $2 \otimes 3$ system, see definition of separability in introduction.

portant here. Namely if the state ϱ is separable then it satisfies positive partial transpose (PPT) test [45] i.e. the new matrix ϱ^{T_B} defined by its matrix elements in product basis

$$\langle m|\langle\mu|[\varrho^{T_B}]|n\rangle|\nu\rangle = \langle m|\langle\nu|\varrho|n\rangle|\mu\rangle \tag{29}$$

has nonnegative spectrum which is symbolised by the notation $\varrho^{T_B} \geq 0$. The states that pass the test are called PPT. The states that do not are called NPT, because spectrum of their partially transposed matrix ϱ^{T_B} is not positive. The operation (29) corresponds simply to transposing indices due to second subsystem. It happens that PPT test is necessary and sufficient [46] for separability of two-qubit states but this is not so in general [46, 13]. In other words, there exist entangled states satisfying PPT test. It has been shown that violation of PPT test is necessary for distillability and this leads to so-called bound entanglement (BE) phenomenon [18]. Namely, somewhat surprisingly, *there exist states that are entangled but nondistillable.* For bipartite systems they occur only when dimensions of the Hilbert spaces $d_A = \mathcal{H}_A$, $d_B = \mathcal{H}_B$ satisfy $d_A d_B > 6$. This amazing phenomenon focused much attention recently. It represents qualitative [18] and quantitative irreversibilities [47, 48]. For extensive review see [30]. In the above context distillable entanglement is called *free entanglement.* It happens that some part of entanglement in mixed state is free and the rest is bound [48] though there are mixed states [49] that contain only free entanglement. All those issues lead to important thermodynamical analogies [50, 51, 14, 52].

For completeness let us recall the necessary and sufficient condition for distillability of state ϱ [18]:

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 $\varrho'_n(\varrho) = P \otimes Q\varrho^{\otimes n} P \otimes Q/\mathrm{Tr}[P \otimes Q\varrho^{\otimes n} P \otimes Q]$ is entangled i.e. violates PPT test.

This criterion can be modified to more suitable form (see [19, 20]).

Example 1. For first physical explicit examples see [13]. Here we shall recall the following one based on [53, 54]:

$$\sigma_1 = \frac{1}{21}\begin{bmatrix} 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 4 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \end{bmatrix}, \tag{30}$$

written in standard basis of $3 \otimes 3$ type: $|0\rangle|0\rangle, |0\rangle|1\rangle, |0\rangle|2\rangle, |1\rangle|0\rangle, \ldots$ It is invariant under PPT operation (29) but cannot be written in the form (43) (see example in Appendix B).

Example 2. This example of bound entangled states on $\mathcal{C}^3 \otimes \mathcal{C}^3$ is based on unextendable product bases [55, 23] that are important for positive maps theory [56]:

$$\varrho_{\mathrm{Pent}} = \frac{1}{4}\left[I \otimes I - \sum_{i=0}^{4} |v_i\rangle|v_{h(i)}\rangle\langle v_i|\langle v_{h(i)}|\right], \quad h(i) = 2i \bmod 5, \tag{31}$$

where

$$|v_k\rangle = \frac{2}{\sqrt{5+\sqrt{5}}}\left[\cos\left(\frac{2\pi k}{5}\right)|0\rangle + \sin\left(\frac{2\pi k}{5}\right)|1\rangle + \frac{\sqrt{1+\sqrt{5}}}{2}|2\rangle\right]. \tag{32}$$

Remark 1. *Robustness of entanglement.* The above states are singular so their properties can strongly depend on possible admixtures that are unavoidable when we want to prepare system in a given state experimentally. Therefore the robustness of entanglement and bound entanglement in this context is important (cf. [25]). In Appendix C we perform elementary analysis of error bar admittable if one wants to produce entangled and bound entangled state.

Remark 2. *Nonadditivity conjecture.* Physical effect of activation of bound entanglement [24] suggested the following conjectures [24, 22]:

Both distillable entanglement D_C and quantum capacities Q_C are in general nonadditive (more precisely — superadditive) functions of quantum state.

In case of quantum channels superadditivity would mean that

$$Q_C(\Lambda_1 \otimes \Lambda_2) \stackrel{?}{>} Q_C(\Lambda_1) + Q_C(\Lambda_2). \tag{33}$$

We shall come back to the above conjecture subsequently.

6.2. NPT bound entanglement conjecture and its possible implications

The bound entangled phenomenon leads to interesting effects like activation of bound entanglement [24, 57, 58] or superactivation [59] in multiparticle case. There are still open problems, one of them is NPT bound entanglement conjecture formulated in [19, 20].

To describe it let us repeat that PPT property of any entangled states implies bound entanglement [18]. The converse statement "bound entanglement has PPT property" (shown to hold for $2 \otimes n$ case (see [60])) has been still an open question in general. It was quite natural to expect its validity because of the relation of partial transposition to time reversal [61] which could be compatible with the fact that entanglement distillation is a "counterfactual" error correction ([10, 1], see Sec. 5).

Those issues stimulated investigation of states that do not have PPT property. They are called NPT states (see Sec. 6.1). The problem was translated to

the question: *are all NPT states distillable?* As we mentioned above for cases $2 \otimes 2,\ 2 \otimes 3$ it was true [44, 40], and this was generalised to $2 \otimes n$ [60]. But there are evidences that the statement is not true in general. The problem was reduced by the following result [40]:

The statement "PPT property is equivalent nondistillability"is true if and only if it is true for the Werner states.

The Werner states [12] are $d \otimes d$ states of the form

$$W(p) = (1-p)\frac{2}{d^2+d}P^{(+)} + p\frac{2}{d^2-d}P^{(-)}, \tag{34}$$

where $P^{(\pm)} = \frac{I \pm V}{2}$ with identity I, and V being "flip" operation i.e. $V\phi\otimes\psi = \psi\otimes\phi$ for any vectors $\psi,\ \phi$. In other words $P^{(+)}$ ($P^{(-)}$) corresponds to projection onto the symmetric (antisymmetric) subspace of $\mathcal{C}^d \otimes \mathcal{C}^d$.

Quite recently some of NPT Werner states has been carefully considered [19, 20] and they have been shown to be nondistillable in so-called single copy case. Moreover, it has been also shown [19, 20] 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 [62]. However, to provide a full proof of existence of NPT BE was still an open problem. The corresponding conjecture can be formally written as follows (see [19, 20]):

Conjecture. Werner states (34) with parameter $\frac{1}{2} < p \leq \frac{3(d-1)}{2(2d-1)}$ (which are entangled and NPT) are not distillable.

It has been shown that if the above were true it would have a highly non-trivial and far-reaching implications concerning distillable entanglement measure [21] as well as so-called 2-positive maps [20]. Here we shall recall results concerning distillability [21]:

A. If the conjecture is true then two-way distillable entanglement is non-additive (possible nonadditivity of D_C was first conjectured in [24]). This has been proven [21] to follow from the conjecture by showing that tensor product of BE state ϱ_{Pent} (31) with $W(p_*)$ (for some special parameters $p_* \in [1/2,\ 3(d-1)/2(2d-1)]$ defined in Ref. [21]) produces distillable state. Thus $D_{\leftrightarrow}(\varrho_{\mathrm{Pent}} \otimes W(p_*)) > 0$ which (as $D_{\leftrightarrow}(\varrho_{\mathrm{Pent}}) = 0$) has been pointed out to produce nonadditivity if only $D_{\leftrightarrow}(W(p_*)) = 0$ holds.

B. If the conjecture is true then the distillable entanglement D is not convex. This was again proved in Ref. [21] to be implied by the conjecture. The idea of the proof is to take $2n$ copies of unbiased mixtures of two BE composed states $W(p_*) \otimes |0\rangle\langle 0|,\ \varrho_{\mathrm{Pent}} \otimes |1\rangle\langle 1|$ where pure state "ancilla" is on the Alice side. After Alice's measurement both Alice and Bob can produce n copies of $\varrho_{\mathrm{Pent}} \otimes W(p_*)$ which concludes the proof.

One of the main results of this paper is to add another serious consequence of the conjecture for quantum communication.

6.3. Binding entanglement channels

Here we shall discuss briefly the issue of binding entanglement channels [22, 23]. Namely there are channels such that if pair of entangled states is send down them then the pair is not distillable. However sometimes it contains bound (nondistillable) entanglement. Such channels have been shown to have zero capacity $Q_{\leftrightarrow}$ which implies that any other capacities for resource $C = \leftarrow, \rightarrow, \phi$ are zero too (see Sec. 3). Simple mathematical protocol [22] producing BE channel uses arbitrary bound entangled state ϱ on $\mathcal{H}_A \otimes \mathcal{H}_B$ with left reduced density matrix ϱ_A of full rank. Namely with help of such state one can consider new (also bound entangled) density matrix

$$\varrho' = \frac{1}{d}(\varrho_A^{-1/2} \otimes I_B)\varrho(\varrho_A^{-1/2} \otimes I_B). \tag{35}$$

This state has maximally reduced left density matrix ϱ_A so one can apply isomorphism (18). The resulting channel is just some BE channel. This channel is *not* separable because then the state (35) were separable. Another idea to provide BE channel [23] is just "teleport" one subsystem of system in maximally entangled state with help of shared bound entangled state. This allows to perform action of BE channel physically.

The peculiarity of BE channel lies in the fact that it contradicts some natural intuitions of what nonzero capacity of the channel means. Namely it happens that not only separable channels have capacity zero. This is the reason why BE channels were first candidates [22] to satisfy superadditivity relation (33).

Example. Using the above method we can "read" BE channel from BE state (30) with help of the scheme above utilising (35). We get

$$\Lambda(\cdot) = \frac{6}{21}\mathcal{I}(\cdot) + \frac{1}{7}[\sigma_x^{01}V_{01}(\cdot)V_{01}\sigma_x^{01} + \sigma_x^{02}V_{20}(\cdot)V_{20})\sigma_x^{02} + \sigma_x^{12}V_{12}(\cdot)V_{12})\sigma_x^{12}], \tag{36}$$

where $V_{km} = 2|k\rangle\langle k| + |m\rangle\langle m|$ and Pauli-like matrices are $\sigma_x^{km} = |k\rangle\langle m| + |m\rangle\langle k|$. Thus the above channel is a convex combination of ideal channel $\mathcal{I}$ (with weight $p = 6/21$) and other three operations that sum up to another channel with weight $1 - p = 15/21$.

7. Nonadditivity of channel capacities from some NPT bound entangled states

Here we shall prove the one of the main results of the paper. Let us introduce two channels

$$\Lambda^{(+)}(\cdot) = \frac{1}{d+1}\left[\sum_{k=0}^{d-1} P_{|k\rangle}(\cdot)P_{|k\rangle} + \sum_{k<m} \sigma_x^{(km)}P_{km}(\cdot)P_{km}\sigma_x^{(km)}\right] \tag{37}$$

and

$$\Lambda^{(-)}(\cdot) = \frac{1}{d-1} \sum_{k<m} \sigma_y^{(km)} P_{km}(\cdot) P_{km} \sigma_y^{(km)} \tag{38}$$

with projections $P_{km} \equiv |k\rangle\langle k| + |m\rangle\langle m|$ and Pauli-type matrices $\sigma_x^{(km)} = |k\rangle\langle m| + |m\rangle\langle k|$ and $\sigma_y^{(km)} = \mathrm{i}|k\rangle\langle m| - \mathrm{i}|m\rangle\langle k|$.

Using statements from Sec. 4.1 the above channels can be easily checked to be bistochastic. This is because $[\mathcal{I} \otimes \Lambda^{(\pm)}](P_+) = 2/(d^2 \pm d)P^{(\pm)}$ and the latter has both reduced density matrices maximally mixed.

This allows us to reproduce one parameter bistochastic channels family for the Werner states (34) with help of isomorphism (18) as follows:

$$\Lambda_p = p\Lambda^{(+)} + (1-p)\Lambda^{(-)}. \tag{39}$$

Let us also apply the construction (35), (18) to the PPT BE states ϱ_{PEnt} (31). This gives via the isomorphism (18) BE channel Λ_{PEnt} having all quantum capacities zero. Let us suppose that p_* is the parameter for which nonadditivity of $D_{\leftrightarrow}$ holds (see Sec. 6.2). We have

Observation. If the Werner state $W(p_*)$ is NPT bound entangled then two-way quantum channels capacity Q_C is not additive. In particular, channels Λ_{p_*} and Λ_{PEnt} satisfy superadditivity relation (33).

Below we shall prove the observation. We have

$$Q_C(\Lambda_{\mathrm{PEnt}}) = 0 \tag{40}$$

for any classical resource C. Now let us consider sending the maximally entangled state $P_+ \otimes P_+$ down the *composed* channel $\Lambda_{\mathrm{PEnt}} \otimes \Lambda_{p_*}$ with p_* defined as in Ref. [21] (see Sec. 6.2). This leads to the composed state $\tilde{\varrho}$ with $D_{\leftrightarrow}(\tilde{\varrho}) > 0$. This is because with help of local filtering operation (see Sec. 3): $\tilde{\varrho}_A^{1/2} \otimes I$ it can be brought to the state $\varrho_{\mathrm{PEnt}} \otimes W(p_*)$ which has been shown to be distillable [21]. But upper bounds from Sec. 5 imply that $Q_{\leftrightarrow}(\Lambda_{\mathrm{PEnt}} \otimes \Lambda_{p_*}) \geq D_{\leftrightarrow}(\varrho') > 0$. Thus we have

$$Q_{\leftrightarrow}(\Lambda_{\mathrm{PEnt}} \otimes \Lambda_{p_*}) > 0 \tag{41}$$

and $Q_{\leftrightarrow}(\Lambda_{\mathrm{PEnt}}) = 0$.

Let us suppose now that $W(p_*)$ were BE state. Then Λ_{p_*} would be BE channel because it has been constructed from $W(p_*)$ with help of (35). Thus NPT bound entangled character of $W(p_*)$ implies $Q_C(\Lambda_{p_*}) = 0$ which concludes nonadditivity because of (40), (41). Let us note that here we would have very strong superadditivity as two zero capacity channels would give together one of nonzero capacity.

Summarising, if the Werner state $W(p_*)$ would be NPT BE then the conjecture (33) were true for $C = \leftrightarrow$. It seems very probable that using the combination of techniques of [21] and the above reasoning (applied to one-way distillable entanglement $D_{\rightarrow}$) will lead to nonadditivity if capacity $Q_{\rightarrow} = Q_{\phi}$.

8. Conclusions

Mixed states entanglement is fundamental tool in investigations of "fully" quantum communication. It is especially useful as far as qualitative problems are concerned. In particular, it can serve as a resource for quantum data transfer and this is made with help of distillation of quantum entanglement. Genuine irreversibility represented by so-called bound entanglement is reflected by existence of binding entanglement channels. Bound entanglement phenomenon together with its physical effects led to the conjectures about superadditivity of: (i) two-way distillable entanglement and (ii) two-way quantum capacity. On the other hand, the conjecture on so-called NPT bound entanglement has been formulated and applied to show that in some versions it would lead to superadditivity of (i). Here we have shown that the conjecture also implies superadditivity of (ii). This was done with help of binding entanglement channels idea.

On the other hand, we have performed simple analysis of robustness of entanglement and bound entanglement (in sense of possible error bar) using positive maps. It would be interesting to prepare bound entangled states in lab because they can be used (with help of teleportation) to produce binding entanglement channel that (as we have shown) presumably have curious physical property — superadditivity. All the above depends on validity of the conjecture that the NPT bound entanglement exists. In any case to prove or disprove this conjecture is more than desirable.

Author thanks M. Horodecki and R. Horodecki for helpful discussions. The work is partially supported by the State Committee for Scientific Research, contract No. 2 P03B 103 16, and by the IST project EQUIP, contract No. IST-1999-11053.

Appendix A — physics of quantum operation

We shall recall in brief how to perform the operation (6) physically [63]. Our aim is to perform operation Λ' in case when $\mathcal{H}_A = \mathcal{H}_B = \mathcal{C}^d$. Let us add to our system defined on $\mathcal{H}_A$ the new system called ancilla with the corresponding associated Hilbert space $\mathcal{H}_a = \mathcal{C}^{m+1}$.

We shall first construct some unitary operation U between our system and ancilla $\mathcal{H}_{\rm tot} \equiv \mathcal{H}_a \otimes \mathcal{H}_A$. Let us take the following operation $\tilde{U}$ on space $\mathcal{H}_{\rm tot} \equiv \mathcal{H}_a \otimes \mathcal{H}_A = \mathcal{C}^{m+1} \otimes \mathcal{C}^d$. Let us take the following operation:

$$\tilde{U} \equiv \sum_{i=0}^{m} |i\rangle\langle 0| \otimes V_i. \tag{42}$$

This is not unitary as it vanishes on any vector of the form $|k\rangle|i\rangle \in \mathcal{H}_{\rm tot}$ with $0 < k \leq m$, but on the subspace spanned by the d-element subbasis $\{|0\rangle|i\rangle\}_{i=0}^{d-1}$ it is isometry, i.e. it keeps the scalar product between vectors in that subspace.

In particular, elements of subbasis are mapped into d *orthonormal* vectors in $\mathcal{H}_{\rm tot}$. This follows from the identity $\tilde{U}^\dagger\tilde{U} = |0\rangle\langle 0| \otimes I$ implied by property of the map (8). Operators satisfying (like our matrix U) property $\tilde{X}^\dagger\tilde{X} = P$ are called *partial isometries*.

Now we can write $\tilde{U}$ in the standard basis $\{|k\rangle|i\rangle\}$, $k = 0, \ldots, m+1$, $i = 0, \ldots, d$ in space $\mathcal{H}_{\rm tot}$. Then, because of partial isometry character of $\tilde{U}$, we conclude that it is $d' \otimes d'$ ($d' = (m+1)d$) matrix with first d columns orthonormal and the rest columns vanishing. Because the matrix is squared we can always construct (in a nonunique way) the rest $(d-1)(m+1)$ columns orthonormal to each other and to first d columns of $\tilde{U}$. From those $(d-1)(m+1)$ columns we can immediately define the complementary $\tilde{U}'$ that is partial isometry (like $\tilde{U}$) but on the subspace space corresponding to the projector $(I - |0\rangle\langle 0|) \otimes I$, i.e. it has first d columns vanishing and other $(d-1)(m+1)$ orthonormal already constructed. Then the new matrix $U = \tilde{U} + \tilde{U}'$ resulting from adding two previous partial isometries is squared $d' \times d'$ matrix with orthonormal columns, hence it is *unitary* matrix on $\mathcal{H}_{\rm tot}$. According to quantum mechanics it can be realised by *interaction* between ancilla and our system with the corresponding Hamiltonian. Let us suppose that our system is in the state ϱ. Then the map (6) can be performed in the following steps:

(i) prepare ancilla in state $|0\rangle\langle 0|$,

(ii) allow for interaction represented by unitary transformation U between system and ancilla,

(iii) perform on ancilla standard two-output von Neumann measurement $P_1 = |m\rangle\langle m|$, $P_2 = I - P_1$ with postselection "discarding" our system unless satisfactory result 2 occurs,

(iv) perform partial trace (or "forget" about the ancilla system) getting the reduced density matrix that describes only system.

This will be ϱ' from (5) we wanted to "produce". If the operation is just quantum channel then one omits step (iii) above.

The whole picture can be extended to the case where the final state (after action of the channel) is of different physical character i.e. the system partially or completely changes its character during "transmission". The most elementary example is the following. Alice sends some photons to Bob, someone captures and measures photons somewhere in between and sends atoms to Bob instead with atomic states depending on measurement results on photons. This is just example of separable channel (see Sec. 3).

Appendix B — separability criteria

Let us recall that there exists the necessary and sufficient condition [44] for separability. This is based on positive maps theory [64–67, 53]. Namely:

(I) Given mixed state ϱ defined on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable if for any linear, (i) positive but (ii) not completely positive map Λ mapping states on $\mathcal{H}_A$ onto

states $\mathcal{H}_B$ the new matrix $[\mathcal{I}\otimes\Lambda](\varrho)$ has nonnegative spectrum.* The latter is written in a symbolic way as

$$[\mathcal{I}\otimes\Lambda](\varrho)\geq 0. \tag{43}$$

Example 1. Positive partial transpose condition due to Peres can be formulated as (43) with transposition operation $\Lambda = T$ that transposes (in usual sense) any matrix written in some fixed basis. This is because [64–66, 53] transposition map is positive and one has $\varrho^{T_B} = [\mathcal{I}\otimes T](\varrho)$ by the very definition.

An important result that separability PPT test is not only necessary [45] but also sufficient [46] for two qubits and so-called qubit–qutrit system is based on very special property (called decomposability) [64–67, 53] of positive maps on low dimensional matrices. The failure of that property implies that for higher dimensional systems PPT is only necessary condition of separability [46, 13].

Example 2. The positive map [67] (transforming matrices on $\mathcal{C}^3$ onto matrices on the same space)

$$\Lambda\left(\begin{bmatrix} a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}\right) = \begin{bmatrix} a_{11}+a_{33} & -a_{12} & -a_{13}\\ -a_{21} & a_{22}+a_{11} & -a_{23}\\ -a_{31} & -a_{32} & a_{33}+a_{22}\end{bmatrix} \tag{44}$$

can be applied to reveal entanglement of state (30). Indeed the resulting matrix $[\mathcal{I}\otimes\Lambda](\sigma_1)$ has negative eigenvalue $-\frac{1}{7}$.

There is another characterisation of separability. Let the observable W be called *entanglement witness* [56, 46] if (i) its mean value on any product state is nonnegative i.e. $\mathrm{Tr}(W|e,f\rangle\langle e,f|)\geq 0$, (ii) it has negative mean value on some state ϱ, i.e.

$$\mathrm{Tr}(W\varrho) < 0. \tag{45}$$

Let us note that because of (i) ϱ has to be entangled. We say that W reveals entanglement of ϱ. Now the second characterisation says [46, 56].

(II) Given mixed state ϱ defined on $\mathcal{H}_A\otimes\mathcal{H}_B$ is separable if

$$\mathrm{Tr}(W\varrho)\geq 0 \tag{46}$$

for all entanglement witnesses. The theory of entanglement witnesses is intensively investigated recently. They allowed to reduce new so-called nondecomposable positive maps ([56] and references therein). The nontrivial and technical results form general description of convex subsets of quantum states. In particular, it has been shown that they can be optimised (to reveal in a sense as much entanglement as possible) and applications to multiparticle cases is extensively developed. We shall not discuss those topics here (for synthetic description see [68]).

*In original paper [46] it was defined without (ii) for historical reasons. In practice completely positive maps were of course always excluded as their presence is redundant — they define trivial separability conditions.

Example 3. The "flip" or "swap" operator V on $\mathcal{C}^d \otimes \mathcal{C}^d$ is entanglement witness because (see [12]): (i) $\mathrm{Tr}(V|\phi\rangle\langle\phi| \otimes |\psi\rangle\langle\psi|) = |\langle\phi|\psi\rangle|^2 \geq 0$ and (ii) $\mathrm{Tr}(V|\psi_-\rangle\langle\psi_-|) = -1 < 0$ because $V|\psi_-\rangle = -\psi_-$ (singlet is antisymmetric). Let us note however that V does *not* reveal entanglement any of highly entangled triplet states (like $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ because they are all symmetric with respect to permutation (see [69]).

There is one to one correspondence between entanglement witnesses W and positive but not completely positive operators Λ which is given by so-called Jamiołkowski isomorphism [65]:

$$W = [\mathcal{I} \otimes \Lambda_W^\dagger](P_+), \tag{47}$$

where P_+ is a projector corresponding to the vector $|\Psi_+\rangle = \sum_{k=1}^{\dim\mathcal{H}_A} |k\rangle \otimes |k\rangle$. The map $\Lambda_W^\dagger$ stands for hermitian conjugate of map Λ_W.

Example 4 [69]. One has $V = [\mathcal{I} \otimes T](P_+)$ which means, according to (47) that transposition map corresponds to "flip" operator. Here we see remarkable practical difference between (I) and (II): for two qubits the map $\mathcal{I} \otimes T$ serves as necessary and sufficient separability condition while the corresponding witness does not — for instance it does not reveal entanglement of triplets. The property that single positive map condition reveals more entanglement than the corresponding (in sense of (47)) witness is even true in general (see [68]).

The condition (I) can be further restricted [70] to such linear, positive (but not completely positive) Λ's that are identity preserving, i.e. $\Lambda(I_A) = I_B$ where I_A (I_B) is simply identity matrix on $\mathcal{H}_A$ ($\mathcal{H}_B$). This can be summarised in the following statement: if positive map Λ reveals entanglement of ϱ then some new identity preserving map $\tilde{\Lambda}$ also does.

Appendix C — positive maps and robustness of entanglement

Here we shall provide some simple estimations[†] of sufficient error bar that still allows state to be entangled (or bound entangled). Let us suppose that we are able to produce some entangled (or bound entangled) ϱ of $d \otimes d$ type with error Δ. This means that instead of ϱ our apparatus produces some (unknown) ϱ' such that $||\varrho - \varrho'|| \leq \Delta$ with some norm $||\cdot||$ measuring distance between two states. What can be maximal delta such that ϱ is still entangled (or bound entangled)? Let us note that it would be interesting to produce bound entanglement in lab because from them it is possible to produce physically [23] binding entanglement channels that are conjectured to be nonadditive in general.

We have two simple observations:

• Let us suppose that minimal eingenvalue of PPT state ϱ is λ_+. Then the new state $\varrho' = \alpha\sigma + (1-\alpha)\varrho$ $(0 \leq \alpha \leq 1)$ is PPT for $\alpha \leq \alpha_2 \equiv \frac{2\lambda_+}{2+\lambda_+}$ and arbitrary state σ.

[†] In some form presented in [71], cf. also [25] especially for general observations on this subject.

• Let us suppose that $[\mathcal{I}\otimes\Lambda](\varrho)$ is not positive and has minimal eigenvalue $-\lambda<0$, so ϱ is entangled. Then the new state $\varrho'=\alpha\sigma+(1-\alpha)\varrho$ is entangled and has $[\mathcal{I}\otimes\Lambda](\varrho')$ not positive for $\alpha<\alpha_1\equiv\lambda/(\lambda+a)$ where $a=\max_{P_\Psi}||[\mathcal{I}\otimes\Lambda](P_\Psi)||_\infty$ with norm $||X||_\infty=\max_{|||\phi\rangle||=1}||X|\phi\rangle||$. Here $|||\phi\rangle||=|\langle\phi|\phi\rangle|^2$. Let us note that $a\leq d||[\mathcal{I}\otimes\Lambda](P_+)||$.

Therefore if ϱ is PPT and violates (43) then ϱ' has also both properties for $\alpha<\alpha_3=\min(\alpha_1,\alpha_2)$. This is important if we would like to produce PPT states that are entangled.

Let us note that above we have considered three sets: S_1, S_2, S_3 which corresponds to entangled states, PPT states and intersection of the two latter sets.

Indeed one has the following property: if $\varrho\in S_k$ and $\alpha<\alpha_k$ (for $k=2,3$) or $\alpha\leq\alpha_k$ (for $k=1$), then any new density matrix of the form $\varrho'=\alpha\sigma+(1-\alpha)\varrho$ (σ arbitrary) also satisfies $\varrho'\in S_k$.

Let us consider now state ϱ of full rank. Let us denote set of all density matrices by $\mathcal{P}$ with interior $\mathrm{int}\mathcal{P}$ and boundary $\partial\mathcal{P}$. Any full rank state belongs to $\mathrm{int}\mathcal{P}$ and can be reproduced by $\varrho'=\alpha\sigma+(1-\alpha)\varrho$ for some $\sigma\in\partial\mathcal{P}$. From that we get by immediate estimates that if $||\varrho-\varrho'||\leq\Delta$ with error $\Delta<\alpha_k\min_{\sigma\in\partial\mathcal{P}}||\varrho-\sigma||$ (again for $k=2,3$) or $\Delta\leq\alpha_k$ (for $k=1$) then $\varrho\in S_k$. Thus error bar Δ can be bounded from above by $\alpha_k\min_{\sigma\in\partial\mathcal{P}}||\varrho-\sigma||$. Let us note that we have had the norm unspecified. If we put the trace norm $||A||_1=\mathrm{Tr}(|A|)$ then we see that $\min_{\sigma\in\partial\mathcal{P}}||\varrho-\sigma||$ is just the distance of vector $\boldsymbol{p}=[p_1,\ldots,p_n]$ (defined by the spectrum $\{p_i\}_{i=1}^n$ of ϱ) to the boundary of n-dimensional simplex where the distance on simplex is simply measured $d(\boldsymbol{p},\boldsymbol{p}')=\sum_i|p_i-p_i'|$. The latter follows from inequality saying that for any states ϱ, ϱ' with spectra $\boldsymbol{p}$, $\boldsymbol{p}'$ one has $||\varrho-\varrho'||\geq d(\boldsymbol{p},\boldsymbol{p}')$ (see lemma 1.7, p. 22 of Ref. [72]).

The problem is that in the above we need states of full rank while most popular examples of BE states are "edge" states (see [68]) that are singular and have $\lambda_+=0$. However, one can admix some full rank state (like maximally mixed one I_A/d_A). Then the procedure outlined above can be applied to give nonzero error Δ allowed.

References

[1] A. Albert, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, A. Zeilinger, *Quantum Information: An Introduction to Basic Concepts and Experiments*, Springer-Verlag, Berlin 2001.

[2] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W.K. Wootters, *Phys. Rev. Lett.* **76,** 722 (1996).

[3] D. Gottesmann, I.L. Chuang, *Nature* **402,** 390 (1999).

[4] E. Knill, R. Laflamme, G. Milburn, http://arXive.org/abs/quant- ph/0006088.

[5] C.H. Bennett, G. Brassard, in: *Proc. IEEE Conf. in Computers, Systems and Signal Processing, Bangalore (India) 1984*, IEEE, New York 1984, p. 175.

[6] A. Ekert, *Phys. Rev. Lett.* **67,** 661 (1991).

[7] P. Shor, in: *Proc. 35th Annual Symp. on Foundation of Computer Science*, IEEE Computer Society Press, Santa Fe, NM 1994.

[8] P. Shor, *Phys. Rev. A* **52,** 2439 (1995).

[9] A. Steane, *Phys. Rev. Lett.* **77,** 793 (1996).

[10] C.H. Bennett, D.P. Di Vincenzo, J. Smolin, W.K. Wootters, *Phys. Rev. A* **54,** 3814 (1997).

[11] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, *Phys. Rev. Lett.* **77,** 2818 (1996).

[12] R.F. Werner, *Phys. Rev. A* **40,** 4277 (1989).

[13] P. Horodecki, *Phys. Lett. A* **232,** 333 (1997).

[14] V. Vedral, M. Plenio, *Phys. Rev. A* **57,** 1619 (1998).

[15] G. Vidal, *J. Mod. Opt.* **47,** 355 (2000).

[16] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **84,** 2014 (2000).

[17] M. Horodecki, *Quantum Inf. Comput. J.* **1,** 27 (2001).

[18] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **80,** 5239 (1998).

[19] D.P. DiVincenzo, P.W. Shor, J.A. Smolin, B. Terhal, A.W. Thapliyal, *Phys. Rev. A* **61,** 062312 (2000).

[20] D. Dür, J.I. Cirac, M. Lewenstein, D. Bruss, *Phys. Rev. A* **61,** 062313 (2000).

[21] P.W. Shor, J.A. Smolin, B.M. Terhal, *Phys. Rev. Lett.* **86,** 2681 (2001).

[22] P. Horodecki, M. Horodecki, R. Horodecki, *J. Mod. Opt.* **47,** 347 (2000).

[23] D. DiVincenzo, T. Mor, P. Shor, J. Smolin, B.M. Terhal, *Commun. Math. Phys.*, in press; quant-ph/9908070.

[24] P. Horodecki, M. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **82,** 1046 (1999).

[25] B.M. Terhal, http://arXive.org/abs/quant-ph/0101032.

[26] N. Gisin, *Phys. Lett. A* **210,** 151 (1996).

[27] C.H. Bennett, H.J. Bernstein, S. Popescu, B. Schumacher, *Phys. Rev. A* **53,** 2046 (1996).

[28] D.P. DiVincenzo, P. Shor, J. Smolin, *Phys. Rev. A* **57,** 830 (1998).

[29] R. Alicki, private communication.

[30] P. Horodecki, R. Horodecki, *Quantum Inf. Comput. J.* **1,** 45 (2001).

[31] S. Popescu, *Phys. Rev. Lett.* **72,** 797 (1994).

[32] H. Barnum, E. Knill, M. Nielsen, *IEEE Trans. Inf. Theory* **46,** 1317 (2000).

[33] S.J. van Enk, J.I. Cirac, P. Zoller, *Science* **279,** 205 (1998).

[34] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **82,** 433 (2000).

[35] B. Schumacher, M.A. Nielsen, *Phys. Rev. A* **54,** 2629 (1996).

[36] M. Horodecki, Ph.D. thesis, University of Gdańsk, Gdańsk 2000.

[37] A. Holevo, R. Werner, *Phys. Rev. A* **63,** 032312 (2001).

[38] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. A* **60,** 1888 (1999).

[39] P. Badziąg, M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. A* **62,** 012311 (2000).

[40] M. Horodecki, P. Horodecki, *Phys. Rev. A* **59,** 4026 (1999).

[41] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W.K. Wootters, *Phys. Rev. Lett.* **70,** 1895 (1993).

[42] W.H. Wootters, W.H. Zurek, *Nature* **299,** 802 (1982).

[43] D. Dieks, *Phys. Lett. A* **92,** 271 (1982).

[44] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **78,** 574 (1997).

[45] A. Peres, *Phys. Rev. Lett.* **77,** 1413 (1996).

[46] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **223,** 1 (1996).

[47] G. Vidal, J.I. Cirac, *Phys. Rev. Lett.* **80,** 5803 (2001).

[48] G. Vidal, J.I. Cirac, http://arXive.org/abs/quant-ph/0107051.

[49] P. Horodecki, M. Horodecki, R. Horodecki, *Acta Phys. Slovaca* **48,** 141 (1998).

[50] S. Popescu, D. Rohrlich, *Phys. Rev.* **56,** 3219 (1997).

[51] M. Horodecki, R. Horodecki, *Phys. Lett. A* **244,** 473 (1998).

[52] R. Horodecki, M. Horodecki, P. Horodecki, *Phys. Rev. A* **63,** 022310 (2001).

[53] M.D. Choi, *Proc. Symp. Pure Math.* **38,** 583 (1982).

[54] P. Horodecki, M. Lewenstein, *Phys. Rev. Lett.* **85,** 2657 (2000).

[55] C.H. Bennett, D. DiVincenzo, T. Mor, P. Shor, J. Smolin, B.M. Terhal, *Phys. Rev. Lett.* **82,** 5385 (1999).

[56] B.M. Terhal, *Lin. Algebr. Appl.* **323,** 61 (2000).

[57] W. Dür, J.I. Cirac, *Phys. Rev. A* **61,** 042314 (2000).

[58] W. Dür, J.I. Cirac, *Phys. Rev. A* **62,** 022302 (2000).

[59] P.W. Shor, J.A. Smolin, A.V. Thaplyial, http://arXive.org/abs/quant-ph/0005117.

[60] B. Kraus, J.I. Cirac, S. Karnas, M. Lewenstein, *Phys. Rev. A* **61,** 062302 (2000).

[61] A. Sanpera, R. Tarrach, G. Vidal, *Phys. Rev. A* **58,** 826 (1998).

[62] M. Lewenstein, D. Bruß, J.I. Cirac, B. Kraus, M. Kuś, J. Samsonowicz, A. Sanpera, R. Tarrach, *J. Mod. Opt.* **47,** 2481 (2000).

[63] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Wiley, New York 1991.

[64] E. Störmer, *Acta Math.* **110,** 233 (1963).

[65] A. Jamiołkowski, *Rep. Math. Phys.* **3,** 275 (1972).

[66] S.L. Woronowicz, *Rep. Math. Phys.* **10,** 165 (1976).

[67] E. Størmer, *Proc. Am. Math. Soc.* **86,** 402 (1982).

[68] D. Bruss, J.I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, A. Sanpera, *J. Mod. Opt.*, in press.

[69] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **283,** 1 (2001).

[70] P. Horodecki, in: *Proc. NATO ARW, Mykonos (Greece) 2000*, in press.

[71] P. Horodecki, unpublished.

[72] M. Ohya, D. Petz, *Quantum Entropy and its Use*, Springer Texts and Monographs in Physics, Springer-Verlag, Berlin 1993.