Advances in classical communication for network quantum information theory

Omar Fawzi,[1] Patrick Hayden,[1] Ivan Savov,[1] Pranab Sen,[2] and Mark M. Wilde[1]
[1] *School of Computer Science, McGill University, Montréal, Québec H3A 2A7, Canada*
[2] *Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India*
(Dated: August 25, 2011)

Introduction and Review. Classical network information theory has been a vibrant area of research [5], ever since Shannon's first paper on the topic [20]. The area considers channels with multiple senders, multiple receivers, or relay stations in between, and the senders attempt to transmit messages to some or all of the receivers. Usually one demands that the average probability of error for these transmissions vanishes in the limit of a large number of uses of the channel. Researchers have devised a variety of clever approaches for the encoding part of the transmission, but nearly every decoder employed in information-theoretical proofs is a "jointly-typical decoder" [5], which has been problematic to generalize to network *quantum* information theory. The impression of quantum information researchers might be that the coding theorem of Holevo [11], Schumacher, and Westmoreland [17] is sufficient to determine good classical communication rates over quantum channels with multiple senders and receivers, but this is far from the case.

The algorithm that specifies a classical jointly typical decoder is rather simple [31]. The receiver combines the sequence output from the channel and a particular codeword sequence, and asks, "Are these sequences jointly typical?", which is akin to determining whether the empirical joint distribution for the sequences is close to the true joint distribution that generated them [32]. The receiver asks this question for every codeword in the codebook until the answer to the question is "yes," at which point he decodes the received sequence as the codeword that is jointly typical with it. For a point-to-point channel, there are two different types of errors that can occur for such a decoder:

1. the received sequence is not jointly typical with any codeword in the codebook, or

2. there is some codeword other than the transmitted one that is jointly typical with the received sequence.

Assuming a random choice of code simplifies the error analysis so that as long as the rate of the code is less than the mutual information between the input random variable and output random variable, the probabilities for both of the above errors vanish in the asymptotic limit of many channel uses.

For a multiple access channel with two spatially separated senders and one receiver, there are two independent codebooks for each sender. The jointly typical decoder operates in a similar fashion, with the receiver now scanning through all codeword pairs and computing whether they are jointly typical with the received output from the channel [33]. As soon as he finds such a codeword pair, he declares the senders' messages to be the ones associated with the corresponding codewords. There are now four different types of errors that can occur:

1. No codeword pair is jointly typical with the received sequence.

2. The transmitted codeword for the first sender and some codeword from the second sender's codebook, other than the transmitted one, are jointly typical with the received sequence.

3. Some codeword from the first sender's codebook, other than the transmitted one, and the transmitted codeword of the second sender are jointly typical with the received sequence.

4. Some codewords other than the transmitted ones (for both senders) are jointly typical with the received sequence.

Assuming a random choice of both senders' codes again simplifies the error analysis. The transmission rates for both senders can be bounded such that the probabilities for all of the above errors vanish in the asymptotic limit of many channel uses. This same type of error analysis for the jointly typical decoder generalizes for nearly every type of encoding that has been devised for broadcast channels, interference channels, relay channels, channels with state, etc. [5]. It appears to have universal application as a decoder in nearly every setting in classical information theory.

In light of the importance that such a jointly typical decoder has for classical information theory, it is clear that a similar type of decoder would be just as important for quantum information theory. Holevo [11], Schumacher, and Westmoreland [17] (HSW) made great progress early on in this direction by constructing a positive operator-valued measure (POVM) from typical and conditionally typical projectors for quantum states received from the quantum channel. They employed the same idea as Shannon's for the encoding, by selecting a code randomly, but the important breakthrough of their work was the construction of the decoding POVM and their ensuing error analysis which demonstrated that the Holevo information is an achievable rate for classical communication over a quantum channel. One might say that their constructed decoder is a "quantum jointly typical decoder." Some years later, Hayashi and Nagaoka significantly simplified the HSW error analysis by introducing a fundamental operator inequality [9]. The error analysis for point-to-point channels with their operator inequality became directly parallel to the aforementioned analysis for classical jointly typical decoding—it showed how we could think of the error as breaking up into two terms, one being the probability that the transmitted codeword is not typical, and the other the probability that some other codeword is typical with the detected channel output. Many researchers have subsequently employed the Hayashi-Nagaoka operator inequality in different contexts [3, 10, 12, 15, 22, 24, 28].

After the breakthrough of HSW, it was not long before several quantum information researchers began to consider network quantum information theory, beginning with the problem of transmitting classical information over quantum multiple access channels with two senders and one receiver [12, 26]. Though, at the outset, it was not clear how to generalize the jointly typical decoder for classical multiple access channels to the quantum setting [4]—a straightforward modification of the HSW decoding POVM simply does not work. So Winter and others employed another approach called "successive decoding" in order to demonstrate achievable rates for quantum multiple access channels [12, 26]. This approach has the receiver decode each sender's codeword successively as though they are encoded for point-to-point channels, and it worked just fine for multiple access channels, but such an approach is not satisfactory for interference channels (channels with two senders and two receivers)—the strategy for achieving the best known inner bound on the capacity of the classical interference channel employs a jointly typical or "simultaneous" decoder [8]. Also, it is currently not known whether successive decoding can perform just as well as simultaneous decoding for the interference channel.

Summary of Results. Our group has developed new techniques that have yielded significant advances in network quantum information theory. We have established the existence of a quantum simultaneous decoder for two-sender quantum multiple access channels by using novel methods to deal with the non-commutativity of the many operators involved, and we have also applied this result in various scenarios, included unassisted and assisted classical communication over quantum multiple access channels, quantum broadcast channels, and quantum interference channels [6, 16, 18, 25, 27]. Prior researchers have already considered classical communication over quantum multiple-access and broadcast channels [12, 26, 29, 30], but our work extends and in some cases improves upon this prior work [25]. Also, we are the first to make progress on the capacity of the quantum interference channel [6, 16, 18], which is a channel with two senders and two receivers, where one sender is interested in communicating with one receiver and the other sender with the other receiver. The aim of the proposed talk at QIP 2012 is to summarize this recent work and its applications as well as to discuss new avenues for network quantum information theory that may make use of these results. Below we provide a brief summary of each of the above results, highlighting the approaches employed.

Our first result is a proof that a quantum simultaneous decoder works for two-sender quantum multiple access channels, where the senders want to transmit classical information without any entanglement assistance [6, 16]. We employ typical projectors in a square-root decoding POVM, much like the HSW decoder, but our proof differs from theirs in several significant ways. We have to order operators in a very particular way due to the general non-commutativity of quantum states and typical projectors—other orderings simply fail to lead to an error analysis where we can make all four types of errors vanish as they do in the classical case. So the first insight is to layer "smaller" typical projectors inside "larger ones", and the second insight is to "smooth" the states output from the channel by a different typical projector before applying the Hayashi-Nagaoka operator inequality. For technical details, we invite the program committee to consult Theorem 2 of Ref. [6] (attached). Our error analysis there bears some similarities with the classical error analysis mentioned above, but it differs from it in that we handle each of the four types of errors in a different way. This asymmetry in the error analysis is not present in the classical proof, but, for the moment, it seems to be necessary for the quantum case. We then go on to exploit this result for the quantum interference channel (a channel with two classical inputs and two quantum outputs) by determining the capacity of such a channel when it exhibits "very strong" or "strong" interference.

The second part of our proposed talk will summarize further work by one of us [18]. In Ref. [18], Sen has developed several new techniques that should find general use in quantum information theory. First, he shows how to construct a useful notion of an "intersection" projector Π from two projectors Π_A and Π_B such that the following operator inequality holds

$$\Pi \leq \Pi_A \Pi_B \Pi_A. \tag{1}$$

(We point the program committee to Lemma 4 in the attached write-up [18].) We should mention that others have exploited a similar idea in various other contexts: quantum walks [21], quantum interactive proofs [23], and witness-preserving amplification in QMA [14]. Next, he has determined a novel way of bounding from below the success probability of a sequence of projectors acting on a state. This lower bound is in terms of a sum over the trace of the orthogonal complements of these projectors taken against the same state:

$$\operatorname{Tr}\left\{\Pi_k \cdots \Pi_1 \rho \Pi_1 \cdots \Pi_k\right\} \geq 1 - 2\sqrt{\sum_{i=1}^{k} \operatorname{Tr}\left\{\left(I - \Pi_i\right)\rho\right\}}, \tag{2}$$

where ρ is a density operator and $\Pi_1, \ldots, \Pi_k$ are orthogonal projectors. The above bound follows from a simple "Pythagorean" geometrical argument (see Lemma 3 in the attached write-up [18]). One nice application of the above bound is a simplified proof of Giovannetti *et al.*'s sequential decoder [7]. Such a sequential decoder is perhaps more analogous to the classical jointly typical decoder than is the HSW square-root decoder because it is operationally equivalent to asking in sequential order for all codewords in the codebook, "Is the i^{th} codeword a reasonable cause for the output of the channel?" Sen applies it both to this problem and then shows further applications of it to quantum simultaneous decoding, by constructing "detection" projectors from the conditionally typical projectors corresponding to the outputs of a quantum multiple access channel. The method of decoding is then simply to ask, in full analogy with the classical case, "Is the codeword pair $(x^n(i), y^n(j))$ a reasonable cause for the output from the channel?" By employing an error analysis using (1), (2), and the properties of typical projectors, Sen demonstrates that this decoding technique works well as long as the transmission rates of the senders lie within the channel's capacity region.

Another of Sen's contributions is to demonstrate that the best known achievable rate region for the classical interference channel is in fact achievable for the quantum interference channel, with Shannon mutual information quantities replaced by Holevo information quantities [18]. He does so by exploiting a recent correspondence between the Han-Kobayashi region and the Chong-Motani-Garg (CMG) region [1, 2, 13], some geometrical arguments concerning the CMG region, and the above two-sender quantum simultaneous decoder.

The above insights have led to some further results that we now mention (these will not be part of the proposed talk but are submitted as supplementary poster presentations for QIP 2012). First, we have leveraged the first method of proof to the case of entanglement-assisted classical communication over a quantum multiple access channel [27]. Hsieh *et al.* had already proved the achievability part of the entanglement-assisted multiple access channel channel capacity theorem with a successive decoding approach [12], but the contribution in Ref. [27] highlights how to achieve it with a quantum simultaneous decoder. This work exploits the same encoding technique of Ref. [12] combined with a quantum simultaneous decoder. The essential ideas behind the proof are similar to what we have described above for the unassisted case, but the mathematical techniques needed are slightly different. In addition, Ref. [27] demonstrates how to achieve the entanglement-assisted and unassisted quantum capacity regions of the multiple access channel (already found in Ref. [30]), by transforming the quantum simultaneous decoder into a coherent quantum simultaneous decoder. We exploited the proof technique of Ref. [6] to obtain the above results, but it is clear that we could have also used Sen's approach from Ref. [18]. These results might eventually be useful in determining achievable rates for entanglement-assisted classical communication over a quantum interference channel.

The other result we have obtained is a quantization [25] of Cover's superposition coding technique for the classical broadcast channel [5]. The resulting technique with a quantum simultaneous decoder leads to a capacity region for the quantum broadcast channel that is generally larger than that for the approach found previously [29], though the regions coincide whenever the broadcast channel is degraded. Nevertheless, there are important channels such as certain lossy bosonic broadcast channels that are not degraded, and it would be worthwhile to take advantage of this new encoding and decoding technique when transmitting data over such channels.

Closing Remarks. Much work still lies ahead in this direction. First and foremost, we have only been able to show that our quantum simultaneous decoder applies when decoding the messages from two senders, and it is not clear how to extend our techniques when decoding the messages of three or more senders (a straightforward generalization of our method does not generally work). Nevertheless, Sen has demonstrated achievability of the best known inner bound on the capacity of the quantum interference channel by exploiting the two-sender decoder and other geometrical arguments [18]. It is also likely that we could exploit the two-sender decoder to obtain natural generalizations of classical techniques that employ jointly typical decoders for recovering the messages of two senders. If we were to find a quantum simultaneous decoder for three or more senders, then it would help for quantizing many known results from classical information theory. This remains the topic of current investigation.

[1] Hon-Fah Chong, Mehul Motani, and Hari Krishna Garg. A comparison of two achievable rate regions for the interference channel. In *Proceedings of the USCD-ITA Workshop*, San Diego, California, USA, February 2006.

[2] Hon-Fah Chong, Mehul Motani, Hari Krishna Garg, and Hesham El Gamal. On the Han-Kobayashi region for the interference channel. *IEEE Transactions on Information Theory*, 54(7):3188–3195, 2008.

[3] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51:44–55, January 2005.

[4] Igor Devetak and Andreas Winter. Private communication, 2010.

[5] Abbas El Gamal and Young-Han Kim. Lecture notes on network information theory. January 2010. arXiv:1001.3404.

[6] Omar Fawzi, Patrick Hayden, Ivan Savov, Pranab Sen, and Mark M. Wilde. Classical communication

over a quantum interference channel. February 2011. arXiv:1102.2624.

[7] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Achieving the Holevo bound via sequential measurements. December 2010. arXiv:1012.0386.

[8] Te Sun Han and Kingo Kobayashi. A new achievable rate region for the interference channel. *IEEE Transactions on Information Theory*, 27(1):49–60, January 1981.

[9] Masahito Hayashi and Hiroshi Nagaoka. General formulas for capacity of classical-quantum channels. *IEEE Transactions on Information Theory*, 49(7):1753–1768, 2003.

[10] Patrick Hayden, Peter W. Shor, and Andreas Winter. Random quantum codes from Gaussian ensembles and an uncertainty relation. *Open Systems & Information Dynamics*, 15:71–89, March 2008.

[11] Alexander S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory*, 44(1):269–273, 1998. arXiv:quant-ph/9611023.

[12] Min-Hsiu Hsieh, Igor Devetak, and Andreas Winter. Entanglement-assisted capacity of quantum multiple-access channels. *IEEE Transactions on Information Theory*, 54(7):3078–3090, 2008.

[13] Kingo Kobayashi and Te Sun Han. A further consideration on the HK and the CMG regions for the interference channel. In *Proceedings of the Information Theory and Applications Workshop*, 2007.

[14] C. Marriott and J.Watrous. Quantum arthur-merlin games. *Computational Complexity*, 14(2):122152, 2005.

[15] Milán Mosonyi and Nilanjana Datta. Generalized relative entropies and the capacity of classical-quantum channels. *Journal of Mathematical Physics*, 50(7):072104, 2009.

[16] Ivan Savov, Omar Fawzi, Mark M. Wilde, Pranab Sen, and Patrick Hayden. Quantum interference channels. *Proceedings of the 2011 Allerton Conference on Communication, Control, and Computing*, February 2011. arXiv:1102.2955.

[17] Benjamin Schumacher and Michael D. Westmoreland. Sending classical information via noisy quantum channels. *Physical Review A*, 56(1):131–138, July 1997.

[18] Pranab Sen. Sequential decoding for some channels with classical input and quantum output, July 2011. see attached PDF.

[19] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[20] Claude E. Shannon. Two-way communication channels. In J. Neyman, editor, *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*, volume 1, pages 611–644, Berkeley, California, June 20–July 30 1961. University of California Press.

[21] M. Szegedy. Spectra of quantized walks and a $\sqrt{\delta\epsilon}$ rule. *quant-ph/0401053*, 2004.

[22] Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. July 2010. arXiv:1007.5456.

[23] J. Watrous. Zero-knowledge against quantum attacks. *In Proc. 38th ACM Symp. on Theory of Computing (STOC)*, 2006.

[24] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. June 2011. arXiv:1106.1445.

[25] Mark M. Wilde. Quantum simultaneous decoding for the quantum broadcast channel. July 2011. see attached PDF.

[26] Andreas Winter. The capacity of the quantum multiple-access channel. *IEEE Transactions on Information Theory*, 47(7):3059–3065, 2001.

[27] Shen Chen Xu and Mark M. Wilde. Sequential, successive, and simultaneous decoders for entanglement-assisted classical communication. July 2011. arXiv:1107.1347.

[28] Jon Yard and Igor Devetak. Optimal quantum source coding with quantum information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55(11):5339–5351, November 2009.

[29] Jon Yard, Patrick Hayden, and Igor Devetak. Quantum broadcast channels. arXiv:quant-ph/0603098, March 2006.

[30] Jon Yard, Patrick Hayden, and Igor Devetak. Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions. *IEEE Transactions on Information Theory*, 54(7):3091–3113, July 2008.

[31] It is computationally difficult to execute in practice, but this is not a concern in the paradigm of quantum Shannon theory.

[32] A question that is loosely equivalent to "Are the two sequences jointly typical?" is "Is the codeword a reasonable cause for the received sequence?" [19].

[33] Whenever a jointly typical decoder is employed in a setting where more than one sequence is being compared with the channel sequence, it is also known as a "simultaneous decoder" [5].