



## Exact Cost of Redistributing Multipartite Quantum States

Igor Devetak<sup>1</sup> and Jon Yard<sup>2,3</sup>

<sup>1</sup>*Electrical Engineering Department, University of Southern California, Los Angeles, California 90089, USA*

<sup>2</sup>*Institute for Quantum Information, Caltech, Pasadena, California 91125, USA*

<sup>3</sup>*Quantum Institute, CNLS, CCS-3, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*

(Received 30 March 2007; published 9 June 2008)

How correlated are two quantum systems from the perspective of a third? We answer this by providing an optimal “quantum state redistribution” protocol for multipartite product sources. Specifically, given an arbitrary quantum state of three systems, where Alice holds two and Bob holds one, we identify the cost, in terms of quantum communication and entanglement, for Alice to give one of her parts to Bob. The communication cost gives the first known operational interpretation to quantum conditional mutual information. The optimal procedure is self-dual under time reversal and is perfectly composable. This generalizes known protocols such as the state merging and fully quantum Slepian-Wolf protocols, from which almost every known protocol in quantum Shannon theory can be derived.

DOI: [10.1103/PhysRevLett.100.230501](https://doi.org/10.1103/PhysRevLett.100.230501)

PACS numbers: 03.67.Hk, 03.65.-w, 89.70.Hj

The statistical approach to information and the asymptotic analysis of the protocols which process it was pioneered by Claude Shannon [1]. He showed that the information content of a random variable  $X$  with distribution  $p(x)$  could be intuitively quantified by the Shannon entropy  $H(X) = -\sum_x p(x) \log_2 p(x)$ . More importantly, he operationally justified this by proving that  $H(X)$  is the minimum average number of bits required to faithfully represent independent instances of  $X$  by any data compression protocol, also proving that such protocols indeed exist. Shannon further defined the conditional entropy as  $H(X|Y) = H(XY) - H(Y)$ , which is also equal to the average entropy of  $X$  given  $Y$ . Conditional entropy measures the information someone knowing only  $Y$  would have to learn in order to know  $X$  as well. Its operational relevance was shown by Slepian and Wolf [2] to be the minimum number of bits needed to describe  $X$  to someone who knows  $Y$ . Shannon also introduced mutual information  $I(X; Y) = H(Y) - H(Y|X)$  and conditional mutual information  $I(X; Y|Z) = H(Y|Z) - H(Y|XZ)$ , each of which is interpreted as the information shared by  $X$  and  $Y$ ; the latter is measured from the perspective of someone knowing  $Z$ . Mutual information plays a fundamental role in characterizing the capacity for a noisy channel to transmit information [1]. Its conditional counterpart arises in the answers to many problems, such as in rate distortion with side information at the decoder [3] and communication with side information at the encoder [4]. It also appears in the analysis of degraded broadcast channels [5]. All four of these quantities can easily be shown to be non-negative.

In recent years, a quantum mechanical generalization [6] of Shannon’s theory has been developing where a random variable is replaced with a quantum system  $C$  with density matrix  $\rho^C$ . The quantum analog of Shannon entropy is von Neumann entropy  $H(C)_\rho = -\text{Tr} \rho^C \log_2 \rho^C$ , which is the Shannon entropy of the eigenvalues of  $\rho^C$ . While von Neumann’s entropy preceded Shannon’s by almost 20

years, its operational interpretation was only found relatively recently by Schumacher [7], who showed that a large number  $n$  of quantum systems, identically prepared in the state  $\rho^C$ , could be compressed into a space of roughly  $nH(C)$  qubits, or two-level quantum systems. Here, a successful compression scheme is one which preserves the correlations  $C$  shares with the rest of the world, modeled by a reference system  $R$ . The combined system is considered to be in any pure state  $|\psi\rangle^{CR}$  satisfying  $\rho^C = \text{Tr}_R |\psi\rangle\langle\psi|^{CR}$ . We then say that Alice holds a purification of the reference  $R$ . The analogy can be continued, defining a quantum counterpart for each of Shannon’s quantities by replacing Shannon with von Neumann entropies. Quantum mutual information [8,9]  $I(A; B)$  can be considered as a measure of correlations between  $A$  and  $B$ . It plays a remarkably similar role as its classical counterpart, describing the classical capacity of a noisy quantum channel in the presence of free entanglement [8,10] (see also [11] for a thermodynamical interpretation). On the other hand, quantum conditional entropy  $H(A|B)$  [9] and quantum conditional mutual information (QCMDI)  $I(A; B|C)$  are less like their classical counterparts, as they cannot generally be viewed as averages. Furthermore,  $H(A|B)$  can be negative;  $-H(A|B)$  is often referred to as the coherent information [12], which plays a role in characterizing the capacity of a quantum channel for transmitting quantum information [13–15]. The operational task of state merging [16] gives meaning to  $H(A|B)$  where, depending on its sign, it corresponds to the rate at which entanglement is either consumed or generated while transferring  $A$  to someone already holding  $B$ . On the other hand, QCMDI can be shown to be non-negative. Unlike the classical case, this amounts to a nontrivial theorem, known as strong subadditivity of quantum entropy, whose original proof [17] relies on nontrivial tools from matrix analysis. More recently, operational proofs have been found [11,16], and we will see that our protocol leads to yet another such proof. Strong sub-

additivity is correspondingly powerful; it underlies virtually every known bound in quantum information theory. Despite its central role, a direct operational interpretation of QCMi on an arbitrary state has been conspicuously absent, although it has arisen in operational interpretations for certain restricted classes of underlying states [18]. Such a general interpretation is provided in this Letter.

The ability to send qubits from Alice to Bob is a resource, and Schumacher’s theorem tells how much of it is needed to transfer  $C$ . A weaker resource is entanglement, because it can be established by sending qubits. A “standard unit” of entanglement is called an ebit and consists of a single EPR pair  $|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  shared between Alice and Bob. By quantum teleportation [19], an ebit can be used to send a qubit, provided that two classical bits are sent as well. In the absence of classical communication, ebits are not helpful for moving  $C$  from Alice to Bob. They are helpful, however, in a variant of Schumacher’s scenario in which Alice and Bob have some side information. We model this with four systems in the state  $|\psi\rangle^{ACBR}$ . We begin by assuming that Alice holds  $AC$ , Bob holds  $B$ , while the reference  $R$  is unavailable to both parties. Alice’s and Bob’s task is to redistribute the quantum information so that it is instead Bob who holds  $C$  as follows:

$$(AC)^{\text{Alice}}(B)^{\text{Bob}} \rightarrow (A)^{\text{Alice}}(CB)^{\text{Bob}}.$$

To achieve this, Alice and Bob may perform local operations, Alice may send Bob qubits, and Alice and Bob may consume or generate entanglement. In particular, no classical communication is allowed, beyond what can be encoded in qubits. We allow the entanglement cost to be any real number, interpreting positive and negative values as in state merging. Our main result is that there exists a protocol—quantum state redistribution—allowing Alice to transfer  $C$  to Bob at a cost of  $Q$  qubits and  $E$  ebits if and only if

$$Q \geq \frac{1}{2}I(C; R|B) \quad Q + E \geq H(C|B).$$

This gives the first direct operational interpretation of QCMi on an arbitrary state. Simultaneously minimizing  $Q$  and  $Q + E$  leads to the optimal cost pair

$$Q = \frac{1}{2}I(C; R|B) \tag{1}$$

$$E = \frac{1}{2}I(C; A) - \frac{1}{2}I(C; B). \tag{2}$$

This pair corresponds to the corner point of the region in Fig. 1. As with Schumacher compression, this result is to be understood in the limit of many identical copies. Let us now point out some remarkable features of this result.

*Self-duality under time reversal.*—As illustrated in Fig. 2, our protocol can be implemented unitarily—if entanglement is consumed by the protocol, reversing those unitaries leads to a protocol which instead sends  $C$  from Bob to Alice, while generating the same amount of entanglement. Perhaps surprisingly, this symmetry is also evi-

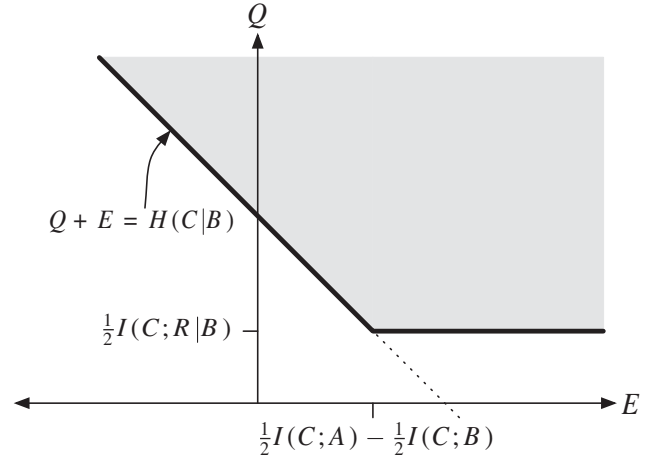


FIG. 1. Region of achievable cost pairs, together with the time-reversed optimal cost pair, assuming  $I(C; A) > I(C; B)$ .

dent in the optimal cost pairs: switching  $A$  and  $B$  reflects the optimal cost pair about the  $Q$ -axis (see Fig. 1). Thus, switching  $A$  and  $B$  changes the sign of  $E$  in (2), but has no effect on the expression (1) for  $Q$  because the identity  $I(C; R|B) = I(C; R|A)$  holds on every pure state  $|\psi\rangle^{ACBR}$ . In fact, our protocol can be considered as providing an explanation for why this identity should be true.

*Perfect composability.*—Suppose that Alice wants to transfer a composite system  $CD$  to Bob. An optimal strategy is for Alice to treat  $CD$  as a single system, sending them both simultaneously using our protocol. The optimal cost pair for this is

$$Q = \frac{1}{2}I(CD; R|B) \quad E = \frac{1}{2}I(CD; A) - \frac{1}{2}I(CD; B).$$

What if she sends the systems successively? The optimal cost for first transferring  $D$  is

$$Q_D = \frac{1}{2}I(D; R|B) \quad E_D = \frac{1}{2}I(D; AC) - \frac{1}{2}I(D; B).$$

Since Bob now has  $D$ , the remaining cost for sending  $C$  is

$$Q_C = \frac{1}{2}I(C; R|DB) \quad E_C = \frac{1}{2}I(C; A) - \frac{1}{2}I(C; DB).$$

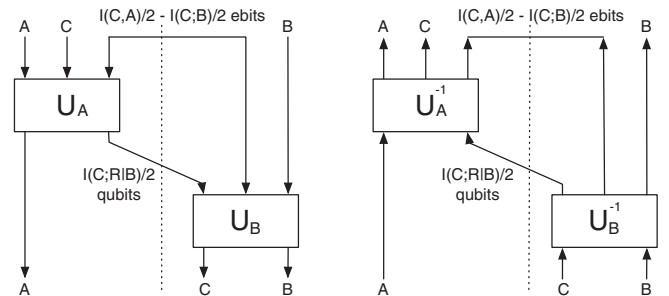


FIG. 2. Left: Unitary quantum state redistribution protocol in which Alice redistributes  $C$  to Bob while consuming entanglement (assuming that  $I(C; A) \geq I(C; B)$ ). Right: Corresponding time-reversed process where Bob redistributes  $C$  to Alice, this time generating the same amount of entanglement.

Simple algebraic manipulations then show that  $Q = Q_C + Q_D$  and  $E = E_C + E_D$ ! This feature parallels successive refinement in classical rate-distortion theory [20], only here the Markov condition is absent.

*Applications.*—Consider the following illustrative examples and applications of state redistribution:

(1) *Four-party cat state.*—The optimal cost pair for the state  $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)^{ACBR}$  is  $Q = E = 0$ . To redistribute  $C$  from Alice to Bob, Alice applies the local isometry  $|0\rangle^A \langle 0|^A + |1\rangle^A \langle 1|^A$ , after which Bob applies  $|00\rangle^{CB} \times \langle 0|^B + |11\rangle^{CB} \langle 1|^B$ .

(2) *Four-party W state.*—If the global state is  $\frac{1}{2} \times (|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle)^{ACBR}$ , we obtain  $Q \approx .38$  and  $E = 0$  for the optimal cost pair. For comparison, a compress-and-send strategy which ignores the side information requires roughly 0.81 qubits.

(3) *States saturating strong subadditivity.*—The states which require a zero rate of communication to redistribute  $C$  are precisely those which saturate strong subadditivity ( $I(C; R|B) = 0$ ), and are thus locally equivalent to a state of the form [21]

$$\sum_x \sqrt{p_x} |x\rangle^{A'} |x\rangle^{B'} |\phi_x\rangle^{A_C B_C C} |\varphi_x\rangle^{A_R B_R R}.$$

The entanglement cost for such states is  $\sum_x p_x (H(B_C)_{\phi_x} - H(A_C)_{\phi_x})$ . Another optimal strategy is thus to coherently concentrate [22] the  $A_C C|B_C$  entanglement while diluting [23] the  $A_C|C B_C$  entanglement in the individual states  $\phi_x^{A_C B_C C}$ .

(4) *State merging.*—Our state redistribution protocol allows for a deeper understanding of state merging [16,24]. By adding the additional resource of free classical communication, we recover their result that the cost, in ebits, for merging  $C$  to  $B$  is equal to  $H(C|B)$ . Accounting for transmitted bits as well, state merging considers  $A$  to be part of the reference, requiring that  $I(RA; C)$  bits be sent per copy of  $C$  merged. By our result, the classical communication cost is reduced to  $I(R; C|A) \leq I(RA; C)$ , which can be shown to be optimal by an argument similar to the one we give for our protocol. Thus, QCMi can also be regarded as the classical communication cost for state transfer in the presence of unlimited entanglement.

(5) *Fully quantum Slepian-Wolf (FQSW).*—A special case of our result is when Alice has no side information. An optimal strategy for this scenario has been found previously and called the fully quantum Slepian-Wolf protocol [25,26], which can transfer  $C$  from Alice to Bob using  $Q$  qubits and  $E$  ebits if and only if

$$Q \geq \frac{1}{2}I(C; R) \quad Q + E \geq H(C|B).$$

(6) *Fully quantum reverse Shannon (FQRS).*—If it is instead Bob who lacks side information, we obtain the previously studied [25,26] fully quantum reverse Shannon protocol as a special case of our result. Here, the required costs for transferring  $C$  to Bob are given by

$$Q \geq \frac{1}{2}I(C; R) \quad Q + E \geq H(C).$$

The optimal cost pair is dual to that of FQSW under time reversal [25].

*The protocol.*—Here we describe the proof that our protocol exists; for a more detailed treatment see [27]. First note that by the FQRS protocol, Alice can use  $\frac{1}{2}I(C; RB)$  qubits and  $\frac{1}{2}I(C; A)$  ebits to simulate the isometry which moves  $C$  to Bob, while keeping  $A$  to herself. In order to take advantage of Bob's side information, Alice can use a modification of that protocol which also transmits  $I(C; B)$  bits per copy of  $C$  which is moved [10,28]. It is furthermore possible to make the classical communication coherent [29,30] in the following sense. We say that Alice sends a coherent bit [29] to Bob if she applies an isometry  $|x\rangle^A \mapsto |x\rangle^A |x\rangle^B$  to a qubit in her possession, where Bob has  $B$  and  $x = 0, 1$ . Asymptotically, two coherent bits can be used to send a qubit and to generate an ebit [29], so Alice can send an additional  $\frac{1}{2}I(C; B)$  qubits, while generating the same number of ebits with Bob. This leads to a catalytic scenario, where extra ebits and qubits are needed to start the protocol, but are returned after completion. The dependence on the catalysts can be eliminated using methods in [31]. Subtracting the resources generated by the protocol from those which were invested yields the optimal cost pair. On the other hand, the optimality of our protocol is shown in [32] to follow from that of FQSW by subtracting the optimal costs for Alice to send only  $A$  from the costs for Alice to send  $AC$ .

*Discussion.*—For an arbitrary pure state  $|\psi\rangle^{ABCR}$ , we have determined the communication and entanglement resources which are necessary and sufficient for Alice and Bob, who, respectively, hold  $A$  and  $B$ , to transfer  $C$  between themselves while retaining the purity of the global state. The optimal communication cost gives the first operational interpretation of QCMi on an arbitrary state and also gives a natural interpretation to the pure state identity  $I(C; R|A) = I(C; R|B)$ : the correlations between  $C$  and  $R$  look the same from each of Alice's and Bob's perspectives. Because of this, the communication cost is symmetric under time reversal. On the other hand, the optimal entanglement cost was shown to be antisymmetric under time reversal, so that if ebits are consumed to move  $C$  one way, the same number are generated while moving it back.

There is a formal time-reversal duality between FQSW and FQRS [25]. We showed that our protocol is self-dual in the same sense, while incorporating both results as special cases. Interestingly, our coding theorem is based on a generalization of that from FQRS, while both the coding theorem and the converse from FQSW are used for our converse.

A corollary of our main result is a direct operational proof of strong subadditivity. Ours differs from other such operational proofs [11,16] because it does not even rely on the subadditivity of entropy, i.e.  $H(A) \geq H(A|B)$ . Before

removing the dependence on catalyst channels, our protocol cannot simulate more qubit identity channels than were initially provided, so that positivity of the overall qubit cost (QCMI) is evident.

Because our protocol involves an arbitrary four-partite pure state, it can be applied as a fundamental primitive for all multiparty state redistribution problems. Indeed, whenever there is a sender (Alice) and a receiver (Bob), there are four natural subsystems: the system  $A$  which stays with Alice, the system  $B$  which Bob already has, the system  $C$  which is being communicated, and the rest of the world  $R$ . Even if there are many more parties, each particular round of communication fits into our setting. For instance, suppose Alice holds  $AC_A$ , Bob has  $BC_B$  and Charlie holds  $C$ , while all systems are purified into a reference system  $R$ . If the goal is to transfer  $C_A$  and  $C_B$  to Charlie, direct application of our result gives a four-dimensional region of achievable costs ( $Q^{A \rightarrow C}$ ,  $Q^{B \rightarrow C}$ ,  $E^{AC}$ ,  $E^{BC}$ ), generated by two corner points, each corresponding to a different order in which Charlie receives the systems  $C_A$  and  $C_B$ . It is likely that other strategies, such as where  $C_A$  and  $C_B$  are split into multiple subsystems and are sent to Charlie in various orders, would lead to even larger achievable regions. Furthermore, it is known [26] that FQSW, when combined with teleportation [19] and superdense coding [33], recovers virtually every known quantum Shannon-theoretic protocol. We expect even more from state redistribution and are currently investigating its further implications for constructing more complex protocols and for understanding the structure of multipartite quantum states.

The authors are grateful to Toby Berger for urging them to find a quantum analogue of successive refinement, which partly inspired this result. They also thank Andrew Childs and Aram Harrow for comments and acknowledge funding from grants through the NSF. J.Y.'s research at LANL is supported by the Center for Nonlinear Studies (CNLS), the Quantum Institute and the LDRD program of the U.S. DOE.

- 
- [1] C. E. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
  - [2] D. Slepian and J. K. Wolf, *IEEE Trans. Inf. Theory* **19**, 471 (1973).
  - [3] A. Wyner and J. Ziv, *IEEE Trans. Inf. Theory* **22**, 1 (1976).
  - [4] C. Shannon, *IBM J. Res. Dev.* **2**, 289 (1958).

- [5] T. Cover, *IEEE Trans. Inf. Theory* **18**, 2 (1972).
- [6] C. H. Bennett and P. W. Shor, *IEEE Trans. Inf. Theory* **44**, 2724 (1998).
- [7] B. Schumacher, *Phys. Rev. A* **51**, 2738 (1995).
- [8] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *Phys. Rev. Lett.* **83**, 3081 (1999).
- [9] N. J. Cerf and C. Adami, *Phys. Rev. Lett.* **79**, 5194 (1997).
- [10] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *IEEE Trans. Inf. Theory* **48**, 2637 (2002).
- [11] B. Groisman, S. Popescu, and A. Winter, *Phys. Rev. A* **72**, 032317 (2005).
- [12] B. Schumacher and M. A. Nielsen, *Phys. Rev. A* **54**, 2629 (1996).
- [13] S. Lloyd, *Phys. Rev. A* **55**, 1613 (1997).
- [14] P. W. Shor (unpublished).
- [15] I. Devetak, *IEEE Trans. Inf. Theory* **51**, 44 (2005).
- [16] M. Horodecki, J. Oppenheim, and A. Winter, *Nature (London)* **436**, 673 (2005).
- [17] E. Lieb and M. B. Ruskai, *J. Math. Phys. (N.Y.)* **14**, 1938 (1973).
- [18] M. Christandl and A. Winter, *J. Math. Phys. (N.Y.)* **45**, 829 (2004).
- [19] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [20] T. M. Cover and W. H. R. Equitz, *IEEE Trans. Inf. Theory* **37**, 269 (1991).
- [21] P. Hayden, R. Jozsa, D. Petz, and A. Winter, *Commun. Math. Phys.* **246**, 359 (2004).
- [22] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, *Phys. Rev. A* **53**, 2046 (1996).
- [23] H.-K. Lo and S. Popescu, *Phys. Rev. Lett.* **83**, 1459 (1999).
- [24] M. Horodecki, J. Oppenheim, and A. Winter, *Commun. Math. Phys.* **269**, 107 (2006).
- [25] I. Devetak, *Phys. Rev. Lett.* **97**, 140503 (2006).
- [26] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, arXiv:quant-ph/0606225.
- [27] J. Yard and I. Devetak, arXiv:0706.2907.
- [28] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, *Quantum Inf. Comput.* **1**, 70 (2001).
- [29] A. W. Harrow, *Phys. Rev. Lett.* **92**, 097902 (2004).
- [30] I. Devetak, A. W. Harrow, and A. Winter, *Phys. Rev. Lett.* **93**, 230504 (2004).
- [31] I. Devetak, A. W. Harrow, and A. Winter, arXiv:quant-ph/0512015.
- [32] Z. Luo and I. Devetak, arXiv:quant-ph/0611008.
- [33] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).