A Family of Quantum Protocols

Igor Devetak,[1,*] Aram W. Harrow,[2,†] and Andreas Winter[3,‡]

[1]IBM T. J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598, USA
[2]MIT Physics Deptartment, 77 Massachusetts Avenue, Cambridge, MA 02139, USA
[3]Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, United Kingdom

(Received 4 February 2004; published 3 December 2004)

We introduce three new quantum protocols involving noisy quantum channels and entangled states, and relate them operationally and conceptually with four well-known old protocols. Two of the new protocols (the mother and father) can generate the other five "child" protocols by direct application of teleportation and superdense coding, and can be derived in turn by making the old protocols "coherent." This gives very simple proofs for two famous old protocols (the hashing inequality and quantum channel capacity) and provides the basis for optimal trade-off curves in several quantum information processing tasks.

DOI: 10.1103/PhysRevLett.93.230504 PACS numbers: 03.67.Hk, 42.50.Dv, 89.70.+c

Introduction.—The central task of quantum information theory is to determine the rates at which the quantum state of any physical object can be transmitted from one location to another. So far quantum information theory incorporates a number of basic coding theorems, including quantum compression [1], and expressions for classical [2] and quantum [3–5] capacities of quantum channels. In [6], these results were formulated in terms of asymptotic interconversion between information processing resources, such as uses of a quantum channel, shared entanglement and so on. For instance, channel coding may be viewed as converting a noisy channel into a noiseless one on a smaller input space. A particularly important class of problems in quantum information theory involves converting a noisy quantum channel or shared noisy entanglement between two spatially separated parties (conventionally denoted by Alice and Bob) into a noiseless one, via local operations possibly assisted by limited use of an auxiliary noiseless resource such as a perfect qubit channel, shared ebits, or one-way classical communication. Previously, this class of problems had only been addressed as a collection of special cases, each requiring its own complicated proof techniques to address. In this Letter we consider basic protocols for each member of this class, three of which are new, and observe that they are naturally organized into two mutually dual hierarchies. This result significantly simplifies the quantum information processing landscape, revealing connections between scenarios previously thought independent. Some of our connections give constructive methods for turning one protocol into another, so that a coding scheme for one protocol yields codes for a whole class of other protocols. Moreover, these basic protocols will provide the crucial ingredient for constructing *optimal* protocols and two-dimensional trade-offs.

The family of resource inequalities.—The following notation for information processing resources was proposed in [6]. A noiseless qubit channel, noiseless classical bit channel, and pure ebit (EPR pair) were denoted by $[q \to q]$, $[c \to c]$, and $[qq]$, respectively, reflecting their classical/quantum and dynamic/static nature. A noisy bipartite state ρ^{AB} is denoted by $\{qq\}$, and a general quantum channel $\mathcal{N}\colon \mathcal{H}_{A'} \to \mathcal{H}_B$ is denoted by $\{q \to q\}$. In either case, one may define a class of pure states $|\psi\rangle^{ABE}$. In the former, it consists of the purifications of ρ^{AB}, i.e., $\rho^{AB} = \mathrm{Tr}_E \psi^{ABE}$. In the latter, it corresponds to the outcome of sending half of some $|\phi\rangle^{AA'}$ through the channel's Stinespring [7] extension $U_{\mathcal{N}}\colon \mathcal{H}_{A'} \to \mathcal{H}_B \otimes \mathcal{H}_E$ ($\mathcal{N}$, mapping states on A' to states on B, is obtained as the isometry $U_{\mathcal{N}}$ followed by the partial trace over E.) One may define the usual entropic quantities with respect to the state $|\psi\rangle^{ABE}$. Recall the definition of the von Neumann entropy $H(A) = H(\psi^A) = -\mathrm{Tr}(\psi^A \log \psi^A)$, where $\psi^A = \mathrm{Tr}_{BE} \psi^{ABE}$. Further define the quantum mutual information [8] $I(A;B) = H(A) + H(B) - H(AB)$ and the coherent information [9] $I_c(A\rangle B) = -H(A|B) = H(B) - H(AB)$; the latter notation is from [10]. Relative to the *pure* state $|\psi\rangle^{ABE}$, $H(AB) = H(E)$ and $H(AE) = H(B)$, so

$$\frac{1}{2}I(A;B) + \frac{1}{2}I(A;E) = H(A),$$

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

It is possible to give meaning to inequalities between the various resources with entropic quantities as coefficients. Consider, for instance, the "mother" *resource inequality* (RI), which we refer to as ♀:

$$\frac{1}{2}I(A;E)[q \to q] + \{qq\} \geq \frac{1}{2}I(A;B)[qq].$$

It embodies an achievability statement: for any $\epsilon, \delta > 0$, for sufficiently large n there exists a protocol that uses up n instances of a noisy bipartite state ρ^{AB} and $\leq n[I(A;E)/2 + \delta]$ instances of a noiseless qubit channel, to produce a state within trace distance ϵ of $\geq n[I(A;B)/2 - \delta]$ ebits. The entropic quantities implicitly refer to any $|\psi\rangle^{ABE}$ associated with the noisy resource ρ^{AB}. The resources on the left- (right-) hand side are called input (output) resources, respectively.

As we shall see, there exists a dual "father" RI, which we refer to as ♂, related to the mother by replacing dynamic resources with static ones and vice versa:

$$\frac{1}{2}I(A;E)[qq] + \{q \to q\} \geq \frac{1}{2}I(A;B)[q \to q].$$

Again, it means that for sufficiently large n there exists a protocol that uses n copies of $\mathcal{N}$ assisted by $\approx nI(A;E)/2$ ebits of entanglement to simulate arbitrarily faithfully the effect of $\approx nI(A;B)/2$ noiseless qubit channels. The entropic quantities implicitly refer to any $|\psi\rangle^{ABE}$ associated with the noisy resource $\mathcal{N}$. Note that in the noiseless case (pure ebit or perfect qubit channel), both parents express trivial identities.

Giving constructive proofs of the parent resource inequalities will be the central result of this Letter. First, though, we demonstrate the consequences of these RIs.

We shall combine the parents with the activating noiseless resource inequalities corresponding to teleportation (TP) [11]

$$2[c \to c] + [qq] \succeq [q \to q]$$

and superdense coding (SD) [12]

$$[q \to q] + [qq] \succeq 2[c \to c],$$

to generate their offspring. Here we use "$\succeq$" to denote exact achievability (as opposed to the asymptotic "$\geq$").

They may be applied to a parent RI by either prepending (the output of TP and SD is used as an input to a protocol implementing the parent RI) or appending (the output of the parent is used as an input to TP and SD). In addition to TP and SD, we shall also make use of a third noiseless RI, "entanglement distribution" (ED), given by

$$[q \to q] \succeq [qq].$$

It is trivially implemented by sending half of an EPR pair through the qubit channel.

Each parent has her or his own children, as shown in Fig. 1. Let us consider the mother first; she has three children. The first one is a new RI, a noisy version of teleportation suggested to us by Burkard [13], in which noisy entanglement is combined with classical communication to teleport a quantum state. It is obtained by appending TP to the mother:

$$I(A;B)[c \to c] + \{qq\} \geq I_c(A\rangle B)[q \to q]. \qquad (1)$$

The second is the recently proved "hashing inequality" [10] (including the classical communication cost), which is known to yield the optimal one-way distillable entanglement. It follows from prepending TP to the mother:

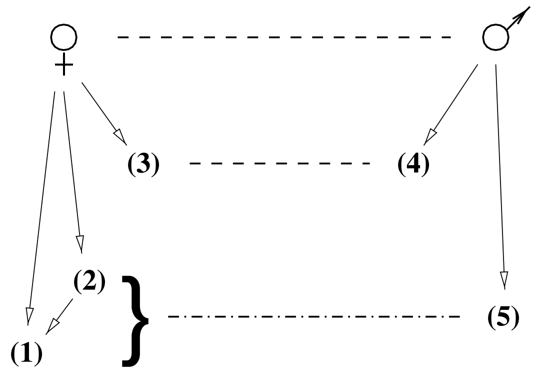

FIG. 1. The family tree: the dashed lines signify duality, and the dash-dotted line is the almost-duality described in the text. The solid arrows signify descendance via TP, SD, or ED.

$$I(A;E)[c \to c] + \{qq\} \geq I_c(A\rangle B)[qq]. \qquad (2)$$

Note that (2) also yields (1), by appending TP.

The third is a noisy version of superdense coding, which first appeared (somewhat disguised) in [14] and is obtained by appending SD to the mother:

$$H(A)[q \to q] + \{qq\} \geq I(A;B)[c \to c]. \qquad (3)$$

The father does not quite make it to three children: he has only two. Appending SD to him gives the coding for entanglement-assisted classical information transmission [15]:

$$H(A)[qq] + \{q \to q\} \geq I(A;B)[c \to c]. \qquad (4)$$

Note that it is dual to (3), at least as far as the quantum parts are concerned.

There is one more thing we can do: append ED to a fraction of the output of ♀ to recover the famous quantum channel capacity result [3–5]

$$\{q \to q\} \geq I_c(A\rangle B)[q \to q]. \qquad (5)$$

This one is almost dual to (2), and can be made formally dual by wasting $I(A;E)[c \to c]$.

The reason that the mother-father duality does not propagate perfectly down the family tree lies in the lack of duality between TP and ED. While SD is self-dual under the interchange of $[qq]$ and $[q \to q]$, TP and ED become mutually dual only by wastefully adding $2[c \to c]$ to the left-hand side of ED. In this light, even (2) has a dual RI: a rather wasteful version of (5).

Coherent communication.—Having demonstrated the power of the parent resource inequalities, we now address the question of constructing protocols implementing them. Recently, the importance of "coherent communication" was recognized [16]: a *coherent bit channel* is defined as the isometric mapping

$$|x\rangle^A \mapsto |x\rangle^A|x\rangle^B \qquad (6)$$

for a basis $\{|x\rangle: x \in [0,1]\}$ of the qubit system A. Note that this transformation implements a noiseless transmission of the classical index x, but may also be used to create entanglement by applying it to superpositions of $|0\rangle$ and $|1\rangle$. Viewed as a resource, we shall denote it by $[q \rightarrow qq]$. In what follows, it shall often be used in lieu of the classical bit channel $[c \rightarrow c]$.

In [16], it is shown that SD can be made "coherent" to yield two coherent bits

$$[q \rightarrow q] + [qq] \geq 2[q \rightarrow qq].$$

On the other hand, using coherent bits for teleportation has the virtue of creating entanglement as a by-product

$$2[q \rightarrow qq] + [qq] \geq [q \rightarrow q] + 2[qq].$$

Hence we have the equivalence, modulo catalytic entanglement (symbolized by the superscript c),

$$2[q \rightarrow qq] \overset{c}{=} [q \rightarrow q] + [qq],$$

which gives us the asymptotic equivalence [16],

$$[q \rightarrow qq] = \frac{1}{2}([q \rightarrow q] + [qq]). \tag{7}$$

Note that in the previous section we have already made use of the fact that recycling allows us to convert catalytic formulas (i.e., cancellation of equal terms left and right) into asymptotic ones, when deriving (2) and (3) from the mother.

When is it possible to make use of this equivalence, or in other words: when can classical communication be made coherent? The lessons learned in [5,10] regarding making protocols coherent and the observations of [16] lead us to two general rules. In what follows we shall work in the "extended Hilbert space" picture: all quantum operations and generalized measurements are implemented by adding ancillas (initially in pure states), performing unitary operations, and performing von Neumann measurements on the ancillas. No subsystems are allowed to be discarded, so the overall quantum system is always in a pure state. In particular, this means that the environment E is always included in our description. Note, however, that without loss of generality, a subsystem may be discarded after a von Neumann measurement has been performed on it; this is because it may always be reset to a standard pure state via a unitary operation depending on the measurement outcome.

Rule I: If $[c \rightarrow c]$ is featured in the *input* of a resource inequality, it may be replaced by $\frac{1}{2}([q \rightarrow q] - [qq])$ if there exists a protocol implementing the RI in which the classical message is almost uniformly distributed and almost decoupled from the overall quantum system at the end of the protocol.

Rule O: If $[c \rightarrow c]$ is featured in the *output* of a resource inequality with quantum inputs, it may be replaced by $\frac{1}{2}([q \rightarrow q] + [qq])$ if there exists a protocol implementing the RI in which the classical message is almost decoupled from the overall quantum system at the end of the protocol. In particular, being decoupled from E implies *privacy.*

In the above, a distribution $\{p_x\}$ is "almost uniform" when close in trace distance to the uniform distribution. A classical message x is "almost decoupled" from a quantum system in the state $|\theta_x\rangle$ if there exists some $|\theta\rangle$ with $|\theta_x\rangle \approx |\theta\rangle$ for all x. Throughout we write $\approx$ to denote a trace distance of $\leq \epsilon_n$ where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$ for asymptotic resource inequalities (we need not consider single-shot resource inequalities here, but the rules apply to this case trivially with $\epsilon_n = 0$).

Proof of Rule I.—Whenever the resource inequality features $[c \rightarrow c]$ in the input, this means that Alice performs a von Neumann measurement on some subsystem A_1, the outcome of which she sends to Bob, who then performs an unitary operation depending on the received information. Before Alice's von Neumann measurement, the joint state of A_1 and the remaining quantum system Q is

$$\sum_x \sqrt{p_x}|x\rangle^{A_1}|\phi_x\rangle^Q,$$

where p is an almost uniform distribution. Upon learning the measurement outcome x, Bob performs some unitary U_x on Q, almost decoupling it from x:

$$U_x|\phi_x\rangle^Q = |\theta_x\rangle^Q \approx |\theta\rangle^Q,$$

for some fixed state $|\theta\rangle$.

If Alice refrains from the measurement and instead sends A_1 through a *coherent* channel (6), the resulting state is

$$\sum_x \sqrt{p_x}|x\rangle^{A_1}|x\rangle^{B_1}|\phi_x\rangle^Q.$$

Bob now performs the *controlled* unitary $\sum_x |x\rangle\langle x|^{B_1} \otimes U_x$, giving rise to

$$\approx \left(\sum_x \sqrt{p_x}|x\rangle^{A_1}|x\rangle^{B_1}\right) \otimes |\theta\rangle^Q.$$

Thus, in addition to the state $|\theta\rangle^Q$, an almost maximally entangled state has been generated. Counting resources, $[c \rightarrow c]$ has been replaced by

$$[q \rightarrow qq] - [qq] = \frac{1}{2}([q \rightarrow q] - [qq]).$$

It can be shown that the uniformity condition on p may be relaxed, requiring only $n^{-1}\log p_x \approx$ const for all x.

Proof of Rule O.—Now the roles of Alice and Bob are somewhat interchanged. Alice performs a unitary operation depending on the classical message to be sent and Bob performs a von Neumann measurement on some subsystem B_1, which almost always succeeds in reproducing the message. Thus, before his measurement, the state of B_1 and the remaining quantum system Q is

$$\approx |x\rangle^{B_1}|\phi_x\rangle^Q.$$

Based on the outcome x of his measurement, Bob performs some unitary U_x on Q:

$$U_x|\phi_x\rangle^Q = |\theta_x\rangle^Q \approx |\theta\rangle^Q,$$

leaving the state of Q almost decoupled from x.

Instead, Alice may perform *coherent* communication. Given a subsystem A_1 in the state $|x\rangle^{A_1}$ she encodes via *controlled* unitary operations, yielding

$$\approx |x\rangle^{A_1}|x\rangle^{B_1}|\phi_x\rangle^Q.$$

Bob refrains from measuring B_1 and instead performs the *controlled* unitary $\sum_x |x\rangle\langle x|^{B_1} \otimes U_x$, giving rise to

$$\approx |x\rangle^{A_1}|x\rangle^{B_1} \otimes |\theta\rangle^Q.$$

By the conditions of Rule O, there were no other measurements made in the original protocol, so that the implementation of the new coherent version is completely unitary. Rule O follows from Eq. (7).

The mother RI (♀) is now obtained from the hashing inequality (2) by applying Rule I. It can be checked that the protocol from [10] implementing (2) indeed satisfies the conditions of Rule I. In this protocol the classical communication is used for sending a kind of "which quantum code" information from which the quantum information "encoded" is readily decoupled by "decoding".

The mother (♀) also follows from the noisy superdense coding inequality (5), as implemented in [14], by applying Rule O. Indeed, Eve only holds the *static* purification of ρ^{AB}, which is unaffected by Alice's encoding.

The father RI (♂) is similarly obtained, via Rule O, from (4). The main observation is that the protocol from [15] implementing (4) in fact outputs a *private* classical channel as it is. More precisely, in [15], Alice and Bob share a maximally entangled state $|\Phi_+\rangle^{A'B'}$. Alice encodes her message x via a unitary U_x:

$$x \mapsto (U_x \otimes \mathbb{1})|\Phi_+\rangle^{A'B'} = (\mathbb{1} \otimes U_x^*)|\Phi_+\rangle^{A'B'}.$$

Applying the channel $U_{\mathcal{N}}^{\otimes n}$ yields

$$(\mathbb{1}^{BE} \otimes U_x^*)|\Psi\rangle^{BEB'},$$

where $|\Psi\rangle^{BEB'} = U_{\mathcal{N}}^{\otimes n}|\Phi_+\rangle^{A'B'}$. Bob decodes x inducing next to no disturbance on the quantum system [17]. Finally he applies U_x^T to B', bringing the system BEB' into the state $|\Psi\rangle$, thus decoupling it from x, and justifying Rule O.

Since (1) is a completely new protocol, the only known implementation is the one we give in the Letter. Therefore, it can trivially be made coherent to regenerate the mother. The only child that cannot regenerate its parent is (5), because ED is clearly an irreversible transformation.

It is remarkable that comparatively simple protocols such as (3) and (4) can yield, via the mother and father protocols, the quantum channel capacity and hashing inequality, respectively, which were long-standing problems until very recently. Of course, after two rounds of processing they become quite complicated.

Conclusion.—We have introduced two purely quantum coding protocols, which we showed to be closely related to entanglement-assisted coding tasks, quantum capacities, and distillability: these once long sought-after protocols descend from the mother (♀) and father (♂) by applying teleportation or superdense coding. Furthermore, most of the children can be made coherent to regenerate their parents. What we have not shown here is that our protocols actually give rise to information theoretically optimal resource trade-offs; a detailed discussion of these will be given in a forthcoming paper.

We thank C. H. Bennett, G. Burkard, J. A. Smolin, and A. Ndirango for useful discussions. I. D. is partially supported by the NSA under the ARO Grants No. DAAG55-98-C-0041 and No. DAAD19-01-1-06. The latter grant also supports A. W. H. A. W. was supported by the U.K. Engineering and Physical Sciences Research Council.

*Electronic address: devetak@us.ibm.com
†Electronic address: aram@mit.edu
‡Electronic address: a.j.winter@bris.ac.uk

[1] B. Schumacher, Phys. Rev. A **51**, 2738 (1995); R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994).
[2] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[3] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[4] P. W. Shor (to be published). Lecture notes and video (RealPlayer) available at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/.
[5] I. Devetak, quant-ph/0304127.
[6] I. Devetak and A. Winter, quant-ph/0304196.
[7] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
[8] N. J. Cerf and C. Adami, Phys. Rev. Lett. **79**, 5194 (1997).
[9] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[10] I. Devetak and A. Winter, quant-ph/0306078; quant-ph/0307053.
[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[12] C. H. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[13] G. Burkard (private communication).
[14] M. Horodecki, P. Horodecki, R. Horodecki, D. W. Leung, and B. M. Terhal, Quantum Inf. Comput. **1**, 70 (2001).
[15] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002).
[16] A. W. Harrow, Phys. Rev. Lett. **92**, 097902 (2004).
[17] A. Winter, IEEE Trans. Inf. Theory **45**, 2481 (1999).