Locally accessible information and distillation of entanglement

Sibasish Ghosh,[1,*] Pramod Joag,[2,†] Guruprasad Kar,[3,‡] Samir Kunkri,[3,§] and Anirban Roy[4,||]
[1] *Department of Computer Science, The University of York, Heslington, York, YO10, United Kingdom*
[2] *Department of Physics, University of Pune, Ganeshkhind, Pune 411 007, India*
[3] *Physics and Applied Mathematics Unit, Indian Statistical Institute, 203, B. T. Road, Kolkata 700 108, India*
[4] *Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India*

(Received 24 March 2004; published 18 January 2005)

A different type of complementarity relation is found between locally accessible information and final average entanglement for a given ensemble. It is also shown that in some well-known distillation protocols, this complementary relation is optimally satisfied. We discuss the interesting trade-off between locally accessible information and distillable entanglement for some states.

DOI: 10.1103/PhysRevA.71.012321 PACS number(s): 03.67.Mn, 03.65.Ud, 03.67.Hk

The problem of local distinguishability of orthogonal quantum states has raised much interest in the arena of quantum information. Interestingly where any two pure orthogonal states can be distinguished locally [1], there exist more than two orthogonal states which cannot be distinguished by local operations and classical communication (LOCC) [2,3]. Again Eisert *et al.* [4] have studied how distillable entanglement is decreased with the loss of classical information about the ensemble. In the light of the above results, it is interesting to investigate the deep connection between classical and quantum information and extraction of classical information about the ensemble by local operations and classical communication.

In this regard, Badziąg *et al.* [5] found a universal Holevo-like upper bound on the locally accessible information. This bound involves not only local entropy but also initial average entanglement. In particular they have shown that for an ensemble $\mathcal{E}=\{p_x,\rho_x\}$, the locally accessible information (i.e., information of x, extractable by LOCC) is bounded by

$$I_{\rm acc}^{\rm LOCC} \leqslant n - \bar{E}, \tag{1}$$

where $n=\log_2 d_1 d_2$ for a $d_1 \otimes d_2$ system and $\bar{E}$ refers to any asymptotically consistent measure of the average entanglement of the ensemble. Now if one writes the inequality in the form $I_{\rm acc}^{\rm LOCC}+\bar{E}\leqslant n$, it shows some kind of complementarity relation between locally accessible information and the average entanglement. Various interesting results follow from this relation. Specifically Badziąg *et al.* [5] checked that given the dimensions of the systems what would be the ensemble that would saturate the bound. One can observe from this inequality that though there are extreme cases where $I_{\rm acc}^{\rm LOCC}=\log_2 d_1 d_2$, there cannot be the other extreme, viz., $\bar{E}=\log_2 d_1 d_2$, rather $\bar{E}\leqslant\min\{\log_2 d_1,\log_2 d_2\}$.

In this article we provide a modified inequality which involves not only the average entanglement of the initial ensemble $(\overline{E_i})$ but also the average entanglement of the final ensemble $(\overline{E_f})$. In other words, the amount of locally accessible information $I_{\rm acc}^{\rm LOCC}$ is bounded above by $n-\overline{E_i}-\overline{E_f}$, which can be rewritten in the following form:

$$I_{\rm acc}^{\rm LOCC} + \overline{E_f} \leqslant n - \overline{E_i}. \tag{2}$$

Thus for the given choice of ensemble (i.e., for fixed n and $\overline{E_i}$), there is a kind of complementarity between $I_{\rm acc}^{\rm LOCC}$ and the final average entanglement.

We shall prove the inequality (2) for one-way LOCC and conjecture it to be true in the multiway case also and will provide some simple examples to check the nice trade-off between the amount of locally accessible information and final average entanglement in the above-mentioned complementarity relation. It is worth noticing how this relation plays a role in the process of entanglement distillation.

Finally we will discuss some famous distillation protocols like hashing, breeding, and also the error-correcting protocol where our bound in inequality (2) saturates.

In the following we will provide a proof of inequality (2) for one-way LOCC. When a source prepares a state ρ_X where $X=0,\ldots,n$ with probabilities $p_0,\ldots,p_n$, the Holevo bound tells us that the maximal accessible information (how well the source state can be inferred) one can derive is bounded by the following limit:

$$I_{\rm acc} \leqslant S(\rho) - \sum_X p_X S(\rho_X),$$

where $\rho=\Sigma_X p_X \rho_X$ and $S(\,)$ is the von Neumann entropy. But we will be considering a more interesting problem. The source is emitting a bipartite state $\rho_X^{(AB)}$ where $X=0,\ldots,n$ with probabilities $p_0,\ldots,p_n$ and two particles A and B are given to two distant parties (Alice and Bob, say) who are trying to guess X by LOCC. We will be trying to derive the upper limit of accessible information by LOCC. As only LOCC is allowed, one among Alice and Bob has to start the protocol. Let Alice start it. Alice can look at it in the follow-

[*] Electronic address: sibasish@cs.york.ac.uk

[†] Electronic address: pramod@physics.unipune.ernet.in

[‡] Electronic address: gkar@isical.ac.in

[§] Electronic address: skunkri_r@isical.ac.in

[||] Electronic address: anirb@imsc.res.in

1050-2947/2005/71(1)/012321(5)/$23.00

ing manner. She gets the states $\mathrm{Tr}_B[\rho_X^{(AB)}]$ with probabilities $p_0,\ldots,p_n$ and she has to identify X. So she performs a measurement described by positive-operator-valued measure (POVM) elements $\{A_y\}=\{A_0,A_1,\ldots,A_m\}$ on her system and by this process the most information she can extract about X is limited by the Holevo bound, which is

$$I^{(A)} \leq S(\rho^{(A)}) - \sum_X p_X S(\rho_X^{(A)}),$$

where $\rho^{(A)}=\mathrm{Tr}_B[\rho^{(AB)}]=\mathrm{Tr}_B[\Sigma p_X\rho_X^{(AB)}]$ and $\rho_X^{(A)}=\mathrm{Tr}_B[\rho_X^{(AB)}]$. The above inequality can be rewritten in the following way:

$$I^{(A)} \leq \log_2 d_1 - \sum_X p_X E(\rho_X^{(AB)}) = \log_2 d_1 - \overline{E_i},$$

where d_1 is the dimension of the Hilbert space at Alice's side and E is any asymptotic entanglement measure. Here we used the fact that $S(\rho_X^{(A)}) \geq E(\rho_X^{(AB)})$ for any asymptotic entanglement measure E. We will define $\overline{E_i}=\Sigma_X p_X E(\rho_X^{AB})$ as the initial average entanglement. After Alice's extraction of information she communicates her result, say K, to Bob. The joint two-particle density matrix has transformed into

$$\frac{\left[A_K\otimes I\sum_X p_X\rho_X^{(AB)}A_K^\dagger\otimes I\right]}{\mathrm{Tr}\left(A_K\otimes I\sum_X p_X\rho_X^{(AB)}A_K^\dagger\otimes I\right)}=\sigma_K^{(AB)}$$

with probability $p_K=\mathrm{Tr}(A_K\otimes I\Sigma_X p_X\rho_X^{(AB)}A_K^\dagger\otimes I)$. Then Bob's state is transformed into $\sigma_K^{(B)}=\mathrm{Tr}_A\sigma_K^{(AB)}$ (which includes information about X accessible by Bob) with probability p_K.

Now we will be using some more notation. We define

$$\sigma_{KX}^{(AB)}=\frac{[A_K\otimes I\rho_X^{(AB)}A_K^\dagger\otimes I]}{\mathrm{Tr}(A_K\otimes I\rho_X^{(AB)}A_K^\dagger\otimes I)}$$

and $p_{KX}=\mathrm{Tr}[A_k\otimes I\rho_X^{(AB)}A_K^\dagger\otimes I]$.

It is now Bob's turn to perform the measurement depending on Alice's outcome (here K, say) to extract information about X. He performed a measurement with POVM elements $\{B_z\}=\{B_0,B_1,\ldots,B_l\}$ on his system to extract information about X on the ensemble

$$\sigma_K^{(B)}=\sum_X\frac{p_Xp_{KX}}{p_K}\mathrm{Tr}_A\sigma_{KX}^{(AB)},$$

which originated from Alice's Kth measurement outcome. The accessible information for Bob $I_K^{(B)}$ must be bounded above by the Holevo quantity $S(\sigma_K^{(B)})-\Sigma_X p'_{KX}S(\mathrm{Tr}_A\sigma_{KX}^{(AB)})$ where $p'_{KX}=(p_Xp_{KX})/p_K$. Thus we have

$$I_K^{(B)}\leq S(\sigma_K^{(B)})-\sum_X p'_{KX}S(\mathrm{Tr}_A\sigma_{KX}^{(AB)})$$

$$= S(\sigma_K^{(B)})-\sum_X p'_{KX}S\left[\mathrm{Tr}_A\left(\sum_i\lambda_i^{KX}|\psi_i^{KX}\rangle\langle\psi_i^{KX}|\right)\right]$$

(where $\Sigma_i\lambda_i^{KX}|\psi_i^{KX}\rangle\langle\psi_i^{KX}|$ is any decomposition of $\sigma_{KX}^{(AB)}$)

$$\leq S(\sigma_K^{(B)})-\sum_X p'_{KX}\sum_i\lambda_i^{KX}S(\mathrm{Tr}_A|\psi_i^{KX}\rangle\langle\psi_i^{KX}|)$$

(by using concavity of von Neumann entropy)

$$=S(\sigma_K^{(B)})-\sum_X p'_{KX}\sum_i\lambda_i^{KX}E_v(|\psi_i^{KX}\rangle\langle\psi_i^{KX}|)$$

$[E_v(|\psi_i^{KX}\rangle\langle\psi_i^{KX}|)$ is the measure of entanglement of $|\psi_i^{KX}\rangle$ given by the von Neumann entropy $S(\mathrm{Tr}_A|\psi_i^{KX}\rangle\langle\psi_i^{KX}|)]$,

$$\leq S(\sigma_K^{(B)})-E_F(\sigma_K^{(AB)})$$

(by the definition of entanglement of formation E_F)

$$\leq S(\sigma_K^{(B)})-E'(\sigma_K^{(AB)})$$

(where E' is any asymptotic measure of entanglement and is smaller than the entanglement of formation)

$$\leq\log_2 d_2-E'(\sigma_K^{(AB)}),$$

where d_2 is the dimension of Hilbert space at Bob's side.

The total bound on Bob's extractable information is $I^{(B)}$ where $I^{(B)}\leq\Sigma_K p_K I_K^{(B)}$, which can be rewritten as

$$I^{(B)}\leq\sum_K p_K\log_2 d_2-\sum_K p_K E'(\sigma_K^{(AB)}),$$

where $\Sigma_K p_K E'(\sigma_K^{(AB)})$ is the average entanglement before Bob's measurement. Let $\overline{E_f}$ be the final average entanglement (using the same measure of entanglement E') after Bob's measurement, and as the average entanglement can only decrease by LOCC, therefore

$$I^{(B)}\leq\sum_K p_K\log_2 d_2-\sum_K p_KE'(\sigma_K^{(AB)})\leq\log_2 d_2-\overline{E_f}.$$

So in this one-way protocol the total locally accessible information satisfies the following relation:

$$I_{\mathrm{acc}}^{\mathrm{LOCC}}\leq I^{(A)}+I^{(B)}\leq\log_2 d_1+\log_2 d_2-\overline{E_i}-\overline{E_f}. \qquad (3)$$

Hence a complementarity relation has been established between locally accessible information and final average entanglement for a given ensemble. Now instead of Alice, if Bob had started the procedure, and depending on his outcome, if Alice performed the subsequent measurement, it is very easy to check that the inequality (3) will be of the same form. Only the actual values of $I_{\mathrm{acc}}^{\mathrm{LOCC}}$ and $\overline{E_f}$ can change. One can also notice here that the asymptotic measures of entanglement E and E', used above to define $\overline{E_i}$ and $\overline{E_f}$, respectively, are, in general, different. In some special cases, if all or some of the component states of the final ensemble generated by the LOCC are maximally entangled states, the process of extraction ofensemble information (locally) has also distilled some entanglement. Obviously the amount of entanglement ($E_{\mathrm{distilled}}$) that may be distilled in this process will satisfy $E_{\mathrm{distilled}}\leq\overline{E_f}$. So for every distillation process, we can also present a complementarity relation as follows:

$$I_{\mathrm{acc}}^{\mathrm{LOCC}}+E_{\mathrm{distilled}}\leq\log_2 d_1d_2-\overline{E_i}.$$

If for some cases, $E_{\mathrm{distilled}}=E_d$ (distillable entanglement) then this process of extraction of locally accessible information is itself the best distillation process.

First we will provide some simple examples (of course avoiding those discussed elsewhere [2]) to find the implication of our inequality [inequality (2)].

Example 1. Consider the following example where the source is producing any one of the states ρ_X, which are three copies of Bell states, $X=1,2,3,4$, with probability $p_X=1/4$, i.e., Alice and Bob have the ensemble $\mathcal{E}=\{p_X=1/4,\rho_X=(|B_X\rangle\langle B_X|)^{\otimes 3}\}$. Here $|B_X\rangle$ are known Bell states $|B_1\rangle=(1/\sqrt{2})(|00\rangle+|11\rangle)$, $|B_2\rangle=(1/\sqrt{2})(|00\rangle-|11\rangle)$, $|B_3\rangle=(1/\sqrt{2})\times(|01\rangle+|10\rangle)$, $|B_4\rangle=(1/\sqrt{2})(|01\rangle-|10\rangle)$. Now the maximum amount of information about X one can extract locally (or globally also) is 2 classical bits (cbits) (i.e., $I_{\text{acc}}^{\text{LOCC}}=2$; see [1,9]). Hence the final average entanglement $\overline{E}_f$ is bounded above by $\log_2 d_1d_2-\overline{E}_i-I_{\text{acc}}^{\text{LOCC}}=6-3-2=1$. By using two copies of the Bell states one can know the Bell state and therefore with the remaining copy, finally one can distill 1 ebit. But there is a process given by Chen *et al.* [6] by which one can extract 2 ebits; then our inequality [inequality (2)] shows that the extractable information $I_{\text{acc}}^{\text{LOCC}}$ is bounded by 1. Using inequality (11) of Chen *et al.* [6] one can easily check that $I_{\text{acc}}^{\text{LOCC}}=1$, which also saturates our bound [7].

One can generalize this process for n copies of Bell states, where n is odd, i.e., the source is producing a state which is n copies of one of the four Bell states with probability 1/4. The distillable entanglement is $(n-1)$ ebit [6]. When one distills this amount of entanglement, $I_{\text{acc}}^{\text{LOCC}}$ can be at most 1 cbit [from (2)]. But if one tries to extract the maximum amount of classical information about the ensemble, i.e., 2 cbits, the amount of entanglement one can distill is at most $(n-2)$ ebit. This can be achieved by using two copies of Bell states for reliable discrimination and the remaining $(n-2)$ copies produce $(n-2)$ ebits.

Example 2. Another interesting example is $\{p_X=1/4,\ \rho_X=(|B_X\rangle\langle B_X|)^{\otimes 4}\}$, $X=1,\ldots,4$. Here $\log_2 d_1d_2=8$, $\overline{E}_i=4$, the maximum allowed value of $I_{\text{acc}}^{\text{LOCC}}$ is 2; and hence $\overline{E}_f$ is boundedabove by 2 which is equal to the entanglement one can distill by locally discriminating four Bell states using two copies. For this ensemble the distillable entanglement E_D is also 2 ebits [6].

For all even cases, as the distillable entanglement is $(n-2)$ [6], here the extraction of the full 2 bits of classical information is the best distillation process, unlike in the odd case.

Example 3. We now take examples in a $3\otimes 3$ system. Take two copies of all nine maximally entangled states each of which is in the canonical form given by Eq. (4) below with equal probability,

$$|\Phi_{pq}^{(3)}\rangle=\frac{1}{\sqrt{3}}\sum_{j=0}^{2}\exp\left(\frac{2\pi ijp}{3}\right)|j\rangle\otimes|(j+q)\text{mod }3\rangle, \quad (4)$$

where $p,q=0,1,2$. Here $n=\log_2 d_1d_2=\log_2 81=4\log_2 3$, and $\overline{E}_i$ is $2\log_2 3$. So if $I_{\text{acc}}^{\text{LOCC}}$ is $2\log_2 3$ (which is the maximum that one can achieve by LOCC [9]), $\overline{E}_f$ is 0. In another possibility, $\overline{E}_f$ can become $\log_2 3$. Then from our inequality [inequality (2)], $I_{\text{acc}}^{\text{LOCC}}\leqslant\log_2 3$. In the case where $I_{\text{acc}}^{\text{LOCC}}=\log_2 3$ we show that the amount of entanglement that can be distilled is $\log_2 3$. We know from the work of Yang *et al.* [8] that the amount of distillable entanglement of $\rho_3^{(2)}=(1/9)\Sigma_{p,q=0}^{2}(|\Phi_{pq}\rangle\langle\Phi_{pq}|)^{\otimes 2}$ is $\log_2 3$. Applying a bilateral controlled-NOT operation, the ensemble $\rho_3^{(2)}$ transforms into $\frac{1}{3}[|\Phi_{00}\rangle\langle\Phi_{00}|\otimes\Sigma_r|\Phi_{0r}\rangle\langle\Phi_{0r}|+|\Phi_{10}\rangle\langle\Phi_{10}|\otimes\Sigma_r|\Phi_{2r}\rangle\langle\Phi_{2r}|+|\Phi_{20}\rangle\langle\Phi_{20}|\otimes\Sigma_r|\Phi_{1r}\rangle\langle\Phi_{1r}|]$. Now one discriminates locally between subspaces spanned by $\{|00\rangle,|11\rangle,|22\rangle\}$, $\{|01\rangle,|12\rangle,|20\rangle\}$, and $\{|02\rangle,|10\rangle,|21\rangle\}$ and extracts $I_{\text{acc}}^{\text{LOCC}}=\log_2 3$ and at the same time distills $\log_2 3$ ebit entanglement.

All the above examples show that whenever the state has some distillable entanglement, some amount of entanglement may be distilled in the process of extracting information about the ensemble. In some cases like Example 1 and Example 3 extracting full information about the ensemble reduces the amount to be distilled, but if one extracts somewhat less information, the amount to be distilled reaches the distillable entanglement.

We now turn to a $d\otimes d$ system. In $d\otimes d$, there are d^2 pairwise orthogonal maximally entangled states which can be written as $|\Phi_{pq}^{(d)}\rangle=(1/\sqrt{d})\Sigma_{j=0}^{d}\exp(2\pi ijp/d)|j\rangle\otimes|(j+q)\text{mod d}\rangle,p,q=0,\ldots,d-1$. These states can be discriminated either by providing two copies of each state [9] or by sharing an additional amount of $\log_2 d$ ebits of entanglement [10]. These also follow from our bound. We also show that after having classical information no entanglement will remain finally. As in the previous example here $I_{\text{acc}}^{\text{LOCC}}=2\log_2 d$, $n=4\log_2 d$, $\overline{E}_i=2\log_2 d$. So $\overline{E}_f\leqslant 0$. So finally no entanglementis there. Similarly for the case when one copy is supplied and $\log_2 d$ amount of entanglement is also supplied, i.e., a known maximally entangled state in $d\otimes d$ is supplied, the final average entanglement becomes zero after discrimination.

Next we shall study the inequality (2) in the context of some famous distillation processes like hashing, breeding, and the error-correction protocol. In a distillation protocol like hashing or breeding, the main idea is the same as the classical problem of identifying a word for a given probability distribution of the alphabets which constitute the word.

In the breeding protocol [11,12], a sufficiently large number of copies of the Bell diagonal state $\rho_B=\Sigma_{i=1}^{4}p_i|B_i\rangle\langle B_i|$, with corresponding Shannon entropy [i.e., $H(p_i)=-\Sigma_i p_i\log_2 p_i$] less than 1, are considered. We are also supplied with $nH(p_i)$ copies of a predistilled maximally entangled state. The n copies of the Bell states (ρ_B) form the string $|B_{i_1}\rangle\langle B_{i_1}|\otimes|B_{i_2}\rangle\langle B_{i_2}|\otimes|B_{i_3}\rangle\langle B_{i_3}|\otimes\cdots\otimes|B_{i_n}\rangle\langle B_{i_n}|$ with probability $p_{i_1}p_{i_2}p_{i_3}\cdots p_{i_n}$, and our job is to identify this string by using the predistilled states. So finally one gets n maximally entangled states. For this problem $I_{\text{acc}}^{\text{LOCC}}=nH(p_i)$ (as the total number of different strings like $|B_{i_1}\rangle\langle B_{i_1}|\otimes|B_{i_2}\rangle\times\langle B_{i_2}|\otimes|B_{i_3}\rangle\langle B_{i_3}|\otimes\cdots\otimes|B_{i_n}\rangle\langle B_{i_n}|$ that can be identified by the protocol is $2^{nH(p_i)}$ in the asymptotic limit), $\overline{E}_i=n[1+H(p_i)]$, $\log_2 d_1d_2=2n[1+H(p_i)]$, and $\overline{E}_f=n$. Here one can see the saturation of the bound given in inequality (2), in the asymptotic limit.

In the hashing protocol [11,12], the string is identified, or equivalently the classical information is extracted at the expense of the entanglement from the string. Starting with n copies of ρ_B one gets $n(1-H(p_i))$ copies of a known maximally entangled state in the asymptotic limit, by locally distinguishing $2^{nH(p_i)}$ likely strings $|B_{i_1}\rangle\langle B_{i_1}|\otimes|B_{i_2}\rangle\langle B_{i_2}|\otimes|B_{i_3}\rangle\times\langle B_{i_3}|\otimes\cdots\otimes|B_{i_n}\rangle\langle B_{i_n}|$ of the four Bell states, in which againour bound (2) saturates.

In this context, our inequality establishes the fact that when distilling from a mixture of Bell states $\Sigma_{i=1}^{4} p_i |B_i\rangle\langle B_i|$, if the process is to identify the strings of Bell states in the ensemble (e.g., in breeding or hashing) by one-way or even two-way LOCC [by conjecturing our inequality (2) to be valid also for two-way LOCC], the highest amount of entanglement that can be distilled per copy of the Bell mixture is $1-H(p_i)$.

We are now going to discuss the relation between our bound and entanglement distillation by error correction. Let Alice and Bob share n nonmaximally entangled states (they need not be the same), which arise due to the possible corruption during transmission of a maximally entangled state from Alice to Bob by some noisy channel. Let the errors that occurred during the transmission belong to a subset, say S, of the Pauli group G_n on n qubits [13], and there exists a stabilizer code tocorrect the errors [14,15]. After the transmission one can write the $2n$-qubit state along with the environment as

$$|\Psi_{ABE}\rangle = \sum_i [I_A \otimes (U_i)_B] |B_1\rangle^{\otimes n} |e_i\rangle$$

where $|e_i\rangle$ are environment states (possibly nonorthogonal and unnormalized). Here $\{U_i\}$ is the set of unitary operators acting on the 2^n-dimensional. Hilbert space of Bob's system, where each U_i belongs to S, that can be corrected by the stabilizer code [characterized by (n,m)], considered in the problem. So the number of linearly independent U_i's is 2^{n-m}. Now in this protocol Alice and Bob perform identical $(n-m)$-generator measurement on n qubits in their possession, and by comparing their measurement results they identify the error syndrome i and then correct it. But in this process of measurement the joint state of Alice and Bob collapsed to a maximally entangled state of $2^m \otimes 2^m$. So finally Alice and Bob come upwith an m-ebit maximally entangled state.

As no knowledge of the environment is used, this problem is equivalent to the problem of distilling a maximally entangled state from the mixture

$$\rho = \frac{1}{2^{n-m}} \sum_i [I_A \otimes (U_i)_B](|B_1\rangle\langle B_1|)^{\otimes n}[I \otimes (U_i)_B^{\dagger}]. \qquad (5)$$

Thus in this process, the amount of information $(I_{\mathrm{acc}}^{\mathrm{LOCC}})$ that has been extracted is $(n-m)$ [by this process of error correction, we are detecting and then correcting 2^{n-m} equally probable errors appearing in Eq. (5) by LOCC], $\overline{E_i}=n$, $\overline{E_f}=m$, and $\log_2 d_1 d_2 = 2n$. So the bound (2) is saturated for this distillation protocol.

In this article, we provided a relation [inequality (2)] among locally accessible information, initial average entanglement, and final average entanglement for any given asymptotic measure of entanglement, allowing even different kinds of asymptotic measures of entanglement for these two averages. We have given a proof of this relation for any one-way LOCC and provided some examples, each of which saturates the above-mentioned relation, revealing complementarity between locally accessible information and the amount of entanglement that has been distilled in this process. We have also shown that in each of the three well-known distillation protocols—breeding, hashing, and distillation by error correction—the above-mentioned relation is saturated. Although all our examples (given here) involve one-way protocols, one can easily check that the inequality (2) is strictly satisfied in the case of the recurrence protocol [16].

Distilling maximally entangled states from a general mixed state (created due to some disturbance in the channel) by LOCC is a fundamental problem in quantum-information processing. Until now, the standard distillation protocols deal with mixtures of Bell states, and in each of these protocols either full or partial (e.g., the recurrence protocol) extraction of information about the ensemble is performed. In particular, when for a state, hashing and breeding protocols yield either no or very little entanglement, initially the recurrence protocol is used, in which partial information about the ensemble is extracted to increase the fidelity. This shows that extraction of full information about the ensemble may reduce the amount of entanglement to be distilled. We have also encountered here some examples where accessing full information about the ensemble distilled less than the corresponding distillable entanglement. All these findings suggest that in order to find a better distillation protocol, one has to take care about the interplay between the amount of accessible information (to be accessed locally) and the final average entanglement (which may equal the amount of entanglement distilled in the process), and optimize it in some clever way.

Note added. Our conjecture [inequality (2)] concerning the two-way protocol has been recently proved by Horodecki *et al.* [17].

S.K. acknowledges support by the Council of Scientific and Industrial Research, Government of India, New Delhi. P.J. acknowledges support provided by the Institute of Mathematical Sciences, Chennai, India and the hospitality provided by the institute while the work was done. Part of this work was done when S.G. and G.K. were at the Institute of Mathematical Sciences, Chennai.

[1] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[2] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001).

[3] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, Phys. Rev. Lett. **90**, 047902 (2003).

[4] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilken, Phys. Rev. Lett. **84**, 1611 (2000).

[5] P. Badziag, M. Horodecki, A. Sen(De), and U. Sen, Phys. Rev. Lett. **91**, 117901 (2003).

[6] Y.-X. Chen, J.-S. Jin, and D. Yang, Phys. Rev. A **67**, 014302 (2003).

[7] Here both the parties apply C-NOT operations on their respective three-qubit systems, transforming $\rho^{(3)}$ to $(1/2)[|B_1^{\otimes 2}\rangle \times\langle B_1^{\otimes 2}|(|B_1\rangle\langle B_1|+|B_2\rangle\langle B_2|)]+(1/2)[|B_3^{\otimes 2}\rangle\langle B_3^{\otimes 2}|(|B_3\rangle\langle B_3|+|B_4\rangle \times\langle B_4|)]$ (see [6]). One now distinguishes between whether the target state belongs to the $\{|00\rangle, |11\rangle\}$ subspace or the $\{|01\rangle, |10\rangle\}$ subspace. This is extracting 1 cbit and after this discrimination one distills 2 ebits.

[8] D. Yang and Y.-X. Chen, Phys. Rev. A **69**, 024302 (2004).

[9] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, Phys. Rev. A **70**, 022304 (2004); H. Fan, Phys. Rev. Lett. **92**, 177905 (2004).

[10] D. Yang and Y.-X. Chen, e-print quant-ph/0311100.

[11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[12] K. G. H. Vollbrecht and M. A. Wolf, Phys. Rev. A **67**, 012303 (2003).

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).

[14] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[15] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

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

[17] M. Horodecki, J. Oppenheim, A. Sen(De), and U. Sen, e-print quant-ph/0405185.