Central European Science Journals
w w w . c e s j . c o m

Central European Journal of Physics
Central European Science Journals
CEJP 4 (2003) 695–707

On entanglement distillation and quantum error correction for unknown states and channels

Paweł Horodecki

Faculty of Applied Physics and Mathematics,
Gdańsk University of Technology,
80–952 Gdańsk, Poland

Received 28 April 2003; accepted 28 July 2003

Abstract: We consider the problem of invariance of distillable entanglement D and quantum capacities Q under erasure of information about single copy of quantum state or channel respectively. We argue that any $2 \otimes N$ two-way distillable state is still two-way distillable after erasure of single copy information. For some known distillation protocols the obtained two-way distillation rate is the same as if Alice and Bob knew the state from the very beginning. The isomorphism between quantum states and quantum channels is also investigated. In particular it is pointed out that any transmission rate down the channel is equal to distillation rate with formal LOCC-like superoperator that uses in general nonphysical Alice actions. This allows to we prove that if given channel Λ has nonzero capacity ($Q_{\rightarrow}$ or $Q_{\leftrightarrow}$) then the corresponding quantum state $\varrho(\Lambda)$ has nonzero distillable entanglement ($D_{\rightarrow}$ or $D_{\leftrightarrow}$). Following the latter arguments are provided that any channel mapping single qubit into N level system allows for reliable two-way transmission after erasure of information about single copy. Some open problems are discussed.

Keywords: quantum entanglement,quantum channels,quantum capacities
PACS (2000): 03.67.-a, 03.65.Bz, 03.65.Ca, 03.67.Hk

1 Introduction

Distillation of quantum entanglement [1] is an interesting way to make some quantum communication possible despite destructive actions of environment (external noise). It allows one to perform quantum teleportation [3] as well as quantum cryptography [2] with entangled states possible in the presence of external noise. In fact both mentioned phenomena require one or more numbers of maximally entangled pairs, say in two spin-$\frac{1}{2}$

state

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

where $|0\rangle$ ($|1\rangle$) correspond to spin-"up" (spin-"down") state. If Alice and Bob stay in separate locations and share pairs of particles in state (1) then they can perform the quantum cryptography scheme or teleport some number of quantum states form one site to another. In practice however, they share a number of mixed (noisy) states ϱ having only some residual entanglement. Then usually they can *distill noisy entanglement* of ϱ getting some smaller number of (approximately) singlet states by means of so called LOCC operations i. e. operations involving an arbitrary local actions plus classical (one-way or two-way, see [4]) communication between Alice and Bob.

The asymptotic rate of singlets produced by LOCC protocol $\mathcal{P}$ is denoted by $D^{\mathcal{P}}(\varrho)$ and it is called *distillable entanglement under the protocol* $\mathcal{P}$. The quantity $D_C = \max_{\mathcal{P}} D_C^{\mathcal{P}}(\varrho)$ is called *distillable entanglement* (see [4]). Here maximum is taken over subclass of protocols that involve only chosen type C of classical communication between two labs where $C = \emptyset, \rightarrow, \leftarrow, \leftrightarrow$ corresponds to zero-way, one-way and two-way communication scheme (see [4]).

In general one says that ϱ is *distillable* or that it represents *free entanglement* when $D_\leftrightarrow$ is nonzero. All bipartite separable states ie. those represented by convex combination of produced states (see [7]) are nondistillable ie. $D_\leftrightarrow = 0$. The entangled state which is distillable is called *free entangled*. There are [10] states which are entangled but not distillable and they are called *bound entangled*. For bipartite spin-like systems bound entanglement phenomena where *global* spin is *greater than* 3/2 (see [10]). In particular for $2 \otimes 2$, $(2 \otimes 3)$ systems [11] all entanglement is free and the corresponding protocol is provided in [9]. For $2 \otimes N$ there is bound entanglement, but any free entanglement must violate PPT separability test [12], and is distillable (see [13]) with help of the immediate extension of two-qubit protocol. There is a long-standing open problem [14] whether so called NPT bound entanglement exists ie. entanglement that violates PPT separability test but is nondistillable. Its existence would lead to serious consequences like nonadditivity of distillable entanglement D [15] or nonadditivity of two-way quantum channels capacity [19](c.f. [20]).

2 States and channels connection

On the other hand there is a quantum channels theory (see [4, 6]) where one of the main tasks is, roughly speaking, to send maximal number of quantum bits down a given quantum channel (completely positive tracepreserving map). In this scenario, like in distillation protocols, sender (Alice) and receiver (Bob) can communicate classically. Optimal rate of sent qubits is called quantum capacity Q_C of given quantum channel and is defined in some analogy to distillable entanglement D_C.

There is well-known connection between quantum states and quantum channels. Namely any quantum channel $\Lambda : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}_B)$ is in one to one correspondence

(called Jamiołkowski isomorphism [16]) with a bipartite quantum state that has maximally mixed subsystem A:

$$\varrho(\Lambda) = [I \otimes \Lambda](P_+^{d_A}) \tag{2}$$

Here $P_+^{d_A} = |\Psi_+^{d_A}\rangle\langle\Psi_+^{d_A}|$ is a projector corresponding to "isotropic" maximally entangled state on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_A$:

$$\Psi_+^{d_A} \equiv \frac{1}{\sqrt{d_A}} \sum_{i=0}^{d_A-1} |i\rangle|i\rangle \tag{3}$$

The above state has an important property (cf. [17]). Namely for any matrix $A : \mathcal{H}_A \to \mathcal{H}_B$ one has

$$I \otimes A|\Psi_+^{d_A}\rangle = \sqrt{\frac{d_B}{d_A}} A^T \otimes I|\Psi_+^{d_B}\rangle \tag{4}$$

The above isomorphism (2) together with the so-called binding entanglement channels idea [18] allows you to point out [19] another consequence of existence of NPT bound entanglement of some special Werner states: nonadditivity of two-way quantum channels capacity.

Moreover in seminal paper [4] the isomorphism together with quantum teleportation idea [3] have been utilised to prove that $D_C(\varrho(\Lambda)) \leq Q_C(\Lambda)$. Hence $D_C > 0$ implies $Q_C(\Lambda) > 0$. Below we shall make the states-channels connection even stronger by showing that *the reverse* implication is also true.

However, maybe the most interesting problem which we would like to address here is the question of distillation and transfer rates in case of prior unknown states and channels respectively.

3 Main problem

The question of whether it is possible to distill entanglement from unknown states was first raised in Ref. [21] where it was shown that for the hashing method [4] (ffollowed by a twirling procedure that transforms any given state to a Bell state) the distillation rate is identical to that of the protocol when the state is unknown. Here we would like to address quite general question:

Question 3.1. Suppose that distillable bipartite state ϱ is completely unknown to Alice and Bob. It is possible:
(1a) to distill nonzero amounts of entanglement from it, and
(1b) to distill a number of singlets equivalent to distillable entanglement of the state?

Below we shall argue that the question (1a) has positive answer in general $2 \otimes N$ case as far as two-way distillation protocols are concerned. We shall also show that the universal protocol for two qubits can be modified to give for unknown states the same distillation rate as for known states. We shall leave the general case of $n \otimes m$ systems as

an open question. In the above context it is natural to ask parallel questions for quantum channels:

Question 3.2. Suppose that quantum channel Λ has nonzero capacity but is completely unknown to Alice and Bob. It is possible:
(2a) to send reliably nonzero amount of qubits down that channel, and
(2b) to achieve the same capacity as if the channel were known to the sender and/or receiver?

Note that analogous questions can be addressed for classical capacities of quantum channel but it goes beyond the scope of the present paper.

Our approach will be more heuristic that of [21]. Indeed we shall assume that after the estimation the state Alice and Bob share can be described by produced $\varrho'^{\otimes n}$ rather than exchangeable state $\varrho_{ex} = \int d\alpha \varrho(\alpha)^{\otimes n}$ (see [21]) with some distribution $d\alpha$.

The present approach is less rigorous but gives intuitions for a much more general case than previously considered Bell-diagonal states.

4 Distilling entanglement from unknown states

Special cases 4.1. Below we shall argue first why the most naive continuity argument does not work in case of the above problems. Given n systems in (unknown) state ϱ the simplest strategy for observers is to scarify some portion of states and perform quantum tomography (see [23] and references therein). Of course they should get nonzero yield during their protocol [4]. Thus they can only use same part of pairs say $f(n)$ where $\frac{f(n)}{n} \to c$, $0 \leq c < 1$ ($c = 0$ means that the number pairs used for tomography is negligible in the limit). It is crucial here that $c < 1$, because otherwise they would get zero efficiency. After performing the quantum tomography on the part of $\frac{f(n)}{n}$ pairs they can take the rest of them $n' = (1 - \frac{f(n)}{n})n \sim (1 - c)n$ and perform $\mathcal{P}'$ some protocol on them *as if each of them were in the estimated state* ϱ'_n. The parameters of estimated state however ϱ'_n must have variance proportional to $\frac{1}{\sqrt{f(n)}}$, since the corresponding standard deviation is proportional to the inverse of number of copies used in quantum tomography. Consider the mixed states fidelity [17]

$$F(\varrho_1, \varrho_2) = \max_{|\Psi_1\rangle, |\Psi_2\rangle} |\langle \Psi_1 | \Psi_2 \rangle|^2, \tag{5}$$

where $|\Psi_1\rangle$, $|\Psi_2\rangle$ are arbitrary purifications of states ϱ_1, ϱ_2 respectively. Recall that $F(\varrho_1 \otimes \sigma_1, \varrho_2 \otimes \sigma_2) = F(\varrho_1, \varrho_2) F(\varrho_2, \sigma_2)$. The variance condition mentioned above makes reasonable to assume that $||\varrho - \varrho'_n|| \sim w \frac{1}{\sqrt{f(n)}}$ for some constant w depending on dimension of Hilbert space but not on n (here $||A|| = Tr|A|$). It is known that [25]

$$F(\varrho, \sigma) \leq 1 - \frac{1}{2} ||\varrho - \sigma||^2. \tag{6}$$

Now one has $F(\varrho^{\otimes n}, \varrho_n'^{\otimes n}) = F(\varrho, \varrho_n')^n \sim (1 - \frac{w^2}{2f(n)})^n \overset{n\to\infty}{\longrightarrow} exp(-w^2/2c)$ and in particular

$$F(\varrho^{\otimes n}, \varrho_n'^{\otimes n}) \overset{c\to 0}{\longrightarrow} 0. \tag{7}$$

This apparently seems to provide a sort of alternative: either Alice and Bob decide do spend finite amount of pairs to estimate the state, or they must operate on the quantum state $\varrho^{\otimes n}$ which becomes "orthogonal" (in the above sense) to the estimated states ${\varrho_n'}^{\otimes n}$. In other words the results of tomography do not diverge in the usual sense to the state one needs. This, however, does not imply automatically that Alice and Bob can not distill any pure entanglement if they do not know ϱ. Indeed, the distillation protocol can be sometimes highly insensitive to changes of the states since during the protocol Alice and Bob can gather some sort of global information or information about sets of states (like in hashing, where parity of sequence of states is checked). Thus the naive representation of the state they operate by ${\varrho'}^{\otimes n}$ will fail at some stage of the protocol. Note also that usually the observers just erase a lot of unknown parameters in the state with help of twirling-like operations (see [4]).

One can define the new quantity $D_C^?(\varrho)$ which is distillable entanglement under the condition that information about a single copy has been erased. The questions are: (a) whether one has $D_C^?(\varrho) > 0$ if $D_C(\varrho) > 0$ (b) whether $D_C^?(\varrho) < D_C(\varrho)$.

We know that for specific protocols (i.e. if we replace distillable entanglement under some, not necessarily optimal, protocol) this inequality does not need to be true. In fact, the case of $2 \otimes 2$ Bell diagonal case has been analysed and it has been shown (taking into account the exchangeability condition mentioned above) that for $D_{\leftrightarrow}^?$ condition (a) above is satisfied and condition (b) is at least satisfied for some special (hashing) protocol [21].

Below we shall argue that $D_{\leftrightarrow,\mathcal{P}} = D_{\leftrightarrow,\mathcal{P}}^?$ is true for the only universal distillation protocol $\mathcal{P}$ we know so far i.e. the one that allows you to distill nonzero amounts of entanglement from an arbitrary entangled $2 \otimes 2$ state [9]. We shall provide here a probabilistic version of the protocol i.e. the one which some pairs are discarded. This implies that the involved superoperators are not tracepreserving. It has been shown, however, that the existence of a probabilistic protocol leads to a deterministic one [8]. So it is justified to restrict oneself to probabilistic protocols.

The universal two-qubit protocol $\mathcal{P}_{univ}$ consists of three steps (see [9]) (i) filtering operation of each pair ϱ followed by the "twirling" operation this gives on average fraction of η_1 $(0 < \eta_1 \leq 1)$ of pairs in Werner state $\varrho_{W,n}$ with the overlap with singlet state $F(\varrho_{W,n}) > \frac{1}{2}$; (ii) recurrence protocol which produces on average the fraction $\eta_2(F) = \frac{1}{2^L}$ of $2 \otimes 2$ Werner states with the parameter $\eta_3 = 1 - S_A(F) > 0$ for local (Alice) von Neumann entropy S_A which can be chosen as *as a nonincreasing function* of F; (iii) hashing protocol which provides on average the fraction $1 - S_A$ singlet pairs from input pairs in Werner state.

The above protocol $\mathcal{P}_{univ}$ has be shown rigorously [26] to produce on average $D_{\leftrightarrow,\mathcal{P}_{univ}} = \eta_1\eta_3\eta_3 > 0$ singlet pairs. Here we address different question: what about if the state of single copy ϱ is completely unknown ? Is it possible to distill at least the some number of singlets? What about optimal protocol distilling all possible entangle-

ment?

First let us recall that both η_1 and F from (i) are *continuous* parameters of single copy. Thus given a number n of entangled but unknown $2 \otimes 2$ states Alice and Bob can proceed as follows: divide the sample of particles into two groups consisting of $\sqrt{n}$ and $n - \sqrt{n}$ pairs. They can spend $\sqrt{n}$ pairs on tomography which will lead to estimated state ϱ'_n such that $||\varrho - \varrho'_n|| \sim \frac{1}{\sqrt[4]{n}}$. Combining the latter with continuity of parameters η_1 and F one concludes that for large n Alice and Bob operate on states with the filtering parameter form (i) not less then some $\eta_1^n > 0$ (somewhat underestimated because of error) and the corresponding Werner state parameter $F(\varrho_{W,n})$ for any n bounded from below by sequence of constants $F^n > \frac{1}{2}$. Moreover we have the convergences: $\eta_1^n \to \eta_1(\varrho)$ and $F^n \to F(\varrho)$. The recurrence protocol relies on the recurrence function which is nondecreasing in F if only initial parameter satisfies $F > \frac{1}{2}$. Thus applying (ii) will result in a fraction η_2^n of Werner states bounded from below by $\eta_2(F_n)$ defined by step (ii) above. The von Neumann entropy S_A^n will converge in a nondecreasing way to S_A determined by the protocol with known states.

The remaining Werner states $\varrho_{W,n}^{(n-\sqrt{n})\otimes}$ are supposed to be subjected to hashing protocol. Form results of Ref. [21] we know that the hashing protocol (iii) can be carried out successfully despite the fact that Alice and Bob do not know the state. This concludes the protocol distilling entanglement from initially unknown state ϱ.

The above reasoning does not take into account the exchangability assumption [21] of joint state ie. that if the joint state is unknown than it should be taken as $\int \varrho(\vec{p})^n d\vec{p}$ over some probability distribution rather than $\varrho(\vec{p})^{\otimes n}$ for some unknown, yet single vector parameter $\vec{p}$ [22]. However, our assumption that Alice and Bob know the Werner state in product ${\varrho'_W}^{\otimes n}$ state up to some error bar of F can be reconstructed as a special case of the distribution $d\vec{p}$ picked around some value of $\vec{p}$.

The efficiency of the whole protocol applied to the remaining pairs for fixed n will give on average $\frac{n-\sqrt{n}}{n}\eta_1^n\eta_2^n\eta_3^n$ which for large n approaches

$$D^{?}_{\leftrightarrow,\mathcal{P}_{univ}} = \eta_1\eta_3\eta_3 > 0. \tag{8}$$

The latter is distillable entanglement of the protocol with known pairs. Since for any $2 \otimes N$ pairs the scheme of distillation is the same as for $2 \otimes 2$ case see [13] the above protocol immediately applies for entangled $2 \otimes N$ systems.

Summarising, any $2 \otimes N$ state remains two-way distillable after erasure of single copy information and the corresponding distillation rate (distillable entanglement) is not greater than (8).

Let us consider the general $n \otimes m$ case. There is a theorem [10] saying that distillability of given state ϱ is always manifested by the existence of a Schmidt rank two tensor such that $(\varrho^{T_2})^{\otimes n}$ for some natural n:

$$\langle\psi|(\varrho^{T_2})^{\otimes n}|\psi\rangle < 0 \tag{9}$$

Using this fact one can immediately make further generalisation of the above results to any $n \otimes m$ state for which Alice and Bob have the following prior information: if the

state is distillable then it is manifested by (9) for some n not greater than some fixed n_0. Usual tomography method applied on clusters of states $\varrho^{\otimes n}$, $n \leq n_0$ pairs and allows than to identify the vector ψ as it was in $2 \otimes 2$ case [9].

We have investigated only two-way distillation so far. To analyse one-way scenario one would consider carefully the classical information flow since any prior one-way state estimation gives full information about the state *only* to Bob. Hence it is much more difficult to answer whether $D^{?}_{\rightarrow}$ is nonzero if only $D^{?}_{\rightarrow} > 0$. It may not be true. Indeed even if only one-way steps (i) (filtering) and (ii) (hashing) are allowed in the original protocol, it can not be excluded that after erasing single copy information Alice will never know which kind of filtering she should apply in step (i). If we relax the conditions seeking for *one-way* distillation with *two-way* prior state estimation then obviously the previous result easily generalises giving nonzero $D^{?}_{\rightarrow}$ in all cases when the original protocol was combined from (i) and (iii).

Let us discuss the result in the context of the behavior (7). It happens that the superoperator works well (even if the states apparently "diverge" as in (7)). However the above reasoning will probably fail if we allow some sophisticated collective superoperators because of counterintutive observation (7). Namely the above analysis strongly relies on two facts:
(a) all the operations transforming states into Werner states $\varrho_{W,n}$ are *continuous* in single copy parameters and are performed *only* on single copy,
(b) all the involved collective LOCC operations behave "well" on partially unknown Werner states (in particular result of Ref. [21] on hashing is crucial here).

But in general if Alice and Bob do not know k_0 they do not know what part of states should subject to tomography. It is likely that this step could be somehow omitted. However the case $D > D^{?}$ (or even, somewhat unlikely, $D > D^{?} = 0$) can not be definitely excluded at the moment. In any case the main problem remains: the *optimal* protocol achieving D (even in $2 \otimes 2$) case might necessarily involve collective operations which will not behave "well" (see (a), (b) above). Then even if the conclusions remain true, the proof must be changed.

5 Quantum states and channels: qualitative equivalence of D and Q

In the above context we shall consider remarkable theorem which shows the power of analogy between mixed-states entanglement and quantum error correction [4]. Namely let us consider the

Observation 5.1. For any channel Λ and $C = \rightarrow, \leftrightarrow$ one has $D_C(\varrho_\Lambda) > 0$ iff $Q_C(\Lambda) > 0$.

Remark 5.2. The implication $D_C(\varrho_\Lambda) > 0 \Rightarrow Q_C(\Lambda) > 0$ is well-known since it has been proven [4] that $D_C(\varrho_\Lambda) \leq Q_C(\Lambda)$ for all types of classical communication involved ($C = \leftarrow, \emptyset, \rightarrow, \leftrightarrow$).

Remark 5.3. The above Observation can be understand to represent *qualitative equivalence* of distillable entanglement and channel capacity. Qualitative equivalence means here that one quantity is not trivial (zero) if and only iff another is not.

Proof 5.4. *Proof of the second implication (⇒).* We shall prove the "only if' part of the theorem. First we need some general observations. Optimal distillable entanglement is achieved by tracepreserving LOCC action [8]. The most general tracepreserving LOCC action Alice and Bob can perform has a form of "ping-pong" protocol. In the protocol Alice and Bob perform sequence of POVM-s in turn where any particular POVM depends on the results of all previously performed. This corresponds to the sequence of families of operations: V_{k_1}, V_{k_1,k_2}, $V_{k_1k_2k_3}$, $V_{k_1k_2k_3k_4}$, ..., $V_{k_1k_2k_3,...,k_m}$. The corresponding k-th POVM with the tracepreserving condition $\sum_{k_1k_2k_3,...,k_l} V^{\dagger}_{k_1k_2k_3,...,k_l} V_{k_1k_2k_3,...,k_l} = I$ for any l represents Alice (Bob) action for odd (even) index k. Roughly speaking Alice and Bob have their operations *correlated*. This is not so in case of zero-way distillation protocol $C = \emptyset$ where one has just product of two operations. Thus given any channel Λ the most general Alice and Bob LOCC protocol corresponds to

$$\Lambda' = \sum_{\mathbf{k}} \Lambda^B_{\mathbf{k}} \circ \Lambda \circ \Lambda^A_{\mathbf{k}}. \tag{10}$$

In the above formula the multiindex $\mathbf{k}$ can be equivalent to sequence

$$\{k_1, k_2, ..., k_{l_{max}}\}. \tag{11}$$

Then the operations $\Lambda^A_{\mathbf{k}}$, $(\Lambda^B_{\mathbf{k}})$ correspond to Alice (Bob) *elementary action*. They are *filtering actions* [27] composed of products of $V_{k_1,...,k_l}$ with even (odd) index l, $(l \leq l_{max})$. It may happen however that the multiindex corresponds to collection of sequences of type (11). Then the maps $\Lambda^A_{\mathbf{k}}$, $(\Lambda^B_{\mathbf{k}})$ correspond to *sum of elementary filtering operations* and can be in general tracepreserving, even bistochastic (both trace and identity preserving). Sometimes it can possess the intermediate property: preserving trace and maximally mixed state (which coincides with bistochasticity only if dimensions of input and output are the same).

Following the above, using standard analysis from quantum channels theory one can conclude that the capacity $Q_C(\Lambda)$, for given channel Λ, $(C = \rightarrow, \leftrightarrow)$ can be achieved by the sequence of LOCC operations which, composed with power of quantum channel, are:

$$\Lambda^{(n)} = \sum_{\mathbf{k}} \Lambda^B_{\mathbf{k}} \circ \Lambda^{\otimes n} \circ \Lambda^A_{\mathbf{k}}. \tag{12}$$

Here for simplicity of the notation we shall consider the channel that acts $\Lambda : \mathcal{H}_A \rightarrow \mathcal{H}_B$ ($\dim \mathcal{H}_A = d_A$, $\dim \mathcal{H}_B = d_B$). The two (equivalent) definitions of quantum capacity have been provided in Refs. [4, 5]. Here it is natural to understand it [4] as a optimal (i. e. optimized over composed actions of type (12)) ratio $log_2 m(n)/(n log_2 d)$ $(d = min[d_A, d_B])$ with the parameter n from (12) and $m(n)$ being the dimension of "reliably sent" Hilbert space playing the role of domain of Alice and Bob actions: $\Lambda^A_{\mathbf{k}} : \mathcal{H}_{m(n)} \rightarrow \mathcal{H}^{\otimes n}_A$, $\Lambda^B_{\mathbf{k}}$:

$\mathcal{H}_B^{\otimes n} \to \mathcal{H}_{m(n)}$. It should be stressed that $\mathbf{k}$ depends on n though we do not make it explicit here. Usually it is assumed that $m(n) = 2^{k(n)}$ and then $log_2 m(n) = k(n)$ is interpreted as *rate of qubits* that can be sent down the channel reliably asymptotically.

Since the channel (12) is assumed to allow for reliable transmission, it preserves maximally entangled state if half of it is sent down that channel. It means that for large n the state

$$\sigma_n = [I \otimes \Lambda^{(n)}](P_+^{m(n)}) \tag{13}$$

satisfies the condition $Tr(P_+^{m(n)}\sigma_n) \to 1$. Now can see that

$$\sigma_n = [\sum_{\mathbf{k}} \overline{\Lambda}_{\mathbf{k}}^B \otimes \Lambda_{\mathbf{k}}^A] \circ [[I \otimes \Lambda](P_+^{d_A}]^{\otimes n} = [\sum_{\mathbf{k}} \overline{\Lambda}_{\mathbf{k}}^B \otimes \Lambda_{\mathbf{k}}^A][\varrho(\Lambda)]^{\otimes n}). \tag{14}$$

Here the definition $\overline{\Lambda} \equiv \frac{(d_A)^n}{m(n)} T \circ \Lambda^\dagger \circ T$ has been used (here $T(\cdot) \equiv (\cdot)^T$ stands for transposition map). For any completely positive (CP) Λ the above formula (14) follows easily from the property (4) and Kraus representation of CP map. Straightforward calculation shows that $\overline{\Lambda}$ shares with Λ the property of complete positivity.

Before continuing the proof we shall made some digression providing two observations.

Observation 5.5. Let the quantum error correction protocol with resource C achieves the rate $Q_C^{\mathcal{P}}$ with the transmission down the channel Λ with help of the protocol $\mathcal{P}$ corresponding to (12). Then there is a "formal" entanglement distillation protocol $\tilde{\mathcal{P}}$ represented by (in general *not* tracepreserving) LOCC-like superoperator family:

$$\mathcal{S}_C = \sum_{\mathbf{k}} \overline{\Lambda}_{\mathbf{k}}^A \otimes \Lambda_{\mathbf{k}}^B \tag{15}$$

that achieves on the state $\varrho(\Lambda)$ the same rate $D_C^{\mathcal{P}'} = Q_C^{\mathcal{P}}$.

The formal distillation protocol may be in general unphysical since it is nontracepreserving, however it preserves still the ping-pong like structure and in that sense it is LOCC-like. Note by the way, that the following superoperators

$$\mathcal{S}'_C \equiv \sum_{\mathbf{k}} \Lambda_{\mathbf{k}}^A \otimes \Lambda_{\mathbf{k}}^B \tag{16}$$

are always legitimate LOCC operations involving resource C. This follows from the fact that each of the observers performs the same actions as in the case of tracepreserving transfer process (12). The only difference is an object the actions concern.

Summarising, Observation 5.5 says us that quantum capacity is equal to optimal distillation rate under in (general nonphysical) class of LOCC superoperators. Note that $\Lambda_{\mathbf{k}}^A$ in the Observation 5.1 correspond to Alice "encoding" actions. As a by-product of the above analysis we have the following immediate consequence:

Observation 5.6. If the transmission rate $Q_C^{\mathcal{P}}$ is achieved under Alice encoding actions $\Lambda_{\mathbf{k}}^A$ that preserves maximally mixed state then there is a distillation protocol $\tilde{\mathcal{P}}$ with the rate $D_C^{\tilde{\mathcal{P}}}(\varrho(\Lambda)) = Q_C^{\mathcal{P}}(\Lambda)$.

Note that the property of preserving maximally mixed state does not imply that the map is identity preserving since input and output have different dimensions in general.

Now we can easily prove the needed implication of the Observation 5.6. To see this note first that reliable transmission with help of above protocol means that the *generalised singlet fraction* $F(\sigma_n)$:

$$F(\sigma_n) = \langle \Psi_+^{k(n)} | \sigma_n | \Psi_+^{k(n)} \rangle \tag{17}$$

approaches unity in the limit of large n. Now for one-way scenario ($C = \rightarrow$) the map $\Lambda^{(n)}$ can be decomposed in a new form:

$$\Lambda^{(n)} = \sum_{\mathbf{k}} \Lambda_{\mathbf{k}}^B \circ \Lambda^{\otimes n} \circ \Lambda_{\mathbf{k}}^A \tag{18}$$

where $\Lambda_{\mathbf{k}}^A(\cdot) = V_{\mathbf{k}}(\cdot)V_{\mathbf{k}}^\dagger$ is a *local filtering* operation ($V_{\mathbf{k}}^\dagger V_{\mathbf{k}} \leq I$) while $\Lambda_{\mathbf{k}}^B$ is *tracepreserving*. This is because Bob can not perform any selection process since he must not inform Alice about it (classical information can flow only form Alice to Bob and not vice versa). The separable superoperator formalism can be easily applied to the new decomposition (18). Convexity of the entanglement fidelity F followed by simple calculation leads to the conclusion that for some $\mathbf{k}$ one must have:

$$F(\varrho_n') \equiv F\left(\frac{[\overline{\Lambda}_{\mathbf{k}}^A \otimes \Lambda_{\mathbf{k}}^B](\varrho(\Lambda))^{\otimes n}}{Tr([\overline{\Lambda}_{\mathbf{k}}^A \otimes \Lambda_{\mathbf{k}}^B](\varrho(\Lambda))^{\otimes n})}\right) \stackrel{n\to\infty}{\longrightarrow} 1 \tag{19}$$

where $\overline{\Lambda}_{\mathbf{k}}^A(\cdot) = [\sqrt{\frac{(d_A)^n}{m(n)}} V_{\mathbf{k}}]^*(\cdot)[\sqrt{\frac{(d_A)^n}{m(n)}} V_{\mathbf{k}}]^T$. Now one can always find some positive constant $\delta > 0$ such that new completely positive map $\delta\overline{\Lambda}_{\mathbf{k}}^A(\cdot)$ is again legitimate local filtering on Alice side. This means that given large number of states $\varrho(\Lambda)$ Alice and Bob can produce probabilistically in one way scenario (since Bob action is tracepreserving) entangled state with arbitrary high fidelity. Now the standard argument combining the above probabilistic scheme with local projections and one-way schemes (i) $U \otimes U^*$ twirling and (ii) hashing protocol achieves finally nonzero distillation rate $D_C > 0$.

For two-way schemes the above reasoning can be just rewritten with the only change of $\mathbf{m}$ back to $\mathbf{k}$ in (18). This turns both Alice and Bob elementary actions into filtering and makes the subsequent protocol two-way. This concludes our proof.

Note that the latter, as it is, it does not generalise to the case $C = \leftarrow$ since in that case any Alice action $\Lambda_{\mathbf{k}}$ in (12) is *tracepreserving* but its counterpart $\overline{\Lambda}_{\mathbf{k}}$ in separable superoperator scheme (14) fails to have that property in general (it is identity preserving). The same problem concerns the case when $C = \emptyset$.

Consider now channels for which *nonzero transmission can be achieved with Alice actions* $\Lambda_{\mathbf{k}}$ *that preserve maximally mixed state*. It is remarkable that for such channels the Observation 5.1 generalises also to resources $C = \leftarrow, \emptyset$.

It is interesting to ask about an example where the rates in Observation 5.6 are optimal ie. when the capacity of Λ is equal to the corresponding entanglement distillation of the state $\varrho(\Lambda)$. An elementary example here is Λ defied as a product of ideal channel and maximally depolarising channel. Application of computable capacity bound [24]

immediately shows that tensor product of the two channels has capacity of the ideal channel that is a part of the product. Now local actions (on both Alice and Bob side) that correspond to optimal distillation scheme are just partial traces. They both preserve maximally mixed state.

6 Quantum capacity after erasure of single channel copy

Consider an arbitrary channel $\Lambda : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ with $dim\mathcal{H}_A = 2$ unknown to Alice and Bob. Following our Observation 5.1 if the channel has nonzero capacity $Q_{\leftrightarrow} > 0$ then the corresponding $2 \otimes (dim\mathcal{H}_B)$ state $\varrho(\Lambda)$ has nonzero distillable entanglement $\mathcal{D}_{\leftrightarrow}$. Let us note that the state $\varrho(\Lambda)$ can be produced by zero-way operation (sending half of singlet down the channel). The state is unknown but, following previous analysis, Alice and Bob can distill nonzero rate of singlets. Final teleportation of unknown qubits down the singlets achieves then nonzero two-way capacity of the channel Λ. Similarly, all the discussion concerning one-way distillable entanglement previously performed can be *mutatis mutandis* applied to one-way capacity.

This concludes the result parallel to that obtained for $2 \otimes N$ states in one of previous paragraphs. The result can be immediately extended to general channels (that have no restriction on input and output dimensions) under the only condition that the corresponding state $\varrho(\Lambda)$ satisfies the condition (9) for n bounded form above by some constant.

Discussion and conclusions

We have considered the problem whether erasure of information about the state (channel) preserves the property of nonvanishing distillable entanglement (capacity). We have argued that for $2 \otimes N$ states and the corresponding quantum channels the erasure of single copy information does not nullify the two-way distillable entanglement and capacity respectively. For the case of one-way schemes the result still holds for some special one-way protocols (filtering plus hashing) under an additional assumption that Alice and Bob had prior tomography with help of two-way communication.

The universal $2 \otimes N$ protocol has a final rate insensitive under the erasure of information about single copy of the state (channel). Some generalisations to the case when Alice system has more levels than two are also possible.

To prove the corresponding results for channels we have utilised the states-channels isomorphism and proven rigorously the Observation 5.1 that nonzero Q_C with $C = \rightarrow, \leftrightarrow$ for given channel leads to nonzero distillable entanglement for the corresponding state. This completes the previous result of other authors and can be viewed as qualitative equivalence between distillable entanglement and quantum capacity for the two classical resources. It is an open problem whether the equivalence is true for resources $C = \leftarrow, \emptyset$ if Alice elementary actions do not preserve maximally mixed state.

Also, there is a general question about what happens in general one-way distilla-

tion schemes. Does one-way classical communication assumption inevitably make the equivalence impossible? One can expect positive answer, but the example is not known. Another question is: what if we forbid naive LOCC tomography and ask for "fully quantum" protocol ? The above questions deserve further investigation probably with more powerful mathematical tools.

Acknowledgments

The author thanks C. H. Bennett, R. Horodecki and M. Horodecki for discussions. The work is supported by the EU projects RESQ (IST-2001-37559) and QUPRODIS (IST-2001-38877).

References

[1] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin and W.K. Wootters: "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels", *Phys. Rev. Lett.*, Vol. 76, (1996), pp. 722-725.

[2] A. Ekert: "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.*, Vol. 67, (1991), pp. 661-663.

[3] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wootters: "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.*, Vol. 70, (1993), pp. 1895-1899.

[4] C.H. Bennett, D.P. Di Vincenzo, J. Smolin and W.K. Wootters: "Mixed-state entanglement and quantum error correction", *Phys. Rev. A*, Vol. 54, (1997), pp. 3824-3851.

[5] H. Barnum, E. Knill and M. Nielsen: "On quantum fidelities and channel capacities", *IEEE T. Inform. Theory*, Vol. 46, (2000), pp. 1317-1329.

[6] A. Albert et al.: *Quantum information: basic concepts and experiments*, Springer, Berlin, 2001.

[7] R.F. Werner: "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model", *Phys. Rev. A*, Vol. 40, (1989), pp. 4277-4281.

[8] E. Rains: "Rigorous treatment of distillable entanglement", *Phys. Rev. A*, Vol. 60, (1999), pp. 173-178.

[9] M. Horodecki, P. Horodecki and R. Horodecki: "Inseparable Two Spin- 1 / 2 Density Matrices Can Be Distilled to a Singlet Form", *Phys. Rev. Lett.*, Vol 78, (1997), pp. 574-577.

[10] M. Horodecki, P. Horodecki and R. Horodecki: "Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?", *Phys. Rev. Lett.*, Vol. 80, (1998), pp. 5239-5242.

[11] If the state of bipartite system is defined on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and $d_A = dim\mathcal{H}_A$, $d_B = dim\mathcal{H}_B$ then we deal with $d_A \otimes d_B$ system.

[12] A. Peres: "Separability Criterion for Density Matrices", *Phys. Rev. Lett.*, Vol. 77, (1996), pp. 1413-1415.

[13] B. Kraus: J.I. Cirac, S. Karnas, and M. Lewenstein: "Separability in 2N composite quantum systems", *Phys. Rev. A*, Vol. 61, (2000), 062302.

[14] D.P. DiVincenzo, P.W. Shor, J.A. Smolin, B. Terhal and A.W. Thapliyal: "Evidence for bound entangled states with negative partial transpose", *Phys. Rev. A*, Vol. 61, (2000), 062312;
D. Dür, J.I. Cirac, M. Lewenstein and D. Bruss: "Distillability and partial transposition in bipartite systems", *Phys. Rev. A*, Vol. 61, (2000), 062312.

[15] P.W. Shor, J.A. Smolin and B.M. Terhal: "Nonadditivity of Bipartite Distillable Entanglement Follows from a Conjecture on Bound Entangled Werner States", *Phys. Rev. Lett.*, Vol. 86, (2001), pp. 2681-2684.

[16] A. Jamiołkowski: "Linear transformations which preserve trace and positive semidefiniteness of operators", *Rep. Math. Phys.*, Vol. 3, (1972), pp. 275-278.

[17] R. Jozsa: "Fidelity for Mixed Quantum States", *J. Mod. Opt.*, Vol. 41, (1994), pp. 2315-2323.

[18] P. Horodecki, M. Horodecki and R. Horodecki: "Binding entanglement channels", *J. Mod. Opt.*, Vol. 47, (2000), pp. 347-354;
D. DiVincenzo, T. Mor, P. Shor, J. Smolin, and B.M. Terhal: "Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement", *Commun. Math. Phys.*, Vol. 238, pp. 379-410.

[19] P. Horodecki: "On Mixed States Entanglement and Quantum Communication: Aspects of Quantum Channels Theory", *Acta Phys. Polon.*, Vol. 101, (2002), pp. 339.

[20] P. Horodecki, M. Horodecki and R. Horodecki: "Bound Entanglement Can Be Activated", *Phys. Rev. Lett.*, Vol. 82, (1999), pp. 1056-1059.

[21] T. A. Brun, C. M. Caves, R. Schack: "Entanglement purification of unknown quantum states", *Phys. Rev. A*, Vol. 63, (2001), (PRA 63 0402309).

[22] Here, in general $\vec{p} \in R^{15}$ since two qubit density matrix is described by 15 parameters. In analysis of hashing of Bell diagonal states [21] effectively one can choose $\vec{p} \in R^3$ since Bell diagonal states depend effectively on 3 parameters.

[23] G.M. D'Ariano, M.G.A. Paris, M.F. Sacchi: "Quantum Tomography", (quant-ph/0302028), http://arxiv.org/abs/quant-ph/0302028.

[24] A.S. Holevo and R.F. Werner: "Evaluating capacities of bosonic Gaussian channels", *Phys. Rev. A*, Vol. 63, (2001), (PRA 63 032312).

[25] C.A. Fuchs, J. van de Graaf: "Cryptographic Distinguishability Measures for Quantum Mechanical States", (quant-ph/9712042), http://arxiv.org/abs/quant-ph/9712042.

[26] P. Horodecki, PhD thesis, Technical University of Gdansk, Gdansk 1999.

[27] N. Gisin: "Hidden quantum nonlocality revealed by local filters", *Phys. Lett. A*, Vol. 210, (1996), pp. 151-156.