Efficient Quantum Communication over Noisy Quantum Channels

Joseph M. Renes,[1] David Sutter,[1] Frédéric Dupuis,[2,3] and Renato Renner[1]

[1] *Institute for Theoretical Physics, ETH Zurich, Switzerland*
[2] *Department of Computer Science, Aarhus University, Denmark*
[3] *Faculty of Informatics, Masaryk University, Brno, Czech Republic*

A major challenge in information theory is to devise schemes for reliable communication via noisy channels that achieve high rates and yet can be efficiently implemented. We construct explicit protocols for quantum communication that achieve a rate not less than the coherent information. For Pauli and erasure channels we also present efficient encoding and decoding algorithms — based on polar codes — with a complexity that is essentially linear in the blocklength. Furthermore, these communication schemes do not require the sender and receiver to share any preshared entanglement before the protocol begins. Due to the close connection between channel coding and entanglement distillation our protocol can also be used for the latter task. We discuss how the scheme can be modified for efficient secret distillation and private channel coding at a rate that is not less than the private information.

Full paper[1]: http://arxiv.org/abs/1307.1136

Motivation — efficient quantum channel coding

Quantum channel coding denotes the scenario where two parties, Alice and Bob, connected by a quantum channel would like to transmit reliably a maximal amount of quantum information. The highest rate at which quantum information can be transmitted asymptotically reliably per channel use is characterized by the quantum capacity [1–3]. It is of fundamental importance to derive coding schemes that are computationally efficient (unlike computer scientists, information theorists usually call a protocol *efficient* if its computational complexity is essentially linear in the blocklength) while achieving optimal rates.

Polar codes, introduced in 2008 by Arıkan [4], are the first family of classical error-correcting codes which meet these two requests. They have been generalized to the quantum setup and shown to be almost optimal in terms of rate and simulaneously efficient for a lot of quantum information processing tasks [5, 6]. By 'almost optimal' we mean that these protocols achieve the non-regularized capacity expressions, i.e., the channel coherent information for the task of quantum channel coding over a quantum channel. Unfortunately, up to date all previous schemes based on quantum polar codes suffer from two important drawbacks. First is the need for noiseless entanglement to be shared by the sender and receiver prior to the start of the protocol. Second, the aforementioned protocols only achieve optimal rates for symmetric quantum channels, which are channels whose coherent information is maximized for a maximally entangled input state.

The key strength of quantum polar codes is their (computationally) efficient implementation while achieving high rates which makes them attractive for practical applications. However at the same time their need for preshared entanglement reduces their appealing characteristics — at least from a practical point of view — as generating entanglement still remains a challenging task. However also from a theoretical point of view the need for preshared entanglement is an undesirable feature that one would like to overcome.

[1] This work was not submitted to QIP 2014 due to a conflict of interest as RR was serving as TPC chair.

Contribution — efficient protocol at almost optimal rate without any preshared entanglement

In our work, we introduce new protocols for the task of entanglement distillation and quantum channel coding based on a concatenated two-level construction. We prove that the protocols that define a CSS code achieve the channel coherent information. For the use of quantum polar codes — which are CSS codes — we can show in addition that the computational complexity of the protocols is essentially linear in the blocklength for Pauli and erasure channels. The main results of our work can be summarized as:

1. **Almost optimal rate:** Our entanglement distillation and quantum channel coding protocols achieve the channel coherent information (i.e., the non-regularized quantum capacity) without any assumptions on the channel such as symmetry. [Precise statement given by Theorem 2 in the full version.]

2. **Efficient:** For Pauli and erasure channels the computational complexity of the protocols is $O(N \log N)$ where N denotes the blocklength. [Precise statement given by Propositions 4 and 5 in the full version.]

3. **Reliable:** The error probability of the two protocols decays exponentially in the square root of the blocklength. [Precise statement given by Corollary 9 in the full version.]

4. **No preshared entanglement:** The protocols do not require any preshared entanglement (not even a small amount).

Our protocols can be modified for the task of *secret-key distillation* and *private channel coding* inheriting all the desirable properties such as achieving the channel private information, being computationally efficient for Pauli and erasure channels and not requiring any preshared key between the two parties before the protocol starts. [See Sections VI and VII in the full version.]

Relevance within quantum information theory

Our protocols show for the first time that it is compatible to have computationally efficient protocols (with an essentially linear complexity) that achieve the non-regularized quantum capacity of an arbitrary quantum channel without requiring any entanglement assistance. In addition, they have an immediate advantage when being used in practice, namely that no noiseless entanglement has to be distributed between Alice and Bob before the protocol starts. This considerably simplifies the task of channel coding or entanglement distillation at high rates which are often used as a primitive inside different quantum information processing protocols.

Relation to previous work

Previous protocols that perform entanglement distillation or quantum channel coding are either computationally inefficient or do not achieve the channel coherent information. This is a direct consequence of the fact that there do not exist efficient quantum error correcting codes (except of the recent quantum polar codes [5, 6]) that are capacity-achieving while being (computationally) efficient. The protocol introduced in [5] can be used for efficient entanglement distillation and quantum channel coding at the drawback that a certain amount of preshared entanglement is needed and that the channel coherent information is only achieved for symmetric channels. Very recent results show that the amount of required entanglement assistance can be very large for certain channels such as a noisy depolarizing channel [7], which emphasizes the need of the presented protocol.

Closing remarks

There are a few interesting currently unsolved questions regarding the protocols introduced in our work. Is it possible that this two-level construction achieves rates that are strictly higher than the non-regularized capacities? [This is discussed in detail in Sections IV and V in the full version.] A positive answer would be of large interest as currently there are only very few ad hoc schemes known that can achieve rates beyond the channel coherent information [8, 9]. We could link this problem to the question whether (quantum) polar codes are universal which is not fully understood so far and displays an active research branch inside the (classical) polar coding community.

In recent work, we showed that the two-level construction used in this work can be successfully applied in classical cryptography to perform efficient one-way secret-key agreement and efficient private channel coding at the optimal rate [10].

[1] Seth Lloyd, "Capacity of the noisy quantum channel," Physical Review A **55**, 1613–1622 (1997).

[2] Peter W. Shor, "The quantum channel capacity and coherent information," Presented at the MSRI Workshop on Quantum Computation (2002).

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

[4] Erdal Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," IEEE Transactions on Information Theory **55**, 3051 –3073 (2009).

[5] Joseph M. Renes, Frédéric Dupuis, and Renato Renner, "Efficient polar coding of quantum information," Physical Review Letters **109**, 050504 (2012).

[6] Mark M. Wilde and Saikat Guha, "Polar codes for degradable quantum channels," IEEE Transactions on Information Theory **59**, 4718–4729 (2013).

[7] Hamed Hassani, Joeseph M. Renes, and David Sutter, "Entanglement assistance for quantum polar codes," (2014), in preparation.

[8] David P. DiVincenzo, Peter W. Shor, and John A. Smolin, "Quantum-channel capacity of very noisy channels," Physical Review A **57**, 830–839 (1998).

[9] Graeme Smith and Jon Yard, "Quantum communication with zero-capacity channels," Science **321**, 1812–1815 (2008).

[10] Joseph M. Renes, Renato Renner, and David Sutter, "Efficient one-way secret-key agreement and private channel coding via polarization," in *Advances in Cryptology - ASIACRYPT 2013*, Lecture Notes in Computer Science 8269, edited by Kazue Sako and Palash Sarkar (Springer Berlin Heidelberg, 2013) pp. 194–213.