Capacity of Quantum Erasure Channel Assisted by Backwards Classical Communication

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1103/PhysRevLett.103.240505">http://dx.doi.org/10.1103/PhysRevLett.103.240505</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>American Physical Society</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Accessed</td>
<td>Fri Feb 01 10:59:41 EST 2019</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/52516">http://hdl.handle.net/1721.1/52516</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td></td>
</tr>
</tbody>
</table>
Capacity of Quantum Erasure Channel Assisted by Backwards Classical Communication

Debbie Leung, Jongkeun Lim, and Peter Shor

1Department of Combinatorics and Optimization and Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1
2Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

(Received 7 December 2007; revised manuscript received 16 November 2009; published 11 December 2009)

We present a communication protocol for the erasure channel assisted by backwards classical communication, which achieves a significantly better rate than the best prior result. In addition, we prove an upper bound for the capacity of the channel. The upper bound is smaller than the capacity of the erasure channel when it is assisted by two-way classical communication. Thus, we prove the separation between quantum capacities assisted by backwards classical communication and two-way classical communication.

DOI: 10.1103/PhysRevLett.103.240505 PACS numbers: 03.67.Hk

In quantum information theory, a capacity $Q(\chi)$ of a channel $\chi$ is a theoretical maximum of the rate $m/n$ that is achievable by some communication protocol that sends $m$-qubit information with $n$ uses of the channel, where $n$ tends to infinity. The above definition of $Q$ is defined without auxiliary resources, and additional free classical communication may increase the capacity. We use $Q$, $Q_1$, $Q_B$, and $Q_2$ to denote the quantum capacities of a quantum channel when unassisted, assisted by unlimited forward, backward, and two-way classical communication, respectively. It was proved that classical forward communication alone does not increase the quantum capacity of any channel; in other words $Q(\chi) = Q_1(\chi)$ for all channels $\chi$ [1]. In contrast, $Q_2$ is greater than $Q$ for some channels [1]. $Q_B$ is also known to be greater than $Q$ for some channels [2], but it has been an open question whether $Q_B(\chi) = Q_2(\chi)$ for all $\chi$.

We study the capacities of the quantum erasure channel, which was first introduced in [3]. The quantum erasure channel of erasure probability $p$, denoted by $\mathcal{N}_p$, replaces the incoming qubit, with probability $p$, with an “erasure state” $|\psi\rangle$ orthogonal to both $|0\rangle$ and $|1\rangle$, thereby both erasing the qubit and informing the receiver that it has been erased. In an equivalent formulation, called the isometric extension, the channel exchanges the incoming qubit with the environmental system in state $|\psi\rangle$ with probability $p$. It was shown in [2] that the quantum capacities $Q$, $Q_1$, and $Q_2$ for $\mathcal{N}_p$ are given by

$$Q(\mathcal{N}_p) = Q_1(\mathcal{N}_p) = \max\{0, 1 - 2p\}$$

and

$$Q_2(\mathcal{N}_p) = 1 - p.$$

However, until the current investigation, little has been known about $Q_B(\mathcal{N}_p)$ except for two lower bounds that follow straightforwardly from one-way hashing [1] and teleportation [4] and an upper bound given by $Q_2(\mathcal{N}_p)$ as

$$Q_B(\mathcal{N}_p) \geq 1 - 2p, \quad \text{if } p \leq 2/5,$$

$$Q_B(\mathcal{N}_p) \geq (1 - p)/3, \quad \text{if } p \geq 2/5,$$

and

$$Q_B(\mathcal{N}_p) \leq Q_2(\mathcal{N}_p) = 1 - p.$$

In this Letter, we present an efficient communication protocol that achieves a better lower bound of $Q_B(\mathcal{N}_p)$, and we prove a new upper bound of $Q_B(\mathcal{N}_p)$. With this upper bound, we show that $Q_B(\mathcal{N}_p) \leq Q_2(\mathcal{N}_p)$ for all $p$ and resolve the previously open question.

Preliminaries and notations.—Recall the definition of von Neumann entropy $H(A) = H(\psi^A) = -\text{tr}(\psi^A \log \psi^A)$, where $\psi^A$ is the density operator for system $A$. The quantum mutual information and coherent information are defined as

$$I(A; B) = H(A) + H(B) - H(AB),$$

and

$$I(A)B) = H(B) - H(AB).$$

The statements in the following lemma will be used in the proof of a theorem in the later section.

Lemma 1. For disjoint systems $A$, $B$, and $C$, (i) $I(AB; C) - I(B; C) \leq I(A; BC)$. (ii) $I(A)B) \leq I(A)BC)$. (iii) $I(A)C) \leq I(AB)C)$. (iv) $I(A)BC) - I(A)B) \leq 2H(CE)$, where $E$ is any subset of $B$.

Proof. Subadditivity and strong subadditivity inequalities [5] easily give (i), (ii), (iii),

$$H(CDE) \leq H(D) + H(CE),$$

$$H(AD) \leq H(CE) + H(ADCE),$$

and

$$H(D) + H(AD) \leq H(AD) + H(DE),$$

for $E \subset B$ and $D = B/E$. Adding these three inequalities yields (iv).

We consider only near-perfect communication protocols that produce, with high probability, output states of high fidelity with the input states. The fidelity of states $\rho_{in}$ and $\rho_{out}$ is defined to be
\[ F(\rho_\text{in}, \rho_\text{out}) = \text{tr} \sqrt{\sqrt{\rho_\text{in}}} \rho_\text{out} \sqrt{\sqrt{\rho_\text{in}}}. \]

From now on, we call the sender, the receiver, and the environment Alice, Bob, and Eve.

**Communication protocol.**—We derive an improved lower bound for \( Q_B(\mathcal{N}_p) \) by providing a communication protocol. The protocol combines two subprotocols that utilize coherent teleportation introduced in [6].

**Coherent teleportation.**—Given an unknown qubit state \( |\psi\rangle = a|0\rangle + b|1\rangle \) in system \( M \) and an ebit (sometimes called an EPR pair or Bell state) \( |\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \) between Alice and Bob, Alice can transmit \( |\psi\rangle \) to Bob by teleportation [4]. In the original teleportation protocol, the change of basis takes the initial state \( |\psi\rangle_0 \) to

\[ \frac{1}{2} \sum_{ij} (i|j\rangle_M |i\rangle_E |j\rangle_E |i\rangle_B \rangle \psi_B, \]

right, \( \mathcal{N}_p \) denotes one use of the erasure channel, and Qbit denotes one use of the noiseless qubit channel. We have used \( \Phi \) and \( \Gamma \) as shorthand for \( |\Phi\rangle\langle\Phi| \) and \( |\Gamma\rangle\langle\Gamma| \). With free back classical communication, one use of \( \mathcal{N}_p \) can prepare one ebit with probability \( 1 - p \).

\[ 1 - p \]

We combine Eqs. (3) and (4) to get

\[ 1 - p \]

and

\[ 1 - p \]

Hence, the rate of the first subprotocol is

\[ 1 - p \]

\[ 1 - p \]

**Second subprotocol.**—This method differs from the previous subprotocol only in that \( |ij\rangle \) will be sent using a coherent version of superdense coding. More specifically, in this case, Alice and Bob first share an ebit \( |\Phi\rangle_{C_1C_2} \) where \( C_1 \) belongs to Alice and \( C_2 \) belongs to Bob. After the change of basis [see Eq. (2)], Alice applies control \( X \) from \( M \) to \( C_1 \) and control \( Z \) from \( A \) to \( C_2 \), resulting in the joint state

\[ \frac{1}{2} \sum_{ij} (i|j\rangle_M |i\rangle_{C_1} |j\rangle_{C_2} X^* Z^* |\psi\rangle_B, \]

and sends \( C_1 \) to Bob using the erasure channel. The states \( |\Phi_{ij}\rangle = X^* Z^* |\Phi\rangle \) are orthogonal (they form the Bell basis) [5]. In case of erase, Bob and Eve share \( |\Phi_{ij}\rangle_{C_1C_2} \) and Alice and Bob will take another ebit and repeat the superdense coding procedure, until Bob receives the transmission (call the two-qubit system in his possession \( D_1D_2 \)). Then, Bob applies the transformation \( |\Phi_{ij}\rangle_{D_1D_2} \rightarrow |ij\rangle_{D_1D_2} \) and coherently reverts the \( X^* Z^* \) not only in \( X^* Z^* |\psi\rangle_B \) but also in all the \( |\Phi_{ij}\rangle \) he shares with Eve (by acting only on his halves), so that the final state becomes

\[ \frac{1}{2} \sum_{ij} (i|j\rangle_M |i\rangle_{D_1} |j\rangle_{D_2} |\Phi_{EB}\rangle_{ik} |\psi\rangle_B, \]

where \( k \) again denotes the number of erasures before the successful transmission. In this method, Alice and Bob always share two 2 ebits at the end.

Once again, Alice needs to apply superdense coding \( \frac{1}{1 - p} \) times on average. This gives the asymptotic resource inequality

\[ \Phi_{AB} + \frac{1}{1 - p} [\mathcal{N}_p + \Phi_{AB}] \geq 1 \text{ Qbit} + 2 \Phi_{AB} 
\]

\[ + \left( \frac{1}{1 - p} - 1 \right) \Phi_{BE}. \]

Note that the above consumes more ebits than it produces for all \( p \); thus, we use Eq. (4) to supply the needed ebits,
and obtain
\[ 1 \mathcal{N}_p \geq (1 - p)^2 \text{ Qbit}. \]
Hence the rate of the second subprotocol is \((1 - p)^2\).

Rate of communication protocol.—Applying the two protocols selectively, the rate of the protocol is
\[ (1 - p)^2, \quad \text{if } p \leq 1/2 \quad \text{and} \quad \frac{1 - p}{1 + 2p}, \quad \text{if } p \geq 1/2. \]

(5)

Upper bound for the capacity.—The purpose of this section is to prove that \( Q_b(\mathcal{N}_p) \leq \frac{1 - p}{1 + p} \mathcal{N}_p \). By the definition of the capacity, for each \( n \), there is a protocol \( \mathcal{P}_n \) that uses back classical communication and \( \mathcal{N}_p \) at most \( n \) times and transmits \( n(Q_b(\mathcal{N}_p) - \delta_n) \) qubits from Alice to Bob with fidelity at least \( 1 - \epsilon_n \) and probability at least \( 1 - \epsilon_n \), where \( \epsilon_n, \delta_n \to 0 \) as \( n \to \infty \).

Our strategy to show the upper bound is as follows. We consider any protocol that transmits \( m \) qubits with \( n \) uses of the channel. In particular, such protocol must be able to transmit \( m \) halves of qubits shared between Alice and a reference system \( R \) [7], without entangling Eve and \( R \) (or else the transmission to Bob will be noisy). This translates to bounds on quantum mutual information between Bob, Eve, and \( R \) that will be contradicted if \( m/n \) is larger than our stated upper bound.

If Alice transmits her halves of the qubits shared with \( R \) directly through the channel, any loss to Eve can never be recovered. Thus, Alice has to transmit quantum states whose potential entanglement with \( R \) can be materialized or nullified depending on Bob’s back communication and Alice’s future transmissions. The finalizing or nullifying process requires further uses of the channel, giving an upper bound to the capacity.

To quantify the above idea, denote by \( S_1, S_2, \ldots, S_n \) the qubits transmitted by Alice through the channel. Each \( S_i \) is delivered to Bob with probability \( 1 - p \) or lost to Eve with probability \( p \). Let \( \mathcal{B} = \{ i | S_i \text{ sent to Bob} \} \) and \( \mathcal{E} = \{ i | S_i \text{ sent to Eve} \} \) be the index sets of qubits delivered to Bob and Eve. We define \( E_i = \bigcup_{1 \leq j \leq i} S_j \) to be Eve’s system after the \( i \)th transmission. For Bob, the most general procedure after each transmission is an isometry followed by a measurement. By double-block coding and by extending Theorem 10 in [8], any such measurement can be approximated by a von Neumann measurement on part of Bob’s system (turning the measured qubits into classical data). Let \( B_i \) be Bob’s quantum system immediately after the \( i \)th channel use, and \( B_i \) be his quantum system after his measurement and classical feedback to Alice. Thus \( B_i = B_{i-1} \cup S_i \) if \( S_i \) is delivered to Bob, and \( B_i = B_{i-1} \) if \( S_i \) is lost to Eve. Suppose a total of \( c \) qubits are measured by Bob in the protocol. After the final decoding operation, Bob produces an \( m \)-qubit system \( B^{(1)} \) that is almost maximally entangled with the system \( R \). We denote the rest of Bob’s quantum system by \( B^{(2)} \).

In the following theorem, \( I(S_i; B_{i-1} R) \) is the amount of mutual information carried by each transmission \( S_i \). For the rest of the Letter, information theoretical quantities are evaluated on the states that are held at the corresponding stages of the protocol. Part (i) of the theorem states that a sufficient amount of mutual information (2\( m \) for \( m \) qubits) has to be delivered to Bob. Part (ii) states that the more mutual information is lost to Eve, the more transmissions are needed to nullify the lost information.

Theorem 2. If the fidelity between the input and output states is at least \( 1 - \epsilon_n \), then (i) \( \sum_{i \in \mathcal{B}} I(S_i; B_{i-1} R) \geq 2m - 2(2\sqrt{2m} \epsilon_n + 1) \). (ii) \( \sum_{i \in \mathcal{E}} I(S_i; B_{i-1} R) \leq n - m + 4(2\sqrt{2m} \epsilon_n + 1) \).

Proof (i) For each \( i \in \mathcal{B} \), apply part (i) of Lemma 1 on the systems \( S_i, B_{i-1} \) and \( R \) to obtain
\[ I(B_i; R) - I(B_{i-1}; R) \leq I(B_{i-1} S_i; R) - I(B_{i-1}; R) \leq I(S_i; B_{i-1} R). \]

Thus,
\[ \sum_{i \in \mathcal{B}} I(S_i; B_{i-1} R) \leq \sum_{i \in \mathcal{B}} (I(B_i; R) - I(B_{i-1}; R)) = I(B_{n-1}; R) = I(B^{(1)}; R) = H(B^{(1)}) + H(R) - H(B^{(1)} R) \leq 2H(R) - H(B^{(1)} R). \]

Note that the fidelity between the state \( \mu \) in \( B^{(1)} R \) and \( \Phi^{\otimes m} \) is at least \( 1 - \epsilon_n \). Let \( D = \frac{1}{2} \text{tr}(\mu - \Phi^{\otimes m})^2 \) be the trace distance [5] between \( \mu \) and \( \Phi^{\otimes m} \). By [5] (p. 415),
\[ D \leq \sqrt{1 - F(\mu, \Phi^{\otimes m})^2} \leq \sqrt{2\epsilon_n}. \]

By Fannes’ inequality [5],
\[ H(\mu R) = |H(\mu) - H(\Phi^{\otimes m})| \leq 2Dm + 2D \log(2D) \leq 2\sqrt{2m\epsilon_n} + 1. \]

(ii) Using 2, 3, and 4 to denote the use of parts (ii), (iii), and (iv) of Lemma 1, respectively, we have
\[ \sum_{i \in \mathcal{E}} I(S_i; B_{i-1} R) \leq c + \sum_{i \in \mathcal{E}} I(S_i; B_{n} R) \leq c + I(\bigcup_{i \in \mathcal{E}} S_i; B_{n} R) \]
\[ \leq c + I(\bigcup_{i \in \mathcal{E}} S_i; B_{n-1} R) \]
\[ \leq c + I(E_n R B^{(1)} B^{(2)} R) + 2H(B^{(1)} R) \]
\[ \leq c + I(E_n R B^{(1)} B^{(2)} R) + 2H(B^{(1)} R) \]
\[ \leq c + I(E_n R B^{(1)} B^{(2)} R) + 2H(B^{(1)} R). \]
where the equalities use the fact that Bob’s decoding is isometric. $I(E_n R) B_n$ is upper bounded by $n - |\mathcal{E}| - c$. $I(R) B^{(1)} B^{(2)}$ is lower bounded as
\[
I(R) B^{(1)} B^{(2)} \geq I(R) B^{(1)} I(R) B^{(1)} T - 2H(T) = m - 2H(B^{(1)} R),
\]
where $T$ purifies $B^{(1)} R$. Putting together the two previous sets of inequalities,
\[
\sum_{i \in \mathcal{E}} I(S_i; B_{i-1} R) \leq n - |\mathcal{E}| - m + 4(2\sqrt{2}m \sqrt{\epsilon_n} + 1).
\]
Hence,
\[
\sum_{i \in \mathcal{E}} I(S_i; B_{i-1} R) \leq \sum_{i \in \mathcal{E}} \left( H(S_i) + I(S_i; B_{i-1} R) \right)
\leq \sum_{i \in \mathcal{E}} \left( 1 + I(S_i; B_{i-1} R) \right)
\leq n - m + 4(2\sqrt{2}m \sqrt{\epsilon_n} + 1).
\]
Since Alice cannot predict whether Bob or Eve will receive the next transmission and a certain fraction of the transmission is lost to Eve, the same fraction of mutual information has to be lost to Eve. Combined with the theorem, the argument gives an upper bound of $Q_B(\mathcal{N}_p)$. To prove this rigorously, consider the following random variable:
\[
X_i = \begin{cases} \frac{1}{2} I(S_i; B_{i-1} R) & \text{if } S_i \text{ is delivered to Bob} \\ \frac{1}{2} (1-p) I(S_i; B_{i-1} R) & \text{if } S_i \text{ is lost to Eve}. \end{cases}
\]
Then $|X_i| \leq 1$ and $E(X_i) = 0$. Note that the $X_i$’s may not be independent variables. Let $Y_i = \sum_{j=1}^i X_j$ and $Y_0 = 0$. Then $Y_0, Y_1, \ldots, Y_n$ is a martingale [9] with $|Y_{i+1} - Y_i| \leq 1$. If the fidelity between the input and output states is at least $1 - \epsilon_n$, then from Theorem 2
\[
Y_n = \frac{p}{2} \sum_{i \in \mathcal{E}} I(S_i; B_{i-1} R) - \frac{(1-p)}{2} \sum_{i \in \mathcal{E}} I(S_i; B_{i-1} R)
\geq \frac{(1 + p)}{2} n - \frac{(1-p)}{2} n - (2-p)(2\sqrt{2}m \sqrt{\epsilon_n} + 1).
\]
Assume by contradiction that $Q_B(\mathcal{N}_p) > \frac{1-p}{1+p}$. Then, for sufficiently large $n$, $\frac{n}{n} \geq \frac{1}{1+p} + 4k$ for some $k > 0$. The above expression for $Y_n$, which holds with probability at least $1 - \epsilon_n$, will exceed $kn$. Therefore $\lim_{n \to \infty} \Pr[Y_n \geq kn] = 1$.

However, Azuma’s inequality [9] applied to martingale $Y_i$ gives $\Pr[Y_n \geq kn] \leq e^{-(k^2/2)n}$, and $\lim_{n \to \infty} \Pr[Y_n \geq kn] = 0$, which is a contradiction. Hence,
\[
Q_B(\mathcal{N}_p) \leq \frac{1-p}{1+p}.
\]

Discussion.—We summarize the previous and our new results in Fig. 1. The lighter region is the previous undetermined area of $Q_B(\mathcal{N}_p)$, given by the previous lower and upper bounds in Eq. (1). The darker region is the new undetermined area of $Q_B(\mathcal{N}_p)$ due to our lower and upper bounds in Eqs. (5) and (6), which are significantly improved over previous results. Since our upper bound of $Q_B(\mathcal{N}_p)$ is strictly less than $Q_2(\mathcal{N}_p)$, we prove the separation between $Q_B$ and $Q_2$ answering the long-standing question raised in [2].

We thank Andrzej Grudka and Michal Horodecki for pointing out an important mistake in an earlier manuscript and for suggesting a solution that also substantially simplifies the proof. This research was partially supported by the W.M. Keck Foundation Center for Extreme Quantum Information Theory. P. W. S. and J. L. would like to thank the National Science Foundation for support through Grant No. CCF-0431787. J. L. thanks SLSF for support. D. L. thanks NSERC, CRC, CFI, ORF, MITACS, ARO, and CIFAR for support.