Multi-party zero-error classical channel coding with entanglement

(extended abstract of arXiv:1403.5003)

Teresa Piovesan[*], Giannicola Scarpa[†], and Christian Schaffner[‡]

We study the effects of quantum entanglement on the performance of two classical zero-error communication tasks among multiple parties. Both of these are generalizations of the two-party zero-error channel coding problem, where a sender and a receiver want to perfectly communicate messages through a one-way classical noisy channel. The field of classical zero-error information theory was started by Shannon's seminal paper on zero-error channel capacity [Sha56] and it has developed and influenced a large research area in between information theory, combinatorics, and computer science. For example, to solve an open problem posed by Shannon [Sha56], Lovász [Lov79] introduced a parameter, known as the Lovász theta number, defined by a positive semidefinite program which bounds a combinatorial quantity. This approach has proven to be very fruitful for many other hard combinatorial problems. Recently, a quantum generalization of zero-error information theory has been developed [MAC$^+$06, Dua09, CCH11, DSW13] and in particular, [CLM+10] and [BBL$^+$13] studied the effect of sharing an entangled state in classical zero-error communication problems between two parties. Along this line of research, we study if entanglement helps in two multi-party scenarios of classical zero-error channel coding. Our most interesting result shows that entanglement allows for a peculiar amplification of information, which cannot happen classically. Before a description of the settings and our findings, we give a brief overview of the two-party channel-coding problem.

The Two-Party Setting Suppose Alice wants to send a message to Bob but they can communicate only through a one-way noisy channel. How much information can she send to him on average such that Bob learns Alice's message with zero probability of error? This question was raised by Shannon in [Sha56] where he proved that multiple uses of the channel can be on average strictly more efficient than a single use. He also showed that the problem can be cast in graph-theoretic terms.

A one-way classical noisy channel $\mathcal{N}$ that connects Alice and Bob is fully characterized by its finite input set V, its finite output set W and a probability distribution $\mathcal{N}(\cdot|v)$ for every $v \in V$. Two inputs $u, v \in V$ are said to be confusable if they can lead to the same output, *i.e.*, there exists $w \in W$ such that $\mathcal{N}(w|v)\mathcal{N}(w|u) > 0$. To a channel $\mathcal{N}$, we associate a *confusability graph* G whose vertices are the set of inputs, and two vertices are adjacent if and only if they are confusable. A set of inputs can be used for zero-error communication if they are pairwise non-confusable. Hence the largest size m of a message set Alice can employ for one use of the channel, called the *one-shot capacity*, is the independence number $\alpha(G)$. (Equivalently, Alice can communicate at most $\log \alpha(G)$ bits of information.) The *Shannon capacity* of a (channel with confusability) graph G, $c(G) = \lim_{n\to\infty} \frac{1}{n} \log \alpha(G^{\boxtimes n})$, is the maximum average number of

[*] Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands.

[†] Universitat Autonoma de Barcelona, Spain.

[‡] Institute for Logic, Language and Computation (ILLC), University of Amsterdam, The Netherlands and Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands.

bits that can be communicated with zero-error. Here, $G^{\boxtimes n}$ is the strong graph power of G and it is exactly the confusability graph of n channel uses.

The variant of this problem where Alice and Bob might share an entangled state was introduced recently in [CLM+10] and the entanglement-assisted variant of the independence number $\alpha^*(G)$ and of the Shannon capacity $c^*(G)$ defined. They also showed that entanglement can improve the one-shot capacity of a channel, *i.e.*, there exists graph G for which $\alpha^*(G) > \alpha(G)$. Moreover, [LMM$^+$12] and [BBG12] exhibit examples of channels for which sharing an entangled state improves the zero-error channel capacity, *i.e.*, graphs G with $c^*(G) > c(G)$.

The entanglement-assisted protocol for a single use of a channel is the following. To send a message $x \in [m]$ to Bob, Alice performs a measurement $\{A_x^u\}_{u \in V}$ on her part of the entangled state and sends the outcome $u \in V$ through the channel $\mathcal{N}$. With probability $\mathcal{N}(w|v)$, Bob receives $w \in W$ and uses this information to perform a measurement $\{B_w^y\}_{y \in [m]}$ on his side of the entangled state getting the message y as outcome. In the zero-error scenario, we require y to be equal to x with probability one. In this work, we extend this entanglement-assisted communication scenario to two multy-party settings.

1 Multiple receivers

Consider a single sender that wants to send a common message to ℓ receivers. The sender is connected to each of the receivers through a classical channel. One of the many applications of this model, known as *compound channels*, is message broadcasting. The classical zero-error version of the compound channels was introduced by [CKS90]. Consider a family of channels $\boldsymbol{\mathcal{N}} = \{\mathcal{N}_1, \ldots, \mathcal{N}_\ell\}$ with the same input set V where $\mathcal{N}_k$ connects the sender with the k-th receiver. A common input $v \in V$ is sent to all the receivers and the k-th receiver gets output w_k according to the distribution $\mathcal{N}_k(w_k|v)$. The goal is for each receiver is to retrieve the original input v with zero probability of error.

We study the entanglement-assisted version of this problem focusing on the particular instance where all the channels are equal. Similarly to the two-party situation, we can reformulate the problem in graph-theoretical terms. We denote by $\alpha_{1,\ell}(G)$ and $\alpha^*_{1,\ell}(G)$ the one-shot compound-channel capacities of one sender and ℓ receivers, respectively without and with a shared entangled state between the parties. Similarly, we use $c_{1,\ell}(G)$ and $c^*_{1,\ell}(G)$ for the *compound-channel capacity.*

Intuitively, one would expect that due to monogamy of entanglement, as the number of receivers goes to infinity, entanglement does not give an advantage. We are able to prove something stronger showing that entanglement does not help in the one-shot compound-channel capacity whenever the number of receivers is above a certain threshold, which depends only on the number of outputs of the channel (in the following theorem, $\theta'_e(G)$ denotes the edge clique cover number of G plus the number of isolated vertices).

Theorem 1. *For any graph G, if $\ell \geq \theta'_e(G)$ then $\alpha^*_{1,\ell}(G) = \alpha_{1,\ell}(G)$.*

The key idea of the proof is to use monogamy of non-signaling distributions [MAG06]. A direct consequence of Theorem 1 is that for any finite number of uses of the channel, entanglement does not improve the communication when the number of receivers is large enough.

This result does not imply, however, that entanglement is useless for this communication task. For every fixed number of receivers $\ell \geq 1$, we can build channels for which the entanglement-assisted compound-channel capacity is strictly greater than the classical compound-channel capacity, *i.e.*, for every fixed ℓ exists G such that $c^*_{1,\ell}(G) > c_{1,\ell}(G)$. To show the existence we use a protocol from [BBL$^+$13], which gives a lower-bound on the entanglement-assisted capacity based on quantum teleportation [BBC$^+$93].

2 Multiple senders

Suppose there are ℓ Alices, each of whom gets access to a classical channel which connects her to a single Bob. We assume that inputs of one sender cannot be confused with inputs from another sender. In other words, the receiver knows which one of the senders sent him the message. Equivalently, this problem can be cast as a two-party situation where Alice has the freedom to use one among a given set of channels and Bob learns for free which channel has been used. As before, we focus on the zero-error scenario which can be reformulated using graph theory. In the classical scenario, this problem was introduced by Alon [Alo98] and further studied in [AL07]. In this latter paper, the authors showed that it is possible to assign channels to senders such that only *privileged subsets* of them are allowed to communicate with high capacity. In particular, it is possible to ensure that every group of $t-1$ cooperating senders can transmit at low capacity while if the group has at least t senders, they can communicate at high capacity. To obtain this result, it is essential that different senders have access to different channels. Unfortunately, we do not know how to study the entanglement-assisted setting for this general problem and we restrict ourselves to the situation where all channels are equal. However, one of our results (Theorem 3) has a similar flavor as [AL07].

We denote by $\alpha_{\ell,1}(G)$ the maximum number of messages that cooperating senders are able to communicate to the receiver with zero error and one use of the channels (with confusability graph G). As before, we denote by $c_{\ell,1}(G)$ the asymptotic quantity. The entanglement-assisted versions $\alpha^*_{\ell,1}(G)$ and $c^*_{\ell,1}(G)$ are the analogous quantities when the parties might share an entangled state (since the senders are allowed to collaborate, we can effectively picture the entangled state as being bipartite).

Not surprisingly, if entanglement improves the communication in the two-party case, we show that such a separation extends also to the multi-sender setting independently from the number of senders (Theorem 2). The idea is that if each Alice is individually able to perfectly communicate m messages using entanglement, then ℓ cooperating Alices can transmit at least $\ell \cdot m$ messages with entanglement.

Theorem 2. *For any graph G with $\alpha^*(G) > \alpha(G)$, we have $\alpha^*_{\ell,1}(G) > \alpha_{\ell,1}(G)$ for every $\ell \in \mathbb{N}$. Furthermore, for any graph G with $c^*(G) > c(G)$, we have $c^*_{\ell,1}(G) > c_{\ell,1}(G)$ for every $\ell \in \mathbb{N}$.*

More interestingly, we present examples of graphs for which ℓ senders have a joint entanglement-assisted strategy that allows them to communicate strictly more than the sum of their individual capabilities (Theorem 3). That is, in the entanglement-assisted setting, if each Alice can transmit m messages there is a joint strategy that allows to send strictly more that $\ell \cdot m$ messages. Note that this effect cannot happen in the classical case. It is known that cooperation among senders with the same channel does not improve the communication neither in the finite nor the asymptotic number of channel uses [Sha56]. Hence, this phenomenon is a peculiarity of the entanglement-assisted setting.

Theorem 3. *In the entanglement-assisted setting, for every $n \in \mathbb{N}$, there exists a channel and a number of senders k such that cooperation among senders allows them to send, with n uses of the channels, strictly more messages than the sum of their individual possibilities.*

This result is surprising and is the one that requires the most technical proof. We use properties of a class of orthogonality graphs[1], of the Lovász theta number together with a parameter introduced in [BBL+13]. It is an interesting open problem whether this improvement gained by cooperation extends also to the asymptotic regime.

[1] The orthogonality graph Ω_k has all the vectors $\{\pm 1\}^k$ as vertex set and two vectors are adjacent if orthogonal.

References

[AL07] N. Alon and E. Lubetzky. Privileged users in zero-error transmission over a noisy channel. *Combinatorica*, 27(6):737–743, 2007.

[Alo98] N. Alon. The shannon capacity of a union. *Combinatorica*, 18:301–310, 1998.

[BBC$^+$93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.

[BBG12] J. Briët, H. Buhrman, and D. Gijswijt. Violating the Shannon capacity of metric graphs with entanglement. *Proceedings of the National Academy of Sciences*, 2012.

[BBL$^+$13] J. Briët, H. Buhrman, M. Laurent, T. Piovesan, and G. Scarpa. Zero-error source-channel coding with entanglement. *arXiv:1308.4283*, 2013.

[CKS90] G. Cohen, J. Körner, and G. Symonyi. Zero-error capacities and very different sequences. *Sequences: combinatorics, compression, security and transmission*, 144–155, Springer-Verlag, 1990.

[CK98] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[CCH11] T. S. Cubitt, J. Chen, and A. W. Harrow. Superactivation of the asymptotic zero-error classical capacity of a quantum channel. *IEEE Transactions on Information Theory*, 57(12):8114 –8126, 2011.

[CLM+10] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter. Improving zero-error classical communication with entanglement. *Physical Review Letters*, 104:230503–230506, 2010.

[Dua09] R. Duan. Super-activation of zero-error capacity of noisy quantum channel. *arXiv:0906.2527*, 2009.

[DSW13] R. Duan, S. Severini, and A. Winter. Zero-error communication via quantum channels, noncommutative graphs, and a quantum Lovász number. *IEEE Transactions on Information Theory*, 59(2):1164 –1174, 2013.

[GKV94] L. Gargano, J. Körner, and U. Vaccaro. Capacities: From information theory to extremal set theory. *Journal of Combinatorial Theory, Series A*, 68(2):296–316, 1994.

[LMM$^+$12] D. Leung, L. Mančinska, W. Matthews, M. Ozols, and A. Roy. Entanglement can increase asymptotic rates of zero-error classical communication over classical channels. *Communications in Mathematical Physics*, 311:97–111, 2012.

[Lov79] L. Lovász. On the Shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25(1):1–7, 1979.

[MAG06] Ll. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, 2006.

[MAC$^+$06] R. A. C. Medeiros, R. Alleaume, G. Cohen, and F. M. de Assis. Quantum states characterization for the zero-error capacity. *arXiv:0611042*, 2006.

[Sha56] C. E. Shannon. The zero error capacity of a noisy channel. *IRE Transactions on Information Theory*, IT-2(3):8–19, 1956.

[Wyn75] A. D. Wyner. The wire-tap channel. *Bell Systems Technical Journal*, 54(8):1355–1387, 1975.