PHYSICAL REVIEW A **77**, 060307(R) (2008)

Entanglement-swapping boxes and their communication properties

Andrzej Grudka,[1,2,3] Michał Horodecki,[1,2] Paweł Horodecki,[2,4] Ryszard Horodecki,[1,2] and Marco Piani[1,4,*]
[1]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[2]*National Quantum Information Centre of Gdańsk, 81-824 Sopot, Poland*
[3]*Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland*
[4]*Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-952 Gdańsk, Poland*
(Received 26 June 2007; revised manuscript received 15 January 2008; published 18 June 2008)

We pose the fundamental question of communication properties of primitives irrespectively of their implementation. To illustrate the idea we introduce the concept of entanglement-swapping boxes, i.e., we consider any quantum operations which perform entanglement swapping, not necessarily via simple quantum teleportation. We ask a question about the properties of such boxes, i.e., what local operations and how much classical communication are needed to perform them. We also ask if any box which performs entanglement swapping can be used to establish classical communication. We show that each box needs at least two bits of classical communication to perform it. It is also shown that each box can be used for classical communication and, most importantly, that there exist boxes which allow one to communicate at most one bit. Surprisingly we find basic irreversibility in the process of entanglement swapping with respect to its classical communication properties.

DOI: 10.1103/PhysRevA.77.060307 PACS number(s): 03.67.Hk, 03.65.Ud

Classical communication properties of quantum bipartite operations have recently been studied ([1,2], and references therein). More precisely, the amount of classical communication (bits) that two parties can exchange by exploiting a given bipartite operation was estimated. The converse question, how much classical communication a given bipartite operation requires to be implemented, was also addressed [3].

However, as far as we know, only communication properties of specifically implemented bipartite quantum operations—completely positive trace-preserving maps—have been analyzed (e.g., one considers a particular protocol and asks the questions: *How much communication is needed to perform it? How much communication classical or quantum can be established with it?*)

In this Rapid Communication we ask another fundamental question: *What are the communication properties of fundamental tasks, or primitives, irrespectively of their implementation?* Indeed, it is often useful to formulate information processing in terms of primitives rather than via specific realizations (e.g., a particular protocol).

In general, one can consider "black boxes"—quantum operations whose details we may not know—which realize a primitive, and analyze the requirements of their inner implementation (the general structure of protocols, i.e., basic quantum operations which can be used such as unitaries, projectors and so on). We investigate for what other tasks they can serve (e.g., if they can be used to establish classical communication). We calculate how much classical communication one needs to implement a particular box and how much classical communication one can establish with this box. We stress that the box is designed to perform some precise task and the possibility of establishing classical communication is only a bonus. We investigate if any box can give us such a bonus, e.g., if there are worst cases where classical communication is not possible at all.

As an example of general interest in the just described framework we introduce the concept of entanglement-swapping (ES) boxes associated to entanglement swapping [4,5]. Entanglement swapping is a process where quantum correlations are distributed by means of (tripartite) local operations and classical communication (LOCC), and it is fundamental for, e.g., long-distance quantum communication based on quantum repeaters [6]. We define the *communication cost* (CC) and the *communication value* (CV) of a *particular* box, i.e., one of the many possible boxes which realize a certain primitive, as the least amount of communication required to implement the box, and allowed by the box itself, respectively [16]. We further define the CC (CV) of a primitive as the minimal CC (CV) over all boxes realizing the primitive, i.e., as the minimal communication that we have to spend to realize (that we can obtain from) *any* black box that we know to perform the primitive. Surprisingly, we show that communication has to be spent to perform a primitive that can be established with it. Hence the process of ES is in general irreversible with respect to classical communication. A similar irreversibility occurs for Popescu-Rohrlich boxes [7], where one needs one bit of classical communication to establish correlations, however this bit cannot be used to send a message, i.e., Popescu-Rohrlich boxes are nonsignaling [3,8–12].

We also report results about boxes associated to other primitives, namely two intermediate steps of ES: creating a GHZ state from two Bell states and creating a Bell state

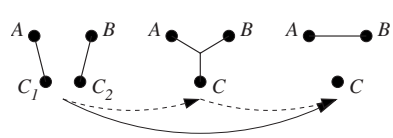

FIG. 1. Entanglement swapping (continuous arrow) in two steps (dashed arrows): from two EPR pairs to a GHZ state, to the final EPR pair. Lines denote quantum correlations.

*Present address: Institute for Quantum Computing, University of Waterloo, Waterloo ON, Canada.

 ©2008 The American Physical Society

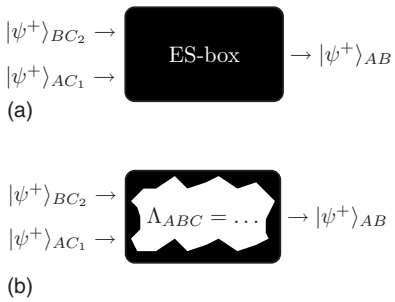

FIG. 2. Entanglement swapping (black) box. (a) Defining action of an ES box. Time goes from left to right. (b) Actual (LOCC) implementation of a given ES box.

between any two parties starting from a GHZ state (Fig. 1).

Imagine that Alice and Bob share maximally entangled states $|\Psi^+\rangle_{AC_1}$ and $|\Psi^+\rangle_{AC_2}$ with (two subsystems of) Charlie. ES corresponds to obtaining, from such initial resource, a state $|\Psi^+\rangle_{AB}$, by LOCC. We define a (black) ES box to be any tripartite-LOCC operation such that ES takes place upon the input of $|\Psi^+\rangle_{AC_1}|\Psi^+\rangle_{BC_2}$ [see Fig. 2(a)]. We will typically refer to the AB output alone, disregarding the output subsystems of Charlie, i.e., effectively tracing them out.

Because of the characterization of all ES boxes we will provide, the CC and the CV will be analyzed with respect to the relevant direction $C \to AB$. If not differently stated, we will allow Alice and Bob to act together when considering the CV. Indeed, while the box is assumed to be (in its *implementation*) tripartite LOCC, this does not force the *users* to have the same limitation. Alternatively, one could think of entanglement between Alice and Bob being consumed while trying to obtain a signal from Charlie by means of the box.

We may imagine that a provider, Paul, sells ES boxes—a tool to process some precious resource such as preshared entanglement—to the users Alice, Bob, and Charlie. Suppose now that Paul wants to minimize the use of the boxes for any other purpose than just entanglement swapping. In particular, he might like to prevent the parties from using the box to communicate. Thus, he tries to minimize the CV of the box. On the other hand, he would like to build the box in the cheapest way, hence he tries to minimize the CC of the box. Among all ES boxes, we will be interested in the best possible boxes from the point of view of the provider, i.e., the ones with the minimal CC and CV, therefore in the CC and CV of the primitive as defined above.

We start by noticing that any ES box Λ_{ABC} is *signaling* with respect to $C \to AB$ [3,12]. In order to see this, we have to show that there exist some initial state ϱ_{ABC} and (at least two) operations on Charlie's subsystem $\{\Gamma_C^i\}$ such that the states $\varrho_{AB}^i = \Lambda_{ABC}[\Gamma_C^i(\varrho_{ABC})]$ are different. To communicate by means of the state ϱ_{ABC} and of the box Λ_{ABC}, (i) Charlie applies one operation Γ_C^i depending on the "letter" he wants to send, (ii) the parties let the box act, and finally (iii) Alice and Bob try to guess which state ϱ_{AB}^i they have. If the states ϱ_{AB}^i are different, the box has nonzero CV. Let us choose the initial state $|\Psi^+\rangle_{AC_1}|\Psi^+\rangle_{BC_2}$, and as Charlie's possible operations the identity and the measurement of his two qubits performed in the computational basis. If Charlie applies the identity—does nothing—then, by definition of the ES box, Alice and Bob obtain as output the state $|\Psi_{AB}^+\rangle$. On the other hand, the measurement by Charlie destroys all the entanglement between the parties, that cannot be restored by the LOCC ES box, thus Alice and Bob can at most obtain a separable state.

We now proceed with a specific example of the ES box. As our tripartite LOCC map we take *any* LOCC teleportation protocol [4] from Charlie to Alice, i.e., such that an input state $|\Psi^+\rangle_{AC_1}|\psi\rangle_B|\phi\rangle_{C_2}$ is transformed into $|\phi\rangle_A|\psi\rangle_B$, for all $|\phi\rangle$. This particular ES box has CV equal to 2 via dense coding [13], even considering just one final receiver, i.e., $C \to A$. Indeed, one can consider an initial state $|\Psi^+\rangle_{AC_1}|\psi\rangle_B|\Psi^+\rangle_{A'C_2}$ involving a local ancilla A' of Alice that is maximally entangled with C_2. Charlie can locally rotate the pair $|\Psi^+\rangle_{A'C_2}$ into one of four orthogonal Bell states, which is fully in the hands of Alice after teleportation. If we choose the standard teleportation protocol, a Bell measurement at the sender followed by a proper unitary rotation at the receiver, the CC is 2, and it could not be anyway less because of causality [4].

As we will show, there are ES boxes which have CV equal to 1. Then the simple argument of causality cannot be used to prove that their CC is greater or equal to 2. Anyway, we will show that every ES box has CC greater or equal to 2. Thus, there are ES boxes which exhibit communication irreversibility: the box needs more bits to be implemented than it can signal.

In the theorem below we characterize all LOCC maps that perform entanglement swapping, i.e., every "internal implementation" of ES boxes [Fig. 2(b)].

Theorem 1. Any ES box Λ_{ABC} is of the form $\Lambda(\varrho_{ABC}) = \mathrm{Tr}_C(\Sigma_i U_A^i U_B^i E_C^i(\varrho_{ABC}) U_A^{i\dagger} U_B^{i\dagger} E_C^{i\dagger})$, where U_A^i and U_B^i are unitary operations and $E_C^i = |u^i\rangle\langle\psi_+^i|$ are rank-one measurement operators, with $|\psi_+^i\rangle$ normalized maximally entangled states of Charlie's particles, which satisfy $\Sigma_i E_C^{i\dagger} E_C^i = \Sigma_i \|u_i\|^2 |\psi_+^i\rangle\langle\psi_+^i| = \mathbb{1}_{C_1C_2}$.

Proof. We provide here only a sketch of the full proof [15], which consists of two parts. In the first part (I) we prove that Alice and Bob cannot perform nonunitary operations. In the second part (II) we find the conditions which have to be satisfied by Charlie's operators.

(I) We will prove this part by contradiction. Every LOCC protocol corresponds to rounds of local actions coordinated by classical communication, by means of which the results of the local operations are transmitted to the other parties. Without loss of generality, let Alice be the first, between her and Bob, to perform an operation different from an isometry. The initial entanglement in the $A|BC$ splitting corresponds to one ebit, and the same holds at the end of the protocol by the ES condition. As the protocol is LOCC, there must be one ebit of $A|BC$ entanglement at every step. One can prove that any operation by Alice that were not an isometry would violate such a condition. Therefore, neither Alice nor Bob can perform any other operation but isometries. Since their output subsystems correspond to their input subsystems, such isometries are indeed unitaries.

(II) Charlie is initially maximally entangled with Alice and Bob. At the end, Alice and Bob, who both can perform only unitary operations, have a pure state. Therefore, Charlie

MOST WIEDZY Downloaded from mostwiedzy.pl

has to disentangle his qubits from Alice and Bob's, i.e., he has to perform a measurement with measurement operators of rank 1: $E_C^i = |u^i\rangle\langle\psi^i|$, with $|\psi^i\rangle$ a normalized state. The output state of Alice's and Bob's subsystem corresponding to a given E_C^i has the same Schmidt coefficients as $|\psi^i\rangle$. Thus, we see that Alice and Bob may obtain a maximally entangled state only if $|\psi^i\rangle$ is maximally entangled. ■

We can now address the problem of the CC of ES boxes. Indeed, given the standard form for ES boxes of Theorem 1, it is clear that all ES boxes can be realized with only $C \to AB$ classical communication, which is used by Charlie to tell Alice and Bob the result of his measurement, so that they can apply the correct local unitary rotations. We will need the entropic quantities $S(A|B) = S(AB) - S(B)$ (conditional entropy), $I(A:B) = S(A) + S(B) - S(AB)$ (mutual information), $I(A:B|R) = S(A|R) + S(B|R) - S(AB|R)$ (conditional mutual information), where for brevity we use the notation $S(X) = S(\varrho_X)$, etc., and the following lemma.

Lemma 1. Consider an ensemble $\{p^i, \varrho_{AB}^i\}$, and the corresponding average state $\varrho_{AB} = \Sigma_i p^i \varrho_{AB}^i$. Then $\Delta I \leqslant \Delta S$, where $\Delta I = \Sigma_i p^i I(\varrho_{AB}^i) - I(\varrho_{AB})$ is the average increase of mutual information, and $\Delta S = S(\varrho_{AB}) - \Sigma_i p^i S(\varrho_{AB}^i)$ is the average decrease of entropy, when Alice and Bob come to know the index of the state they actually share among the ones in the ensemble.

Proof. Let us introduce an ancilllary system R and consider the tripartite state $\varrho_{ABR} = \Sigma_i p^i \varrho_{AB}^i \otimes |i\rangle_R\langle i|_R$, with orthogonal $|i\rangle_R$ on R. Note that $\Delta I = I(A:B|R) - I(A:B)$ and $\Delta S = I(AB:R)$, with the right-hand sides of these equalities calculated with respect to ϱ_{ABR}. We therefore have

$$\Delta I - \Delta S = -I(A:R) - I(B:R) \leqslant 0, \tag{1}$$

because of positivity of mutual information. ■

The number of bits sent by Charlie to Alice and Bob per each realization of an ES box can not be less than the Shannon entropy $H(\{p_i\}) = -\Sigma_i p_i \log_2 p_i$ of the probability distribution of the outcomes of Charlie.

Theorem 2. Any ES box has CC at least equal to 2.

Proof. After Charlie's measurement, Alice and Bob have an ensemble $\{p^i, \varrho_{AB}^i\}$. Each ϱ_{AB}^i is a (different) maximally entangled state, and $\varrho_{AB} = \Sigma_i p^i \varrho_{AB}^i = \mathbb{1}_4/4$ corresponds to Alice and Bob's initial reduced state. From Lemma 1 we have

$$H(\{p_i\}) \geqslant S(\varrho_{AB}) - \sum_i p^i S(\varrho_{AB}^i) \geqslant \sum_i p^i I(\varrho_{AB}^i) - I(\varrho_{AB}) = 2. \tag{2}$$

■

Since we know that for the standard teleportation map the CC is equal to 2, by using Theorem 2 we obtain that CC of ES is equal to 2.

Let us now consider the CV of an ES box: the theorem below gives a lower bound valid for all ES boxes.

Theorem 3. Any ES box has CV at least equal to 1.

Proof. One can check that if the initial state ϱ_{ABC} is $|\Psi^+\rangle_{AC_1}|\Psi^+\rangle_{BC_2}$, and Charlie's possible operations $\{\Gamma^i\}$ before the ES box correspond to the set of unitaries $S = \{\mathbb{1}_{C_1} \otimes \mathbb{1}_{C_2}, Z_{C_1} \otimes \mathbb{1}_{C_2}\}$, then the states $\{\varrho_{AB}^i = \Lambda_{ABC}[\Gamma_C^i(\varrho_{ABC})]\}$ are orthogonal and can be perfectly distinguished by Alice and Bob. ■

It should be emphasized that, in order to communicate, Charlie can apply operations $\{\Gamma^i\}$ that do not depend on the ES box, so that communication is achieved whatever the *black* ES box [see Fig. 2(a)] at disposal, i.e., the internal structure of the box—the particular LOCC map Λ_{ABC}—is not relevant. We now prove that the bound CV=1 can be achieved. The maps we provide to this purpose happen to be also $C \to A$ and $C \to B$ *nonsignaling*, i.e., Charlie cannot communicate to neither Alice nor Bob separately. We will use the standard bipartite operation of UU^*-twirling $\Lambda_{AB}^T(\sigma_{AB}) \equiv \int dU (U_A \otimes U_B^*)\sigma_{AB}(U_A \otimes U_B^*)^\dagger$, where $\int dU$ denotes integration over the unitary group with respect to the Haar measure, and U^* is the complex conjugate of U.

Theorem 4. Apply the UU^* twirling to the output of any ES box Λ_{ABC}: the resulting map is again an ES box, with CV equal to 1, and nonsignaling with respect to $C \to A$ and $C \to B$.

Proof. Consider the map $\tilde{\Lambda}_{ABC} = \Lambda_{AB}^T \circ \Lambda_{ABC}$. $\tilde{\Lambda}_{ABC}$ is obviously an ES box, since Λ_{AB}^T leaves $|\Psi^+\rangle$ invariant. To provide an upper bound that takes care of the possibility of exploiting preestablished quantum correlations, on the CV of $\tilde{\Lambda}_{ABC}$ we use the entanglement-assisted classical capacity of a quantum channel (EACCQC) [14]. Consistently with the idea of obtaining an upper bound, we apply the formula for EACCQC by pretending that Charlie has complete control over all the input—not only on its subsystem, so that it reads

$$C(\tilde{\Lambda}_{ABC}) = \max_{\varrho_{ABC}}[S(\varrho_{ABC}) + S(\tilde{\Lambda}_{ABC}(\varrho_{ABC})) - S((\tilde{\Lambda}_{ABC} \otimes \mathrm{id}_E)(\Phi_{ABCE}))], \tag{3}$$

where Φ_{ABCE} is any purification of ϱ_{ABC}, and the maximum is taken over all input states ϱ_{ABC}. For our channel we have $\tilde{\Lambda}_{ABC}(\varrho_{ABC}) = F|\Psi^+\rangle_{AB}\langle\Psi^+|_{AB} + \frac{1-F}{3}(\mathbb{1}_{AB} - |\Psi^+\rangle_{AB}\langle\Psi^+|_{AB})$ and $(\tilde{\Lambda}_{ABC} \otimes \mathrm{id}_E)(\Phi_{ABCE}) = F|\Psi^+\rangle_{AB}\langle\Psi^+|_{AB} \otimes \varrho_E^0 + \frac{1-F}{3}(\mathbb{1}_{AB} - |\Psi^+\rangle_{AB}\langle\Psi^+|_{AB}) \otimes \varrho_E^1$, with $0 \leqslant F \leqslant 1$. After some algebra, we obtain

$$C(\tilde{\Lambda}_{ABC}) = \max\{S[F\varrho_E^0 + (1-F)\varrho_E^1] - [FS(\varrho_E^0) + (1-F)S(\varrho_E^1)]\} \leqslant 1.$$

On the other hand, from Theorem 3 we know that any ES box has CV at least 1, therefore we find that the CV of $\tilde{\Lambda}_{ABC}$ is 1. Moreover, $\mathrm{Tr}_{B(A)}(\tilde{\Lambda}_{ABC}(\varrho_{ABC})) = \frac{1}{2}\mathbb{1}_{A(B)}$, for whatever ϱ_{ABC}, therefore $\tilde{\Lambda}_{ABC}$ is $C \to A(B)$ *nonsignaling*. ■

From Theorems 3 and 4 we conclude that ES has CV equal to 1. We note also that a map $\tilde{\Lambda}_{ABC}$, as defined in Theorem 4, has CC less or equal to that of the map Λ_{ABC} from which it derives. This follows from the fact that twirling can be performed without communication by means of shared randomness. We may take Λ_{ABC} to be standard teleportation, so that $\tilde{\Lambda}_{ABC}$ has CC equal to 2 and CV equal to 1. Thus both CC and CV of this specific ES box coincide with those of ES.

One may say that ES is an irreversible primitive from the point of view of classical communication, because the mini-

MOST WIEDZY Downloaded from mostwiedzy.pl

mal amount of communication required by any ES box is higher than the minimal amount of communication that we can expect to obtain from an ES box. Indeed, there are specific ES boxes which incarnate this irreversibility.

As a primitive, ES may be split into two subprimitives, or intermediate steps (Fig. 1): the transformation of two EPR pairs into a GHZ state, and of the latter into an EPR pair between any two subsystems. We remark that this does not mean that every ES box can be split correspondingly into two sub-boxes. By essentially the same methods used for the full ES, one can prove [15] that both the CC and CV of the second (sub)primitive are equal to 1, so that such primitive is *reversible* from the point of view of classical communication. With respect to the first subprimitive, one can show [15] that there exists a corresponding box which has CC equal to 1 and CV strictly less than 1. Moreover this subprimitive has CV strictly positive. In order to prove this last statement, let us notice that after the action of the box on $|\Psi^+\rangle_{AC_1}|\Psi^+\rangle_{BC_2}$, Alice and Bob's reduced density matrix is $\varrho_{AB}=\frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)$. We now argue that, before the box is applied, Charlie can transform the input state in such a way that the output of the box yields a different reduced density matrix for Alice and Bob. To this end, Charlie applies a random unitary operations which produce the state $\varrho_{ABC}=\frac{1}{4}I_{AB}\otimes\frac{1}{4}I_C$. As the (conditional) action of the box on Alice's and Bob's systems consists of unitary operations, it cannot change Alice's and Bob's reduced density matrix $\varrho_{AB}=\frac{1}{4}I_{AB}$, which commutes with all unitaries. Since CV for the first subprimitive is strictly greater than 0 and CV for the second subprimitive as well as for the "composed" ES box is equal to 1, we conclude that CV for primitives is strictly subadditive. On the other hand, CC is additive.

In this article we have considered communication properties of primitives irrespectively of their implementation. We exemplified this by introducing the concept of entanglement-swapping boxes, and characterizing them with respect to LOCC operations. We studied their classical-communication properties, and discovered a phenomenon of irreversibility of the primitive itself: it needs more bits to be implemented than it can signal. We also reported results of a similar analysis for primitives corresponding to intermediate steps of entanglement swapping. We believe that studying communication properties of primitives will lead to a better understanding of the interplay between the quantum and the classical, at the level both of properties and of interconversion of resources.

We thank K. Horodecki for useful discussions. This work was supported by the European Commission through the Integrated Project FET/QIPC "SCALA." A.G. was also supported by Grant No. 1 P03B 014 30 of the State Committee for Scientific Research.

[1] C. H. Bennett *et al.*, IEEE Trans. Inf. Theory **49**, 1895 (2003); A. W. Harrow and D. W. Leung, Quantum Inf. Comput. **5**, 380 (2005).
[2] A. M. Childs *et al.*, Int. J. Quantum Inf. **4**, 63 (2006).
[3] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, Phys. Rev. A **64**, 052309 (2001).
[4] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[6] H.-J. Briegel, W. Dur, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[7] S. Popescu and D. Rohrlich, e-print arXiv:quant-ph/9709026; Found. Phys. **24**, 379 (2001).
[8] J. Barrett *et al.*, Phys. Rev. A **71**, 022101 (2005).
[9] B. F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003).
[10] J. Degorre, S. Laplante, and J. Roland, Phys. Rev. A **72**, 062314 (2005).
[11] N. J. Cerf, N. Gisin, S. Massar, and S. Popescu, Phys. Rev. Lett. **94**, 220403 (2005).
[12] M. Piani, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **74**, 012305 (2006).
[13] C. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[14] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).
[15] A. Grudka, M. Horodecki, P. Horodecki, R. Horodecki, and M. Piani (unpublished).
[16] We will refer to the number of bits of communication required (allowed) in the asymptotic limit of many instances of the box to be implemented (exploited).

MOST WIEDZY Downloaded from mostwiedzy.pl