Trading Resources in Quantum Communication

A quantum channel has different capacities for communication, depending upon the type of information being transmitted and whether assisting resources are available. For example, an information processing task could generate or consume public classical communication, private classical communication, secret key, quantum communication, and entanglement along with the consumption of many uses of a quantum channel. An optimization question then arises for future "quantum telephone companies": How can we optimally trade these resources for a given quantum channel? Here, we do not answer the full question for all five resources, but instead overview two different but related trade-off questions.

The transmission of information over a noisy quantum channel is one of the fundamental tasks in quantum Shannon theory. This theory bears many similarities with Shannon's classical theory, but it also admits several striking differences because a quantum channel has various capacities for information transmission, depending upon the type of resource that a sender wishes to transmit to a receiver and whether any assisting resources are available [1]. Several examples of resources that we can consider are public classical communication, private classical communication, secret key, quantum communication, and entanglement.

A quantum channel has a capacity for generating each of the aforementioned resources on its own, but one can also consider the task of transmitting some of the resources simultaneously, while using others for assistance. The simplest strategy for the simultaneous transmission of different resources is to use a particular communication strategy for one resource for a fraction of the channel uses and employ a different strategy for the other resource for the other fraction of the channel uses. This naive strategy is known as time-sharing, but it is often not the optimal strategy. For example, consider the case where a sender would like to transmit both classical and quantum information [4]. Time-sharing is the optimal strategy for certain channels such as the noiseless qubit channel and the quantum erasure channel, but it is not the optimal strategy for other channels such as the dephasing channel [4].

In recent work, we have made much progress in understanding two different trade-off settings [8, 6, 7, 2, 10, 5, 9]. The first setting involves the trade-off between classical communication, quantum communication, and entanglement when many uses of a quantum channel are available [8, 6, 7, 2, 10]. In this first setting (the CQE setting), we do not distinguish whether the classical communication is public or private. Our main result in these works is a theorem that we call the quantum dynamic capacity theorem. It gives the full trade-off between these resources regardless of whether a given protocol generates or consumes them in addition to the usage of the quantum channel. We also found an important formula that characterizes this trade-off, and we showed how additivity of it allows one to simplify the description of the three-dimensional capacity region [10]. A careful analysis of this formula even leads to an explicit analytic description of the capacity region for several channels such as erasure channels, dephasing channels, and cloning channels.

The second trade-off setting we have considered is that between public classical communication, private classical communication, and secret key [5, 9]. Our goal in the second setting (the RPS setting) was to study the information-theoretic analog of the Collins-Popescu analogy—this analogy states that classical communication, quantum communication, and entanglement tend to interact with each other similarly to the way that public classical communication, private classical communication, and secret key interact [3]. The latest work in Ref. [9] gives a capacity theorem that is analogous to the quantum dynamic capacity theorem. We also found another important formula that plays an analogous role in this setting, and we can compute and plot the capacity region for several examples of channels.

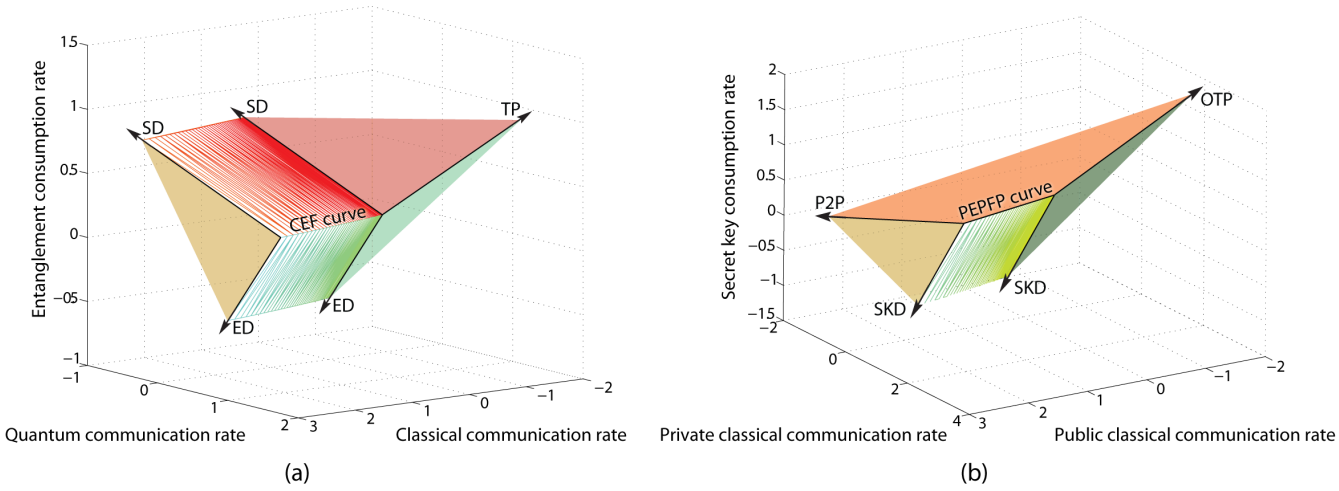

Figure 1: The capacity regions for a qubit dephasing channel with parameter $p = 0.2$. (a) The classically-enhanced father (CEF) trade-off curve lies along the boundary of the capacity region. The rest of the region is the combination of the CEF points with teleportation (TP), super-dense coding (SD), and entanglement distribution (ED). (b) The private dynamic triple trade-off for the same channel. P2P is in the direction of private-to-public transmission, SKD is in the direction of secret-key distribution, OTP is in the direction of the one-time pad protocol, and PEPFP is the publicly-enhanced private father trade-off curve. The region exhibits a non-trivial resource trade-off only on the surface below the PEPFP trade-off curve in the direction of secret key distribution. Observe that the two regions are dramatically different: (a) has two regions where non-trivial trade-offs occur, but (b) has only one.

We review here the important results and a simple example. The requisite protocols for achievability in the CQE setting are teleportation, super-dense coding, entanglement distribution, and a protocol we named the classically-enhanced father protocol [8]. The classically-enhanced father protocol exploits the "piggybacking" technique from Ref. [4] in order to "piggy-back" classical information "on top of" entanglement-assisted quantum codes. The cleanest method we have developed for proving the converse part of the capacity theorem is the catalytic, information-theoretic proof in Section 4 of Ref. [10]. This technique assumes that the sender and receiver have some amount of each resource in the CQE setting available for consumption and that they are trying to generate each resource as well. We then obtain bounds on the net rates for each resource, regardless of whether the protocol ends up generating or consuming it.

The important protocols for achievability in the RPS setting are a protocol we named the publicly-enhanced private father protocol [5], the one-time pad, private-to-public transmission, and secret key distribution. The publicly-enhanced private father protocol is analogous to the classically-enhanced father, and we even exploited similar techniques for proving its achievability. Section 4 of a recent paper also develops a catalytic, information-theoretic converse proof for this setting [9]. The main difference between this setting and the CQE setting is the lack of an analogy of the super-dense coding protocol, as Collins and Popescu first observed [3]. This has dramatic consequences for the shape of the RPS capacity region when compared to the CQE region.

One of the major contributions of these works is the analysis of the capacity regions for several examples of channels. Brádler *et al.* first realized that a particular class of channels, known as the Hadamard channels, have "single-letter" capacity regions, meaning that it is only necessary to evaluate the formulas for the region over one use of the channel [2]. Channels in this class include the practically relevant dephasing channels and cloning channels. Our later work follows up on this result in full generality for the CQE and RPS settings [10, 9], while also including proofs for the erasure channel. Figure 1 plots both capacity regions for the qubit dephasing channel with dephasing parameter equal to 0.2.

There are many questions to consider going forward for this line of inquiry. Are there other examples of channels besides Hadamard or erasure channels for which we can obtain analytic expressions for the capacity regions? Are there other interesting trade-offs to consider besides the ones that we have studied so far? What is the analysis for the capacity regions of bipartite quantum states instead of quantum channels? (We have a solution for the CQE region of a state in Ref. [7], but the analysis is not quite as clean as those for channels in Refs. [9,10].) What are the trade-offs for communication settings in network quantum Shannon theory? The answers to these and other questions should further illuminate the nature of information transmission over quantum channels.

We acknowledge the many useful conversations with our colleagues Kamil Brádler and Dave Touchette and those with our mentors David Avis, Igor Devetak, and Andreas Winter. We are especially grateful to Patrick Hayden for his guidance, insight, and encouragement.

References

[1] Charles H. Bennett and Peter W. Shor. Quantum channel capacities. *Science*, 303(5665):1784-1787, March 2004.

[2] Kamil Brádler, Patrick Hayden, Dave Touchette, and Mark M. Wilde. Trade-off capacities of the quantum Hadamard channels. To appear in *Physical Review A*, 2010. arXiv:1001.1732.

[3] Daniel Collins and Sandu Popescu. Classical analog of entanglement. *Physical Review A*, 65(3):032321, February 2002.

[4] Igor Devetak and Peter W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, 256(2):287-303, 2005.

[5] Min-Hsiu Hsieh and Mark M. Wilde. Public and private communication with a quantum channel and a secret key. *Physical Review A*, 80(2):022306, August 2009.

[6] Min-Hsiu Hsieh and Mark M. Wilde. *Theory of Quantum Computation, Communication, and Cryptography*, volume 5906 of *Lecture Notes in Computer Science*, chapter Optimal Trading of Classical Communication, Quantum Communication, and Entanglement, pages 85-93. Springer-Verlag, May 2009.

[7] Min-Hsiu Hsieh and Mark M. Wilde. Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. To appear in the *IEEE Transactions on Information Theory*, 2010. arXiv:0901.3038.

[8] Min-Hsiu Hsieh and Mark M. Wilde. Entanglement-assisted communication of classical and quantum information. To appear in the *IEEE Transactions on Information Theory*, 2010. arXiv:0811.4227.

[9] Mark M. Wilde and Min-Hsiu Hsieh. Public and private resource trade-offs for a quantum channel, May 2010. arXiv:1005.3818.

[10] Mark M. Wilde and Min-Hsiu Hsieh. The quantum dynamic capacity formula of a quantum channel. April 2010. arXiv:1004.0458.

Mark M. Wilde *is a postdoctoral fellow with the Quantum Computing Group in the School of Computer Science at McGill University.* ***Min-Hsiu Hsieh*** *is with the ERATO-SORST Quantum Computation and Information Project of the Japan Science and Technology Agency in Tokyo, Japan. Both completed their PhDs in Electrical Engineering in 2008 at the University of Southern California under the supervision of Todd Brun. The opinions expressed here are their own and do not reflect those of any other organization or individual.*