Efficient Approximation of Quantum Channel Capacities

David Sutter,[1] Tobias Sutter,[2] Peyman Mohajerin Esfahani,[2] and Renato Renner[1]

[1] *Institute for Theoretical Physics, ETH Zurich, Switzerland*

[2] *Automatic Control Laboratory, ETH Zurich, Switzerland*

The capacity of a quantum channel characterizes the ultimate rate at which information can be transmitted reliably over the channel. Its computation, however, turns out to be difficult. Here we introduce a framework that connects recent techniques from convex optimization with quantum information theoretic problems. It can be used to derive an iterative algorithm with an attractive rate of convergence to efficiently approximate the capacity of channels with a classical input and a quantum mechanical output. The method, using the idea of a universal encoder, can be extended to approximate the Holevo capacity for channels with a quantum mechanical input and output. In particular, we show that the problem of approximating the Holevo capacity can be reduced to a multidimensional integration problem. For certain families of channels we prove that the complexity to derive an ε-close solution to the Holevo capacity is subexponential or even polynomial in the problem size. We provide several examples to illustrate the performance of the approximation scheme in practice.

Full version: http://arxiv.org/abs/1407.8202

Motivation — quantum channel capacities

Consider the scenario where a sender wants to transmit information over a noisy channel to a receiver. Information theory says that there exists operational quantities called *channel capacities* characterizing the maximal amount of information that can be transmitted, asymptotically reliably per channel use [1]. Depending on the channel and allowed auxiliary resources, there exists a variety of different capacities for different communication tasks. For a lot of these tasks, the corresponding capacity can be recast as an optimization problem. Some of them seem to be intrinsically more difficult than others, however none of them in general is straightforward to compute efficiently.

Due to its operational significance, knowing the capacity of a channel is of fundamental importance. As the capacity in general does not admit a closed form expression, using an algorithm to numerically approximate it is basically the only possibility to determine its value. In particular as the channel dimension increases the computational complexity of the approximation scheme becomes important.

In this work, we focus on the scenario of sending classical data over a classical-quantum (cq) or a quantum-quantum (qq) channel. A cq channel is described by a mapping $\rho : \mathcal{X} \ni x \mapsto \rho_x \in \mathcal{D}(\mathcal{H})$, where $\mathcal{X} = \{1, \ldots, N\}$ denotes the input alphabet and $\mathcal{D}(\mathcal{H})$ the set of density operators on a Hilbert space $\mathcal{H}$ with $M := \dim \mathcal{H}$. We consider the setup of an additional input constraint of the form $\langle p, s \rangle \leq S$, where S is some non-negative constant, $s : \mathcal{X} \to \mathbb{R}_{\geq 0}$ be some cost function and $p \in \Delta_N$ denotes the input distribution. As shown by Holevo, Schumacher and Westmoreland [2–4], the capacity of a cq channel ρ satisfying the input constraint is given by

$$C_{\mathsf{cq},S}(\rho) = \begin{cases} \max\limits_{p \in \Delta_N} & H\left(\sum_{i=1}^N p_i \rho_i\right) - \sum_{i=1}^N p_i H(\rho_i) \\ \text{s. t.} & \langle p, s \rangle \leq S. \end{cases} \tag{1}$$

A qq channel is described by a completely positive trace preserving (cptp) map $\Phi : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$, where $\mathcal{S}(\mathcal{H})$ denotes the space of bounded operators acting on some Hilbert space $\mathcal{H}$ with unit trace and $n := \dim \mathcal{H}_A$. The classical capacity of Φ was shown to be [2, 4] $C(\Phi) = \lim_{k\to\infty} \frac{1}{k} C_{\mathcal{X}}(\Phi^{\otimes k})$, where

$$C_{\mathcal{X}}(\Phi) = \sup_{\{p_i,\rho_i\}} H\left(\sum_i p_i \Phi(\rho_i)\right) - \sum_i p_i H(\Phi(\rho_i)) \,, \tag{2}$$

with $p \in \Delta_{n^2}$ and $\rho_i \in \mathcal{D}(\mathcal{H})$ for all $i \in \{1, \ldots, n^2\}$ denotes the *Holevo capacity*. Note that $C_{\mathcal{X}}(\Phi) \leq C(\Phi)$ is immediate and since Hastings' result [5] it is known that there exist channels for which the inequality is strict. Nevertheless, approximating the Holevo capacity is an important task as computing $C(\Phi)$ via the regularized expression seems intractable and as it is always a lower bound to $C(\Phi)$. To the best of our knowledge there is no algorithm known yet to compute (1) nor (2) with a provable rate of convergence.

Contribution — efficient approximation schemes with explicit error bounds

The main contribution of our work is to provide a framework that shows how recent advances in convex optimization can be used to approximately solve problems in quantum information theory. We demonstrate the performance of the framework on the problem of approximating the classical capacity of cq and qq channels.

Result 1 (Capacity approximation for cq channels [cf. Sec. 2 in full version])**.** We present an algorithm that generates an ε-close solution to the capacity of cq channels with a complexity $O\big(\frac{\max\{N,M\} M^3 \log(N)^{1/2}}{\varepsilon}\big)$.

Result 2 (Holevo capacity approximation for qq channels [cf. Sec. 3 & 4 in the full version])**.**

(i) We present an algorithm for approximating the Holevo capacity of qq channels that quantifies the approximation error. Furthermore a rate on the approximation error is derived.[1]

(ii) We show that the problem of approximating the Holevo capacity for qq channels can be reduced to a multidimensional integration problem.

(iii) We determine families of channels for which our approximation scheme has a complexity to find an ε-solution that is polynomial or subexponential in the problem size.

These two results present, for the first time, approximation algorithms to compute the classical capacity of cq and qq channels with a provable rate of convergence.

Methods and proof techniques

The main idea of the presented approximation scheme is summarized in Fig. 1. The key elements are the fact that the dual problem of the capacity formula (with strong duality) exhibits a specific structure that allows us to apply smoothing techniques motivated by [6] that map it into an entropy maximization problem which admits a closed form solution [7, 8] — even if the optimizer is infinite-dimensional [cf. Lem. 2.1 & Lem. 3.8 in the full version]. This feature enables us to treat cq channels with a bounded continuous input alphabet and a finite-dimensional output.

A second important ingredient to our approximation scheme is the idea of a universal encoder which is a mapping that translates a classical into a quantum state as explained in Fig. 2. As our method can treat cq channels with a continuous input alphabet, this makes it possible to approximate the Holevo capacity $C_{\mathcal{X}}(\Phi)$ by approximating the capacity of the induced cq channel $C_{\mathsf{cq}}(\Phi \circ \mathsf{E})$ where E denotes the universal encoding mapping.

Related work

Unlike for classical channels where there exists an efficient method — the *Blahut-Arimoto algorithm* [9, 10] — to numerically compute the capacity with a known rate of convergence, for cq channels an efficient approximation scheme with a provable rate of convergence does not exist up to date. In [11], Shor discusses a combinatorial approach to approximate the Holevo capacity of a qq channel, but he does not prove the

[1] See caption of Fig. 1 for an explanation of the two different error bounds provided.

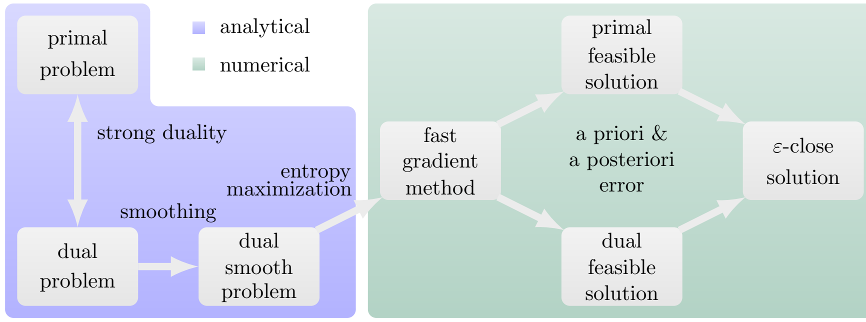

FIG. 1. **Illustration of the approach.** In a first step the capacity formula (called the primal problem) is dualized and strong duality is established. The favorable structure of the dual problem allows us to apply smoothing techniques which then leads to an entropy maximization problem that admits a closed form solution. Thanks to these analytical preliminaries, a fast gradient method can be applied that iteratively constructs feasible points to the primal and dual problem which gives an a posteriori error. In addition, we derive an explicit error bound (called a priori error) for this method.

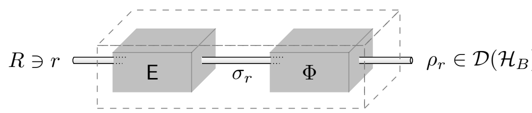

FIG. 2. **How to embed a qq into a cq channel.** Using a universal encoder $\mathsf{E} : R \ni r \mapsto |r\rangle\langle r| =: \sigma_r \in \mathcal{D}(\mathcal{H}_A)$ we embed the qq channel $\Phi : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)$ into a cq channel $\rho : R \ni r \mapsto (\Phi \circ \mathsf{E})(r) = \Phi(|r\rangle\langle r|) =: \rho_r \in \mathcal{D}(\mathcal{H}_B)$ with a continuous bounded input alphabet. We then have $C_{\mathsf{cq}}(\Phi \circ \mathsf{E}) = C_{\mathcal{X}}(\Phi)$.

convergence of his method. There are numerous different ad hoc attempts to approximate the Holevo capacity of qq channels, where however no convergence guarantees are given [12–15]. Our algorithm closes this gap. Simulations confirm that the theoretical work presented in this paper performs well in practice [cf. Sec. 2.A and Sec. 4.C in the full version].

The optimization problem expressing the Holevo capacity of a qq channel has been shown to be NP-complete [16] and also difficult to approximate [17]. However, this does not preclude the existence of classes of channels for which the Holevo capacity can be computed efficiently. Our approach via its smoothed dual version reduces it to a multidimensional integration — a problem that is well-studied and oftentimes can be solved efficiently [18]. For certain families of channels we prove that the complexity to derive an ε-close solution to the Holevo capacity is subexponential or even polynomial in the problem size [cf. Cor. 4.12 in the full version].

Discussion

Our framework has already been proven useful to approximate the capacity of classical channels whose value is unknown, e.g., the capacity of a discrete-time Poisson channel [19]. This suggests that the presented methods can be used to approximate other important quantities in quantum information theory that are described via optimization problems with a similar structure. Possible candidates are the *entanglement of formation*, which is an important measure of entanglement [20], the *quantum rate distortion function* describing the maximal compression rate up to a certain distortion [21], and the *channel coherent information*, which is the best generic lower bound to the quantum capacity that characterizes the highest possible rate at which quantum information can be transmitted reliably over a quantum channel [3].

The presented algorithm could also be a potential tool to find a low dimensional qq channel Φ with a Holevo capacicty that is not additive, i.e., that satisfies $C(\Phi) > C_{\mathcal{X}}(\Phi)$. So far this phenomenon could only be verfied for high dimensional channels [5] and it is of general interest to find out if low dimensional channels also exhibit such a behavior.

[1] Claude E. Shannon, "A mathematical theory of communication," Bell System Technical Journal **27**, 379–423 (1948).

[2] Alexander S. Holevo, "The capacity of the quantum channel with general signal states," IEEE Transactions on Information Theory **44**, 269–273 (1998).

[3] Alexander S. Holevo, *Quantum Systems, Channels, Information* (De Gruyter Studies in Mathematical Physics 16, 2012).

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

[5] Matthew B Hastings, "Superadditivity of communication capacity using entangled inputs," Nature Physics **5**, 255–257 (2009).

[6] Yurii Nesterov, "Smooth minimization of non-smooth functions," Mathematical Programming **103**, 127–152 (2005).

[7] Edwin T. Jaynes, "Information theory and statistical mechanics. ii," Physical Review **108**, 171–190 (1957).

[8] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory* (Wiley Interscience, 2006).

[9] Richard E. Blahut, "Computation of channel capacity and rate-distortion functions," IEEE Transactions on Information Theory **18**, 460–473 (1972).

[10] Suguru Arimoto, "An algorithm for computing the capacity of arbitrary discrete memoryless channels," IEEE Transactions on Information Theory **18**, 14–20 (1972).

[11] Peter W. Shor, "Capacities of quantum channels and how to find them," Mathematical Programming **97**, 311–335 (2003).

[12] Hiroshi Nagaoka, "Algorithms of arimoto-blahut type for computing quantum channel capacity," Proceedings IEEE International Symposium on Information Theory (ISIT) , 354– (1998).

[13] Hiroshi Nagaoka and Susumu Osawa, "Algorithms of arimoto-blahut type for computing quantum channel capacity," Proceedings of the second QIT , 107112 (1999).

[14] Susumu Osawa and Hiroshi Nagaoka, "Numerical experiments on the capacity of quantum channel with entangled input states," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E84**, 2583–2590 (2001), available at arXiv:ph/0007115v4.

[15] Masahito Hayashi, Hiroshi Imai, Keiji Matsumoto, Mary Beth Ruskai, and Toshiyuki Shimono, "Qubit channels which require four inputs to achieve capacity: Implications for additivity conjectures," Quantum Information and Computation **5**, 13–31 (2005).

[16] Salman Beigi and Peter Shor, "On the complexity of computing zero-error and holevo capacity of quantum channels," (2008), available at arXiv:0709.2090.

[17] Aram W. Harrow and Ashley Montanaro, "Testing product states, quantum merlin-arthur games and tensor optimization," J. ACM **60**, 3:1–3:43 (2013).

[18] C. Robert and G. Casella, *Monte Carlo Statistical Methods*, Springer Texts in Statistics (Springer, 2004).

[19] Tobias Sutter, Peyman Mohajerin Esfahani, David Sutter, and John Lygeros, "Capacity approximation of memoryless channels with countable output alphabets," Proceedings IEEE International Symposium on Information Theory (ISIT) , 2909–2913 (2014).

[20] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, "Mixed-state entanglement and quantum error correction," Physical Review A **54**, 3824–3851 (1996).

[21] Howard Barnum, "Quantum rate-distortion coding," Phys. Rev. A **62**, 042309 (2000).