Extensive Nonadditivity of Privacy

Graeme Smith* and John A. Smolin†
IBM T.J. Watson Research Center, Yorktown Heights, New York 10598, USA
(Received 1 May 2009; published 18 September 2009)

Quantum information theory establishes the ultimate limits on communication and cryptography in terms of channel capacities for various types of information. The private capacity is particularly important because it quantifies achievable rates of quantum key distribution. We study the power of quantum channels with limited private capacity, focusing on channels that dephase in random bases. These display extensive nonadditivity of private capacity: a channel with $2\log d$ input qubits that has a private capacity less than 2, but when used together with a second channel with zero private capacity, the joint capacity jumps to $(1/2)\log d$. In contrast to earlier work which found nonadditivity vanishing as a fraction of input size or conditional on unproven mathematical assumptions, this provides a natural setting manifesting nonadditivity of privacy of the strongest possible sort.

DOI: 10.1103/PhysRevLett.103.120503 PACS numbers: 03.67.Dd, 03.67.Hk

Introduction.—Communication channels are subject to interference and noise, even under the best operating conditions. By modeling noise probabilistically, information theory characterizes the fundamental limitations for communication in terms of the capacity of a channel [1]. The capacity, measured in bits per channel use, establishes the boundary between communication rates that are achievable in principle and those that are not. Furthermore, there is a simple formula for the capacity, which can provide insight for designing practical protocols and give explicit bounds on the performance of real-world systems [2].

While a probabilistic description of noise is often a good approximation, ultimately all communication systems are fundamentally quantum. Furthermore, in the regime where quantum effects become important, there are several distinct notions of information transmission. One may be interested in the capacity of a channel for classical, private, or quantum transmission. The sender and receiver may have access to some auxiliary resources, such as entanglement or classical communication. The simplest case which involves no such assistance will be the focus of this Letter.

The capacity of a channel for private classical communication [3] is of particular importance because of its relation to quantum key distribution [4]. The private capacity of a quantum channel $\mathcal{N}$ is usually called $\mathcal{P}(\mathcal{N})$ and is no larger than the classical capacity, $\mathcal{C}(\mathcal{N})$. Since fully quantum transmission is necessarily private, the private capacity of a channel is at least as large as its quantum capacity, $\mathcal{Q}(\mathcal{N})$. As a result, we have $\mathcal{Q}(\mathcal{N}) \leq \mathcal{P}(\mathcal{N}) \leq \mathcal{C}(\mathcal{N})$. In contrast to the classical capacity of a *classical* channel, no simple expression is known for any of these three capacities of a quantum channel. In fact, it is known that the natural guesses for $\mathcal{Q}$, $\mathcal{P}$, and $\mathcal{C}$ are simply false [5–7]. As a result, very little has been known about the capacities of a quantum channel.

Lately, there have been some surprising discoveries about the additivity properties of quantum capacities [8–13]. A function on channels is called additive if its value on the tensor product of two channels is equal to the sum of the value on the individual channels: $f(\mathcal{N} \otimes \mathcal{M}) = f(\mathcal{N}) + f(\mathcal{M})$. Additivity of a capacity means that the communication capabilities of channels do not interact when you use them together—a channel is good for the same amount of communication no matter what other channels are available. Conversely, when a capacity is nonadditive, it means that the value of a channel for communication depends on what other channels it might be used with. It was found in [10] that the quantum capacity is strongly nonadditive. In fact, there are pairs of channels with $\mathcal{Q}(\mathcal{N}) = \mathcal{Q}(\mathcal{M}) = 0$ but $\mathcal{Q}(\mathcal{N} \otimes \mathcal{M}) > 0$. Something similar was found for the private capacity in [13], where channels were presented with $\mathcal{P}(\mathcal{N}) = 0$ and $\mathcal{P}(\mathcal{M}) \approx 1$ but $\mathcal{P}(\mathcal{N} \otimes \mathcal{M}) \gg 1$. So, it appears that the communication value of a quantum channel is not a simple function of the channel itself but also of the context in which it is used.

In this Letter, we present a family of channels displaying extensive nonadditivity of private capacity, meaning additivity violations proportional to the input size. This involves two crucial innovations over previous work. First, our channels are much simpler than those of [11,13,14] and do not rely on an assumption of additivity of Holevo information as in [11,14]. Second, while it was shown in [13] that $\mathcal{P}$ is not additive, the violation is a vanishingly small fraction of the channel's input size. Our work shows additivity violation of the strongest possible sort, with violations proportional to the log of the input dimension. Since $\log D$ is the largest possible capacity (classical or quantum) for a channel with input dimension D, and thus the natural scale of the capacity, violations of this sort show that nonadditivity is an essential feature of the private capacity.

Random phase coupling channels.—The channels we will focus on are pictured in Fig. 1. $\mathcal{R}_d$ has two

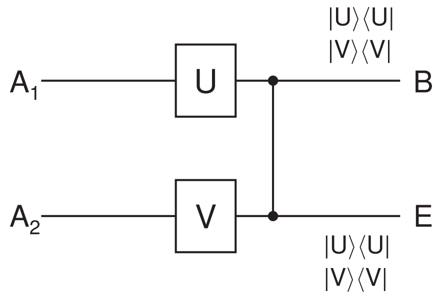

FIG. 1. Random phase coupling channel. Unknown randomly chosen unitaries are applied independently to A_1 and A_2. A controlled phase is then applied to between A_1 and A_2, which we now relabel B and E, respectively. The E system is traced out, while the B system is delivered to the receiver together with a classical description of the unitaries U and V.

d-dimensional inputs, A_1 and A_2. After local random unitaries U and V are applied individually to these inputs, a controlled phase is applied and A_2 is discarded. In addition to receiving the A_1 system (now relabeled B), the receiver is given a classical register describing which U and V were chosen.

More formally, we let $W_{UV} = PU \otimes V$, where $P = \sum_{i,j} \omega^{ij} |i\rangle\langle i|_{A_1} \otimes |j\rangle\langle j|_{A_2}$ is the controlled phase gate on A_1A_2 and ω is a primitive dth root of unity. Note that W_{UV} maps A_1A_2 to BE. We let $\mathcal{R}_{UV}(\phi) = \mathrm{Tr}_E W_{UV} \phi W_{UV}^\dagger$, and define our channel $\mathcal{R}_d = \mathbb{E}_{U,V} \mathcal{R}_{UV} \otimes |U\rangle\langle U| \otimes |V\rangle\langle V|$, where $\mathbb{E}_{U,V}$ is the expectation with respect to random variables U and V. Throughout, we will let $U^n = U_1 \otimes \ldots \otimes U_n$ and similarly for V, and define $\mathcal{R}_{U^nV^n} = \mathcal{R}_{U_1V_1} \otimes \ldots \otimes \mathcal{R}_{U_nV_n}$.

A key feature of our channel $\mathcal{R}_d$ is that the unitaries U and V are unknown to the sender. If she were told V before using the channel, she would be able to carefully choose the input to A_2 so as to avoid any dephasing of A_1. However, since she does not know V, she is unable to avoid choosing an input that results in a significant amount of dephasing when averaged over the choice of V. This rules out much quantum capacity. If at least she knew U in advance, she would still be able to send classical messages in the basis of dephasing, but since the dephasing is in a random basis, known only to the receiver, even the classical capacity of the channel is low.

However, when entanglement between sender and receiver is available, things change dramatically. We will see below that by having the sender feed half of a maximally entangled pair into the A_2 system, the other half sitting with the receiver, the channel can transmit quantum information at a rate of $\log d$. Since quantum communication is necessarily private, private communication is also possible at this rate. We will be able to use this property, together with the probabilistic entanglement provided by a 50% erasure channel, $\mathcal{A}_d^e$, which itself has zero private capacity, to show that $\mathcal{R}_d \otimes \mathcal{A}_d^e$ has a quantum capacity of at least $(1/2)\log d$, even though the individual private capacities are much smaller.

Small classical capacity.—Our goal now is to show that $\mathcal{R}_d$ has a small classical capacity—$\mathcal{C}(\mathcal{R}_d) \le 2$. To do this, we first have to review some well-known facts.

For an ensemble $\mathcal{E} = \{p_i, \phi_i\}$, we define the Holevo information [15]

$$\chi(\mathcal{N}, \mathcal{E}) = S(\rho) - \sum_i p_i S(\rho_i)$$

where $\rho_i = \mathcal{N}(\phi_i)$ and $\rho = \sum_i p_i \rho_i$, $S(\rho) = -\mathrm{Tr}\rho\log\rho$, and throughout logarithms will be taken base two. The classical capacity of a quantum channel is given as follows [16,17]:

$$\mathcal{C}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{E}} \chi(\mathcal{N}^{\otimes n}, \mathcal{E}). \tag{1}$$

Our main technical result is the following lemma, whose proof may be skipped on a first reading.

Lemma 1.—Let $\rho_{U^nV^n} = \mathcal{R}_{U^nV^n}(\psi_{A_1^nA_2^n})$. Then for $d \ge 9$,

$$\mathbb{E}_{U^nV^n} S(\rho_{U^nV^n}) \ge n(\log d - 2).$$

Proof.—First, note that $\mathbb{E}S(\rho_{U^nV^n}) \ge -\log \mathbb{E}\mathrm{Tr}\rho_{U^nV^n}^2$, so it will suffice to give an upper bound on $\mathbb{E}\mathrm{Tr}\rho_{U^nV^n}^2$. To do this, we will use the fact that

$$\mathrm{Tr}\,(\rho_{U^nV^n}^2) = \mathrm{Tr}(\rho_{U^nV^n}^{B^n} \otimes \rho_{U^nV^n}^{B'^n} F_{B^nB'^n})$$

where $F_{B^nB'^n}$ is the unitary that swaps B^n and B'^n. In particular, letting $X = (P_n^\dagger \otimes P_n^\dagger) F_{B^nB'^n} \otimes I_{E^nE'^n}(P_n \otimes P_n)$, we find that

$$\mathbb{E}\,\mathrm{Tr}(\rho_{U^nV^n}^2) = \mathrm{Tr}(\Psi X)$$

where $\Psi = \mathbb{E} U_{BB'}^n \otimes V_{EE'}^n \psi_{A_1^nA_2^n} \otimes \psi_{A_1'^nA_2'^n} U_{BB'}^{\dagger n} \otimes V_{EE'}^{\dagger n}$ with $U_{BB'}^n = \otimes_{l=1}^n (U_l \otimes U_l)$, similarly for $V_{EE'}^n$ and $P_n = P^{\otimes n}$. In fact, we will not even need to calculate Ψ exactly, since by Schur's Lemma [18], it takes the form

$$\Psi = \sum_{\mathbf{s}_b\mathbf{s}_e} \alpha_{\mathbf{s}_b\mathbf{s}_e} \frac{\Pi_{\mathbf{s}_b}^{BB'}}{d_{\mathbf{s}_b}^B} \otimes \frac{\Pi_{\mathbf{s}_e}^{EE'}}{d_{\mathbf{s}_e}^E}, \tag{2}$$

where $\mathbf{s}_b$ and $\mathbf{s}_e$ are n-bit strings, and $\alpha_{\mathbf{s}_b\mathbf{s}_e}$ are probabilities. Here, we have used the notation

$$\Pi_{\mathbf{s}_b}^{BB'} = \Pi_{(\mathbf{s}_b)_1}^{B_1B_1'} \otimes \ldots \otimes \Pi_{(\mathbf{s}_b)_n}^{B_nB_n'},$$

where $\Pi_0^{BB'}$ is the projector onto the symmetric space of BB', $\Pi_1^{BB'}$ projects onto the antisymmetric space, similarly for $\Pi_{\mathbf{s}_e}^{EE'}$, and $d_{\mathbf{s}_b}^B$ and $d_{\mathbf{s}_e}^E$ are the ranks of $\Pi_{\mathbf{s}_b}^{BB'}$ and $\Pi_{\mathbf{s}_e}^{EE'}$, respectively.

Because of Eq. (2), we can understand $\mathrm{Tr}(\Psi X)$ by focusing on a term of the form

$$\mathrm{Tr}\,(\Pi_{\mathbf{s}_b}^{BB'} \otimes \Pi_{\mathbf{s}_e}^{EE'} X).$$

This, in turn, is the product of n terms of the form

$$\mathrm{Tr}\,[\Pi_{s_b}^{BB'} \otimes \Pi_{s_e}^{EE'}(P_{BE} \otimes P_{B'E'})I \otimes F_{BB'}(P_{BE} \otimes P_{B'E'})^\dagger],$$

which it is easy to verify equals

$$\frac{(-1)^{s_e}}{4} \sum_{i,j,i'j'} \omega^{(i-i')(j-j')}[\delta_{ii'} + (-1)^{s_b}][\delta_{jj'} + (-1)^{s_e}].$$

Evaluating this sum explicitly gives us

$$\frac{(-1)^{s_e}}{4}[d^2 + (-1)^{s_b}d^3 + (-1)^{s_e}d^3 + (-1)^{s_b+s_e}d^3]$$

which, in turn, is no larger than $d^2(3d+1)/4$. As a result, we have

$$\mathrm{Tr}\,(\Pi_{\mathbf{s}_b}^{BB'} \otimes \Pi_{\mathbf{s}_e}^{EE'}X) \leq (d^2(3d+1)/4)^n.$$

Using this bound in combination with the fact that $d_{\mathbf{s}_b}^B \geq [d(d-1)/2]^n$ and similarly for $d_{\mathbf{s}_e}^E$, we find

$$\mathrm{Tr}\,(\Psi X) \leq \frac{[d^2(3d+1)/4]^n}{[d(d-1)/2]^{2n}} = \left(\frac{3d+1}{(d-1)^2}\right)^n.$$

Finally, we translate this back to a lower bound on the average entropy of B^n:

$$\mathbb{E}\,S(\rho_{U^nV^n}) \geq n\log[(d-1)^2/(3d+1)],$$

which, noting that for $d \geq 9$ we have $(d-1)^2/(3d+1) \geq d/4$, proves the result. □

We now turn to the classical capacity of our channel. Because our channels have infinite dimensional classical registers, to avoid technical complications, we write the Holevo quantity for $\mathcal{R}^{\otimes n}$ together with ensemble $\mathcal{E}$ as

$$\chi(\mathcal{R}^{\otimes n}, \mathcal{E}) = \mathbb{E}_{U^nV^n}\chi(\mathcal{R}_{U^nV^n}, \mathcal{E}).$$

Now, for any input ensemble $\{p_i, \phi_i\}$ to n copies of our channel $\mathcal{R}_d^{\otimes n}$, we have

$$S\left[\mathcal{R}_{U^nV^n}\left(\sum_i p_i\phi_i\right)\right] \leq n\log d.$$

Furthermore, by the Lemma, for each ϕ_i, the entropy of $\mathcal{R}_{U^nV^n}(\phi_i)$ averaged over U^nV^n is at least $n(\log d - 2)$. As a result, for any ensemble $\mathcal{E}$, we have $\mathbb{E}\chi(\mathcal{R}_{U^nV^n}, \mathcal{E}) \leq 2n$. In light of Eq. (1), this gives $\mathcal{C}(\mathcal{R}_d) \leq 2$.

Large joint quantum capacity.—We now show that the joint quantum capacity of a random phase coupling channel, $\mathcal{R}_d$, and a 50% erasure channel is at least $(1/2)\log d$. To do this, we will need the following lower bound for the quantum capacity [3,19,20], called the coherent information:

$$\mathcal{Q}(\mathcal{N}) \geq \max_{\phi_{AA'}}[S(B) - S(AB)],$$

where the entropies are evaluated on the state $(I \otimes \mathcal{N})(\phi)$.

In our case, since $\mathcal{R}_d$ has infinite dimensional classical outputs, the correct lower bound to consider is the coherent information of the channel given U and V, averaged over U, V.

The way to use the two channels together is as follows. We prepare two maximally entangled states $|\varphi\rangle = |\phi_d\rangle_{AA_1}|\phi_d\rangle_{B'A_2}$ and feed A_1A_2 into $\mathcal{R}_d$ and B' into $\mathcal{A}_d^e$. The coherent information then breaks up into a sum of two terms. The first, which occurs when the input to $\mathcal{A}_d^e$ is not erased (which has probability 1/2) is equal to $\log d$, as explained in Fig. 2. The second, which occurs when $\mathcal{A}_d^e$ emits an erasure flag (and also has probability 1/2), is the coherent information of a completely dephasing channel in a basis known only to the receiver. The resulting coherent information in this second case is exactly zero. The coherent information of $\mathcal{R}_d \otimes \mathcal{A}_d^e$ evaluated on $|\varphi\rangle$ is just the average of these two, $(1/2)\log d$. Recalling that $\mathcal{P}(\mathcal{R}_d) \leq \mathcal{C}(\mathcal{R}_d) \leq 2$ and $\mathcal{P}(\mathcal{A}_d^e) = 0$ gives the nonadditivity we sought.

Discussion.—We have shown that the quantum and private capacities of a quantum channel are extremely nonadditive. This nonadditivity illustrates, in contrast to the classical theory, that the communication capabilities of a quantum channel depend inherently on the setting in which they are used. Our construction is essentially a simplification and strengthening of the retrocorrectible channels studied in [11,14]. As a result, in addition to nonadditivity, our channels also provide unconditional separations of capacities which were only conjectured in [14].

In particular, we can show, contrary to the classical case, that the classical capacity of a quantum channel, assisted by backwards classical communication, may substantially exceed the unassisted capacity. To see this, note that if, upon putting halves of maximally entangled states into

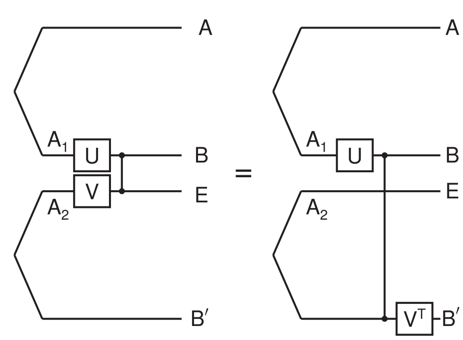

FIG. 2. Reversing random phase coupling with entanglement. Using a maximally entangled state, $|\phi_d\rangle_{A_2B'}$, the action of $\mathcal{R}_d$ on A_1 can be reversed. This depends on the fact that for any M, $M \otimes I|\phi_d\rangle = I \otimes M^T|\phi_d\rangle$, so that by inserting half of $|\phi_d\rangle_{A_2B'}$ into A_2, the receiver holding B and B' can invert U, V^T, and P, the controlled phase operation. By feeding B' into a 50% erasure channel, half the time, this gives a coherent information of $\log d$ between sender and receiver. The other half of the time, the coherent information is exactly zero so that the overall coherent information is $(1/2)\log d$.

$\mathcal{R}_d$, the receiver tells the sender U and V, she can easily invert U, V, and P to establish a d-dimensional maximally entangled state. In fact, we will use two copies of $\mathcal{R}_d$ to establish two d-dimensional maximally entangled states. We will use one maximally entangled state, together with a third copy of the channel, to simulate a perfect d-dimensional quantum channel as explained in Fig. 2. The second maximally entangled state can be used, together with this perfect channel, to send $2\log d$ classical bits by using superdense coding [21]. This results in a back-assisted classical capacity of at least $2/3 \log d$ with an unassisted classical capacity of no more than 2.

In terms of magnitude, superadditivity of private and quantum capacities cannot exceed $\log D$ for channels with input dimension D. Our channels achieve $(1/4)\log D$ in the limit of large input dimension. We suspect this is optimal both because of the simplicity of these channels and the structure of all known examples of superadditivity. However, we have not yet found a proof.

While the channels above have finite input dimension, as described they have infinite dimensional (indeed, continuous) outputs. This is not a serious drawback because our main technical argument (Lemma 1) depends only on the fact that a random unitary ensemble is a so-called two design. Luckily, the Clifford group is finite and has this property [22] so that we can replace the infinite output above with an output of size $O((\log d)^2)$.

The superactivation effect of [10] is not yet completely understood. From that work, it appeared that the fundamental effect was one of transforming noncoherent privacy [23,24] to coherent communication with the assistance of an erasure channel. However, our results here show conclusively that strong superadditivity of this sort is possible using channels with almost no private capacity, and, in fact, the private classical capacity is just as superadditive. What exactly is the source of superadditivity and which channels can be activated remain elusive open questions.

We are grateful to Ke Li and Andreas Winter for providing us an early draft of [13]. We both received support from the DARPA QUEST program under Contract No. HR0011-09-C-0047.

*gsbsmith@gmail.com
†smolin@watson.ibm.com

[1] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[2] T. Richardson and R. Urbanke, IEEE Commun. Mag. **41**, 126 (2003).
[3] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[4] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Bangalore, 1984) p. 175.
[5] D. DiVincenzo, P. W. Shor, and J. A. Smolin, Phys. Rev. A **57**, 830 (1998).
[6] G. Smith, J. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).
[7] M. Hastings, Nature Phys. **5**, 255 (2009).
[8] P. Shor, J. Smolin, and B. Terhal, Phys. Rev. Lett. **86**, 2681 (2001).
[9] P. Shor, J. Smolin, and A. Thapliyal, Phys. Rev. Lett. **90**, 107901 (2003).
[10] G. Smith and J. Yard, Science **321**, 1812 (2008).
[11] G. Smith and J. A. Smolin, Phys. Rev. Lett. **102**, 010501 (2009).
[12] L. Czekaj and P. Horodecki, Phys. Rev. Lett. **102**, 110505 (2009).
[13] K. Li, A. Winter, X. Zou, and G. Guo, arXiv:0903.4308.
[14] C. H. Bennett, I. Devetak, P. W. Shor, and J. A. Smolin, Phys. Rev. Lett. **96**, 150502 (2006).
[15] A. S. Holevo, in *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, edited by G. Maruyama and J. V. Prokhorov, Lecture Notes in Mathematics (Springer-Verlag, Berlin, 1973), Vol. 330, pp. 104–119.
[16] A. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[17] B. Schumacher and M. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[18] B. Simon, *Representations of Finite and Compact Groups* (Amer. Math. Soc., New York, 1996).
[19] P. W. Shor, lecture notes, MSRI Workshop on Quantum Computation, (2002). Available online at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/.
[20] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[21] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[22] D. P. Divincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).
[23] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[24] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).