Efficient Approximation of Quantum Channel Capacities

David Sutter, Tobias Sutter, Peyman Mohajerin Esfahani, and Renato Renner

Abstract

We propose an iterative method for approximating the capacity of classical-quantum channels with a discrete input alphabet and a finite-dimensional output under additional constraints on the input distribution. Based on duality of convex programming, we derive explicit upper and lower bounds for the capacity. To provide an additive ε-close estimate to the capacity, the presented algorithm requires $O((N \vee M)M^3 \log(N)^{1/2}\varepsilon^{-1})$ steps, where N denotes the input alphabet size and M the output dimension. We then generalize the method to the task of approximating the capacity of classical-quantum channels with a bounded continuous input alphabet and a finite-dimensional output. This, using the idea of a universal encoder, allows us to approximate the Holevo capacity for channels with a finite-dimensional quantum mechanical input and output. In particular, we show that the problem of approximating the Holevo capacity can be reduced to a multi-dimensional integration problem. For certain families of quantum channels we prove that the complexity to derive an additive 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.

Index Terms

Quantum capacity, Holevo capacity, convex optimization, duality, smoothing techniques, entropy maximization, universal encoder

1. Introduction

Consider the scenario where a sender wants to transmit information over a noisy channel to a receiver. Information theory says that there exist fundamental quantities called *channel capacities* characterizing the maximal amount of information that can be transmitted on average, asymptotically reliably, per channel use [1]. Depending on the channel and allowed auxiliary resources, there is a variety of capacities for different communication tasks. An excellent overview can be found in [2], [3]. For a lot of these tasks, their corresponding capacity can be recast

D. Sutter and R. Renner are with the Institute for Theoretical Physics, ETH Zurich, Zurich 8092, Switzerland (e-mail: {suttedav, renner}@phys.ethz.ch).

T. Sutter and P. Mohajerin Esfahani are with the Department of Information Technology and Electrical Engineering, ETH Zurich, Zurich 8092, Switzerland (e-mail: {sutter, mohajerin}@control.ee.ethz.ch).

DS and RR acknowledge support by the Swiss National Science Foundation (through the National Centre of Competence in Research 'Quantum Science and Technology' and grant No. 200020-135048) and by the European Research Council (grant No. 258932). TS and PME were supported by the ETH grant (ETH-15 12-2) and the HYCON2 Network of Excellence.

as an optimization problem. Some of them seem to be intrinsically more difficult than others and in general no closed form solution is available. Moreover, to the best of our knowledge, no efficient algorithm to compute these formulas is known.

In this article, we focus on two cases. First, we consider the task of sending classical information over a classical-quantum (cq) channel which maps each element of a classical input alphabet to a finite-dimensional quantum state. We do not allow any additional resources such as entanglement shared between the sender and receiver nor feedback. The capacity for this task has been shown in [4], [3], [5] to be the maximization of a quantity called the *Holevo information* over all possible input distributions. Unlike the classical channels where a specific efficient method — the *Blahut-Arimoto algorithm* [6], [7] — is known for numerical computation of the capacity with a provable rate of convergence, there is no counterpart for cq channels to date. On a superficial level, there are proposals [8], [9], [10] of algorithmic ideas that might be useful (such as interior point or ellipsoid methods), however to the best of our knowledge they have not been analyzed rigorously and as a result it is unclear if they lead to a provable rate of convergence or not.

The second case considered in this article is to send classical information over a quantum-quantum (qq) channel with a finite-dimensional quantum mechanical input and output. Similarly we do not allow additional resources such as entanglement shared between the sender and receiver nor feedback. In comparison with the setup of a cq channel, this task is more delicate as one could make use of entangled input states at the encoding. Indeed, it has been shown that the classical capacity of a qq channel is still poorly understood [11], as only a *regularized* expression is known that describes it [4], [3], [5], which in general is computationally intractable. The best known generic lower bound for the classical capacity of a qq channel with a single letter expression is the *Holevo capacity*, which is mathematically described by a finite-dimensional non-convex optimization problem. It has been shown that the respective optimization problem is NP-hard and also difficult to approximate [12], [13]. In [14], Shor suggests an approach to approximate the Holevo capacity that is heavily based on linear programming methods, though the convergence of the proposed approach is not discussed. There are numerous different ad hoc attempts to approximate the Holevo capacity, where however no convergence guarantees are given [9], [10], [15], [16].

In this work, we show how recent techniques from convex optimization can be utilized to approximate the classical capacity of cq and qq channels. For cq channels, we propose an algorithm that, to the best of our knowledge, is the first practical method to efficiently find an additive ε-close solution. For the second task described above, the idea of a universal encoder allows us to apply similar methods to compute close upper and lower bounds for the Holevo capacity that coincide asymptotically. This leads to the first algorithm, as far as we know, for approximating the Holevo capacity with a provable rate of convergence. Further, we show that for certain classes of channels the Holevo capacity can be approximated up to an arbitrary precision in subexponential or even polynomial time. Thus whenever the capacity of a cq or a qq channel has to be evaluated (e.g., in a physical experiment involving quantum communciation) the methods presented in this article could find practical use.

Summary of results.— Our main results are efficient approximation algorithms for the capacity of cq and qq

channels with a provable rate of convergence. Deriving an additive ε-close solution[1] to the capacity of a cq channel requires $O\big((N\vee M)M^3\log(N)^{1/2}\,\varepsilon^{-1}\big)$, where N is the input alphabet size, M the output dimension of the channel and $N\vee M$ denotes the maximum between N and M (see Theorem 3.15). We show that the task of approximating the Holevo capacity of a qq channel can be reduced to a multi-dimensional integration problem and characterize families of channels for which an additive ε-close solution can be found in subexponential or even polynomial time. The precise complexity required to compute an additive ε-close solution is given in Theorem 5.4. The overall idea of the presented approximation schemes is summarized in Figure 1.

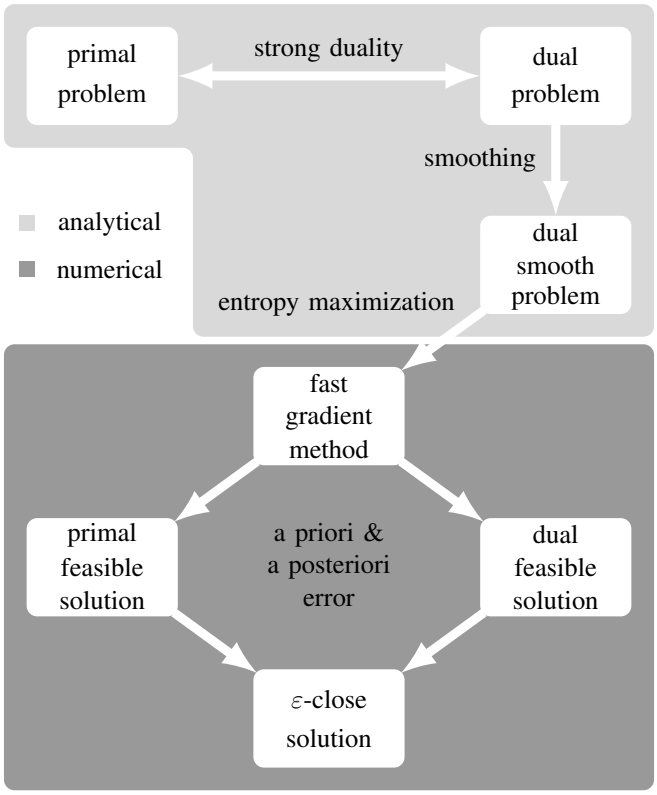

Fig. 1. **Illustration of the approach.** In a first step the capacity formula (called the primal problem, given in (11) and (28)) is dualized and strong duality is established. The favorable structure of the dual problem (given in (12) and (29)) allows us to apply smoothing techniques which then leads 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, yielding an a posteriori error. In addition, we derive an a priori error bound for this method.

Notation.— The logarithm with basis 2 is denoted by $\log(\cdot)$ and the natural logarithm by $\ln(\cdot)$. The space of all Hermitian operators in a finite-dimensional Hilbert space $\mathcal{H}$ is denoted by H^M, where M is the dimension of $\mathcal{H}$. The cone of positive semidefinite Hermitian operators is H^M_+. For $\sigma\in\mathrm{H}^M$ we denote its set of eigenvalues by $\mathrm{spec}(\sigma)=\{\lambda_1(\sigma),\ldots,\lambda_M(\sigma)\}$. We denote the set of density operators on a Hilbert space $\mathcal{H}$ by $\mathcal{D}(\mathcal{H}):=$

[1]Within this article an (additive) ε-close solution denotes an approximate solution with an *additive* error of at most ε.

$\{\rho \in \mathrm{H}_+^M \ : \ \mathrm{tr}\,[\rho] = 1\}$. We consider cq channels $\rho : \mathcal{X} \to \mathcal{D}(\mathcal{H})$, $x \mapsto \rho_x$ having a finite input alphabet $\mathcal{X} = \{1, 2, \ldots, N\}$ and a finite output dimension $\dim \mathcal{H} = M$. Each symbol $x \in \mathcal{X}$ at the input is mapped to a density operator ρ_x at the output and therefore the channel can be represented by a set of density operators $\{\rho_x\}_{x\in\mathcal{X}}$. The input probability mass function is denoted by the vector $p \in \mathbb{R}^N$ where $p_i = \mathbb{P}[X = i]$. A possible input cost constraint can be written as $\mathbb{E}[s(X)] = p^\top s \leq S$, where $s \in \mathbb{R}^N$ denotes the cost vector and $S \in \mathbb{R}_{\geq 0}$ is the given total cost. We define the standard $n-$simplex as $\Delta_n := \{x \in \mathbb{R}^n : x \geq 0, \sum_{i=1}^n x_i = 1\}$. For a probability mass function $p \in \Delta_N$ we denote the entropy by $H(p) := -\sum_{i=1}^N p_i \log p_i$. The binary entropy function is defined as $H_\mathrm{b}(x) := -x\log(x) - (1-x)\log(1-x)$ with $x \in [0, 1]$. For a probability density p supported at a measurable set $B \subset \mathbb{R}$ we denote the differential entropy by $h(p) := -\int_B p(x) \log p(x)\,\mathrm{d}x$. The von Neumann entropy is defined by $H(\rho_x) := -\mathrm{tr}\,[\rho_x \log \rho_x]$ where $\rho_x \in \mathcal{D}(\mathcal{H})$ is a density operator. Let $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$, where $\mathcal{B}(\mathcal{H})$ denotes the space of bounded linear operators in some Hilbert space $\mathcal{H}$ that are equipped with the trace norm, be a quantum channel that is described by a complete positive trace preserving (cptp) map. We denote the canonical inner product by $\langle x, y\rangle := x^\top y$ where $x, y \in \mathbb{R}^n$. For two matrices $A, B \in \mathbb{C}^{m\times n}$, we denote the Frobenius inner product by $\langle A, B\rangle_F := \mathrm{tr}\left[A^\dagger B\right]$ and the induced Frobenius norm by $\|A\|_F := \sqrt{\langle A, A\rangle_F}$. The trace norm is defined as $\|A\|_\mathrm{tr} := \mathrm{tr}[\sqrt{A^\dagger A}]$. The operator norm is denoted by $\|A\|_\mathrm{op} := \{\sup_X \|AX\|_F \ : \ \|X\|_F = 1\}$. For a cptp map $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ its diamond norm is defined by $\|\Phi\|_\diamond := \|\Phi \otimes \mathrm{id}_{\mathcal{H}_A}\|_\mathrm{tr}$, where $\|\cdot\|_\mathrm{tr}$ denotes the trace norm for resources which is defined as $\|\Theta\|_\mathrm{tr} := \max_{\rho\in\mathcal{D}(\mathcal{H}_A)} \|\Theta(\rho)\|_\mathrm{tr}$. We denote the maximum and minimum between a and b by $a \vee b$ respectively $a \wedge b$. The symbol $\preccurlyeq$ denotes the semidefinite order on self-adjoint matrices. The identity matrix of appropriate dimension is denoted by $\mathbf{1}$.

Structure.— The remainder of this article is structured as follows. Section 3 shows how to efficiently compute tight upper and lower bounds for the capacity of cq channels having a discrete input alphabet. In Section 4 we then show how to extend the methods introduced in Section 3 to approximate the capacity of cq channels with a continuous input alphabet. Using the concept of a universal encoder, this allows us to approximate the Holevo capacity of finite-dimensional quantum channels as shown in Section 5. We conclude in Section 6 with a summary and possible subjects of further research. In the interest of readability, some of the technical proofs and details are given in the appendices.

2. Preliminaries

In this section we recall two standard preliminary results that are used in the derivation of the approximation scheme. One of them is Nesterov's seminal work on how to efficiently solve convex optimization problems with a specific structure by applying smoothing techniques [17]. The second preliminary result we recall is a famous concentration of measure inequality that is known as *McDiarmid's inequality* or also as *bounded differences inequality*. It states that a function of independent random variables that satisfies a regularity property (the bounded differences property) exhibits exponential concentration.

A. Nesterov's smoothing technique [17]

Consider finite-dimensional normed vector spaces V_1 and V_2. The dual spaces are denoted by V_1^* and V_2^* and $\langle \cdot, \cdot \rangle_i : V_i^* \times V_i \to \mathbb{R}$ for $i \in \{1, 2\}$ denotes a bilinear form on the vector spaces. We are interested in the optimization problem

$$\min_{x \in Q_1} f(x) \ , \tag{1}$$

where $Q_1 \subseteq V_1$ is a compact convex set and f is a continuous convex function. We consider objective functions f with a particular structure, i.e.,

$$f(x) = \hat{f}(x) + \max_{y \in Q_2} \{ \langle Ax, y \rangle_2 - \hat{\phi}(y) \} \ , \tag{2}$$

for a linear operator $A : V_1 \to V_2^*$ and $Q_2 \subset V_2$ a compact convex set. The function $\hat{f}$ is continuously differentiable, convex and has a Lipschitz continuous gradient with constant L. The function $\hat{\phi}$ is convex and continous. Since the objective function in (1) is non-smooth in general the complexity to compute an additive ε-close solution using subgradient type methods is $O(1/\varepsilon^2)$. Nesterov's work shows that for objective functions with the particular structure (2), one can compute an additive ε-close solution within $O(1/\varepsilon)$ steps. The main idea is to consider a smoothed version of (1) given by

$$\min_{x \in Q_1} f_\nu(x) \ , \tag{3}$$

where

$$f_\nu(x) = \hat{f}(x) + \max_{y \in Q_2} \{ \langle Ax, y \rangle_2 - \hat{\phi}(y) - \nu d(y) \} \ . \tag{4}$$

$d : Q_2 \to \mathbb{R}$ is a regularization term that is assumed to be strongly convex. It can be shown that f_ν has a Lipschitz continuous gradient and therefore can be solved efficiently by a fast gradient method. Nesterov's work [17] shows that by solving the smoothed optimization problem (3) (which can be done more efficiently) we can construct good upper and lower bounds to the original problem (1). Furthermore, it is proven how fast these bounds converge to the optimal solution of (1).

B. McDiarmid's inequality

A function $f : \mathcal{X}^n \to \mathbb{R}$ for some set $\mathcal{X}$ has the *bounded differences property* if there exist non-negative constants $c_1, \ldots, c_n$ such that

$$\sup_{x_1, \ldots, x_n, x_i' \in \mathcal{X}} |f(x_1, \ldots, x_n) - f(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_n)| \leq c_i \ , \quad 1 \leq i \leq n \ . \tag{5}$$

McDiarmid's inequality (also known as bounded differences inequality) shows that such functions satisfy a sub-Gaussian tail inequality. Let f satisfy the bounded difference assumption with constants $c_1, \ldots, c_n$, let $\kappa := \frac{1}{4} \sum_{i=1}^n c_i^2$ and let $X_1, \ldots, X_n$ be independent random variables then we have

$$\mathbb{P}[f(X_1, \ldots, X_n) - \mathbb{E}[f(X_1, \ldots, X_n)] > t] \leq \exp\Big(\frac{-t^2}{2\kappa} \Big) \ . \tag{6}$$

We note that there also exists a version of (6) that applies for matrices [18, Cor. 7.5]. McDiarmid's inequality is one of many different concentration of measure inequalities, see [19] for a comprehensive overview.

3. Capacity of a Discrete-Input Classical-Quantum Channel

In this section we show that concepts introduced in [20] for a purely classical setup can be generalized to compute the capacity of cq channels with a discrete input alphabet and a bounded output. We consider a discrete input alphabet $\mathcal{X} = \{1, \dots, N\}$ and a finite-dimensional Hilbert space $\mathcal{H}$ with $\dim \mathcal{H} =: M$. The map $\rho : \mathcal{X} \to \mathcal{D}(\mathcal{H})$, $x \mapsto \rho_x$, represents a cq channel. Let $s : \mathcal{X} \to \mathbb{R}_+$ be some cost function, $p \in \Delta_N$ and consider the input constraint

$$\langle p, s \rangle \leq S, \tag{7}$$

where S is some non-negative constant. As shown by Holevo, Schumacher and Westmoreland [4], [3], [5], the capacity of a cq channel ρ satisfying the input constraint (7) is given by

$$C_{\mathsf{cq},S}(\rho) = \left\{ \begin{array}{ll} \max\limits_{p} & I(p,\rho) := H\Big(\sum_{i=1}^N p_i \rho_i\Big) - \sum_{i=1}^N p_i H(\rho_i) \\ \text{s.t.} & \langle p, s \rangle \leq S \\ & p \in \Delta_N. \end{array} \right. \tag{8}$$

To keep the notation simple we consider a single input constraint as the extension to multiple input constraints is straightforward.

In the following, we reformulate (8) such that it exhibits a well structured dual formulation and show that strong duality holds. We then show how to smooth the objective function of the dual problem such that it can be solved efficiently using a fast gradient method. Doing so leads to an algorithm that iteratively computes lower and upper bounds to the capacity which converge with a given rate. A key concept in our analysis is that the following problem — called *entropy maximization* — with $\lambda \in \mathrm{H}^M$ features an analytical solution

$$\left\{ \begin{array}{ll} \max\limits_{\rho} & H(\rho) + \operatorname{tr}[\rho\lambda] \\ \text{s.t.} & \rho \in \mathcal{D}(\mathcal{H}). \end{array} \right. \tag{9}$$

Lemma 3.1 (Entropy maximization [21])**.** *Let $\rho^\star = 2^{-\mu \mathbf{1} + \lambda}$, where μ is chosen such that $\rho^\star \in \mathcal{D}(\mathcal{H})$. Then $\rho^\star$ uniquely solves (9).*

We next derive the dual problem of (8) and show how to solve it efficiently. We therefore reformulate (8) by introducing an additional decision variable $\sigma := \sum_{i=1}^N p_i \rho_i$.

Lemma 3.2. *Let $\mathcal{F} := \arg\max\limits_{p \in \Delta_N} I(p,\rho)$ and $S_{\max} := \min\limits_{p \in \mathcal{F}} \langle p, s \rangle$. If $S \geq S_{\max}$, the optimization problem (8) has the same optimal value as*

$$\text{(primal problem)} \;:\; \left\{ \begin{array}{ll} \max\limits_{p,\sigma} & H(\sigma) - \sum_{i=1}^N p_i H(\rho_i) \\ \text{s.t.} & \sigma = \sum_{i=1}^N p_i \rho_i \\ & p \in \Delta_N,\, \sigma \in \mathcal{D}(\mathcal{H}). \end{array} \right. \tag{10}$$

If $S < S_{\max}$, the optimization problem (8) has the same optimal value as

$$\text{(primal problem)} \;:\; \left\{ \begin{array}{ll} \max\limits_{p,\sigma} & H(\sigma) - \sum_{i=1}^N p_i H(\rho_i) \\ \text{s.t.} & \sigma = \sum_{i=1}^N p_i \rho_i \\ & \langle p, s \rangle = S \\ & p \in \Delta_N, \sigma \in \mathcal{D}(\mathcal{H}). \end{array} \right. \tag{11}$$

Proof: See Appendix A. ∎

Note that the constraint $\sigma \in \mathcal{D}(\mathcal{H})$ in (10) and (11) is redundant since $\rho_i \in \mathcal{D}(\mathcal{H})$ and $p \in \Delta_N$ imply that $\sigma \in \mathcal{D}(\mathcal{H})$. The Lagrange dual program to (11) is given by

$$(\text{dual problem}) \;:\; \begin{cases} \min\limits_{\lambda} & G(\lambda) + F(\lambda) \\ \text{s.t.} & \lambda \in \mathrm{H}^M, \end{cases} \tag{12}$$

with $F, G : \mathrm{H}^M \to \mathbb{R}$ of the form

$$G(\lambda) = \begin{cases} \max\limits_{p} & \sum_{i=1}^N p_i \left(-H(\rho_i) + \operatorname{tr}\left[\rho_i \lambda\right]\right) \\ \text{s.t.} & \langle p, s \rangle = S \\ & p \in \Delta_N \end{cases} \quad \text{and} \quad F(\lambda) = \begin{cases} \max\limits_{\sigma} & H(\sigma) - \operatorname{tr}\left[\sigma\lambda\right] \\ \text{s.t.} & \sigma \in \mathcal{D}(\mathcal{H}). \end{cases} \tag{13}$$

Note that since the coupling constraint $\sigma = \sum_{i=1}^N p_i \rho_i$ in the primal program (11) is affine, the set of optimal solutions to the dual program (12) is nonempty [22, Prop. 5.3.1] and as such the optimum is attained. The function $G(\lambda)$ is a (parametric) linear program and $F(\lambda)$ is of the form given in Lemma 3.1, i.e., $F(\lambda)$ has a unique optimizer $\sigma^\star = 2^{-\mu\mathbf{1}-\lambda}$, where μ is chosen such that $\sigma^\star \in \mathcal{D}(\mathcal{H})$, which gives

$$\mu = \log\left(\operatorname{tr}\left[2^{-\lambda}\right]\right). \tag{14}$$

We thus obtain

$$\begin{aligned} F(\lambda) &= H(\sigma^\star) - \operatorname{tr}\left[\sigma^\star\lambda\right] \\ &= -\operatorname{tr}\left[2^{-\mu\mathbf{1}-\lambda}\log\left(2^{-\mu\mathbf{1}-\lambda}\right)\right] - \operatorname{tr}\left[2^{-\mu\mathbf{1}-\lambda}\lambda\right] \\ &= 2^{-\mu}\mu \operatorname{tr}\left[2^{-\lambda}\right] \\ &= \log\left(\operatorname{tr}\left[2^{-\lambda}\right]\right), \end{aligned} \tag{15}$$

where the last step uses (14). The gradient of $F(\lambda)$ is given by [23, p. 639 ff.]

$$\nabla F(\lambda) = -\frac{2^{-\lambda}}{\operatorname{tr}\left[2^{-\lambda}\right]}. \tag{16}$$

Remark 3.3. Note that the dual formulation for the capacity given in (12) can be shown to be equivalent to the formula for the divergence radius of the channel image as discussed in [24], [25], [26].

The following proposition shows that the gradient (16) is Lipschitz continuous, which is essential for the optimization algorithm that we will use to solve (12).

Proposition 3.4 (Lipschitz constant of ∇F)**.** *The gradient $\nabla F(\lambda)$ as given in (16) is Lipschitz continuous with respect to the Frobenius norm with Lipschitz constant* 2*.*

Proof: To prove the Lipschitz continuity of $\nabla F(\lambda)$, we focus on the representation of $F(\lambda)$ as an optimization problem, given in (13). According to [17, Thm. 1], the function $\nabla F(\lambda)$ is Lipschitz continuous with Lipschitz constant $L = \frac{1}{\kappa}$, where κ is the strong convexity parameter of the convex function $\mathcal{D}(\mathcal{H}) \ni \sigma \mapsto -H(\sigma) \in \mathbb{R}$, where according to [27, Thm. 16] $\kappa = \frac{1}{2}$. ∎

Another requirement to solve (12) with a specific rate of convergence using a fast gradient method is that the set of feasible optimizers is compact. In order to assure that and to precisely characterize the size of the set of all feasible optimizers (with respect to the Frobenius norm), we need to impose the following assumption on the cq channel ρ, that we will maintain for the remainder of this article.

Assumption 3.5 (Regularity)**.** $\gamma := \min\limits_{x\in\mathcal{X}} \min \operatorname{spec}(\rho_x) > 0$.

Even though Assumption 3.5 may seem restrictive at first glance, it holds for a large class of cq channels. Moreover, according to the Fannes-Audenaert inequality [28], [29] the von Neumann entropy is uniformly continuous in its argument with respect to the trace norm. Furthermore as shown in [30] even the conditional entropy is uniformly continuous with respect to the trace norm. Therefore, cq channels having density operators ρ_x that violate Assumption 3.5 can be avoided by slight perturbations of these density operators (see Example 3.17 for a numerical illustration) and by using the explicit continuity statements for the conditional entropy [30], we get an explicit error term as a function of the perturbation parameter. Furthermore, it can be seen that the mutual information is strictly concave as a function of the input distribution, for a fixed channel under Assumption 3.5. This implies the uniqueness of the optimal input distribution.

Lemma 3.6. *Under Assumption 3.5, the dual program* (12) *is equivalent to*

$$\min_{\lambda} \left\{ G(\lambda) + F(\lambda) \ : \ \lambda \in \Lambda \right\},$$

where $\Lambda := \left\{ \lambda \in \mathrm{H}^M \ : \ \|\lambda\|_F \leq M \log\left(\gamma^{-1} \vee \mathrm{e}\right) \right\}$.

Proof: See Appendix B. ∎

Lemma 3.7. *Strong duality holds between* (11) *and* (12)*.*

Proof: The assertion follows by a standard strong duality result of convex optimization, see [22, Prop. 5.3.1, p. 169]. ∎

The goal is to efficiently solve (12), which is not straightforward since $G(\cdot)$ is non-smooth and as therefore in general the subgradient method is optimal to solve such problems [31]. The idea is to use the particular structure of (12) that allows us to invoke Nesterov's smoothing technique [17]. Therefore, we consider

$$G_\nu(\lambda) := \begin{cases} \max\limits_{p} & \left\langle p, b(\lambda) \right\rangle - \left\langle p, a \right\rangle + \nu H(p) - \nu \log N \\ \text{s.t.} & \left\langle p, s \right\rangle = S \\ & p \in \Delta_N, \end{cases} \tag{17}$$

with smoothing parameter $\nu \in \mathbb{R}_{>0}$ and $a, b(\lambda) \in \mathbb{R}^N$ defined as $a_i := H(\rho_i)$ and $b_i(\lambda) := \operatorname{tr}[\rho_i \lambda]$. We denote by $p_\nu(\lambda)$ the optimal solution that is unique since the objective function is strictly concave. Clearly for any $p \in \Delta_N$, $G_\nu(\lambda) \leq G(\lambda) \leq G_\nu(\lambda) + \nu \log(N)$, i.e., $G_\nu(\lambda)$ is a uniform approximation of the non-smooth function $G(\lambda)$. According to Lemma 2.2 in [20] an analytical optimizer $p_\nu(\lambda)$ is given by

$$p_\nu(\lambda)_i = 2^{\mu_1 + \frac{1}{\nu}(b_i(\lambda) - a_i) + \mu_2 s_i}, \quad 1 \leq i \leq N, \tag{18}$$

where $\mu_1, \mu_2 \in \mathbb{R}$ have to be chosen such that $\langle p_\nu(\lambda), s \rangle = S$ and $p_\nu(\lambda) \in \Delta_N$.

Remark 3.8. In case of no input constraints, the unique optimizer to (17) is given by

$$p_\nu(\lambda)_i = \frac{2^{\frac{1}{\nu}(b_i(\lambda)-a_i)}}{\sum_{j=1}^N 2^{\frac{1}{\nu}(b_j(\lambda)-a_j)}}, \quad 1 \leq i \leq N,$$

whose straightforward evaluation is numerically difficult for small ν. A numerically stable method for this computation is presented in [20, Rmk. 2.6].

Remark 3.9 ([20])**.** In case of an additional input constraint, we need an efficient method to find the coefficients μ_1 and μ_2 in (18). In particular if there are multiple input constraints (which will lead to multiple μ_i) the efficiency of the method computing them becomes important. Instead of solving a system of non-linear equations, it turns out that the μ_i can be found by solving the following convex optimization problem [32, p. 257 ff.]

$$\sup_{\mu \in \mathbb{R}^2} \left\{ \langle y, \mu \rangle - \sum_{i=1}^N p_\nu(\lambda, \mu) \right\}, \tag{19}$$

where $y := (1, S)$. Note that (19) is an unconstrained maximization of a concave function, whose gradient and Hessian can be easily computed, which would allow us to use second-order methods.

Finally, we can show that the uniform approximation $G_\nu(\lambda)$ is smooth and has a Lipschitz continuous gradient with known Lipschitz constant.

Proposition 3.10 (Lipschitz constant of ∇G_ν)**.** *$G_\nu(\lambda)$ is well defined and continuously differentiable at any $\lambda \in \Lambda$. Moreover, it is convex and its gradient $\nabla G_\nu(\lambda) = \sum_{i=1}^N \rho_i \, p_\nu(\lambda)_i$ is Lipschitz continuous with respect to the Frobenius norm with constant $\frac{1}{\nu}$.*

Proof: See Appendix C. ∎

We consider the smooth, convex optimization problem

$$\text{(smoothed dual problem)} \; : \; \begin{cases} \min\limits_{\lambda} & F(\lambda) + G_\nu(\lambda) \\ \text{s.t.} & \lambda \in \Lambda, \end{cases} \tag{20}$$

whose objective function has a Lipschitz continuous gradient with respect to the Frobenius norm with Lipschitz constant $L_\nu := 2 + \frac{1}{\nu}$. According to [27, Thm. 16] the function $\mathrm{H}^M \ni A \mapsto d(A) := \frac{1}{2} \|A\|_F^2 \in \mathbb{R}_{\geq 0}$ is $\frac{1}{2}$-strongly convex with respect to the Frobenius norm. As such (20) can be be approximated with Nesterov's optimal scheme for smooth optimization [17], which is summarized in Algorithm 1, where π_Λ denotes the projection operator onto the set Λ, defined in Lemma 3.6, that is the Frobenius norm ball with radius $r := M \log\left(\gamma^{-1} \vee \mathrm{e}\right)$.

Proposition 3.11 (Projection on Frobenius norm ball)**.** *Consider the Frobenius norm ball $\Lambda := \{A \in \mathrm{H}^M : \|\varsigma(A)\|_2 \leq r\}$ of radius $r \geq 0$, where $\varsigma(A) \in \mathbb{R}^M$ denotes the vector of singular values of A. The unique projection of a matrix $B \in \mathrm{H}^M$ onto Λ in the Frobenius norm is given by*

$$\pi_\Lambda(B) = U \mathsf{diag}\left(\pi_\Lambda(\varsigma(B))\right) V^\top,$$

where $B = U\mathsf{diag}\left(\varsigma(B)\right)V^\top$ *is the singular value decomposition of* B *and* π_Λ *is the projection operator of the* ℓ_2*-norm ball of radius* r*, i.e.,*

$$\pi_\Lambda(x) := \begin{cases} r\frac{x}{\|x\|_2}, & \|x\|_2 > r \\ x, & \textit{otherwise.} \end{cases}$$

Proof: The proof follows the lines in [33, Prop. 5.3]. ■

Algorithm 1: Optimal scheme for smooth optimization for cq channels

Choose some $\lambda_0 \in \mathrm{H}^M$

For $m \geq 0$ **do***

Step 1: Compute $\nabla F(\lambda_m) + \nabla G_\nu(\lambda_m)$

Step 2: $y_m = \pi_\Lambda\left(-\frac{1}{L_\nu}\left(\nabla F(\lambda_m) + \nabla G_\nu(\lambda_m)\right) + \lambda_m\right)$

Step 3: $z_m = \pi_\Lambda\left(-\frac{1}{2L_\nu}\sum_{i=0}^m \frac{i+1}{2}\left(\nabla F(\lambda_i) + \nabla G_\nu(\lambda_i)\right)\right)$

Step 4: $\lambda_{m+1} = \frac{2}{m+3}z_m + \frac{m+1}{m+3}y_m$

[*The stopping criterion is explained in Remark 3.13]

The following lemma ensures that by solving the dual smooth problem (20) using Algorithm 1, we can generate approximate solutions to the non-smooth problems (11) and (12).

Lemma 3.12 ([17])**.** *Let* $D = \frac{1}{2}\left(M\log(\gamma^{-1}\vee \mathrm{e})\right)^2$*,* $p_\nu(\cdot)$ *be given by* (18)*, and consider a smoothing parameter* $\nu = \frac{2}{k+1}\left(\frac{2D}{\log N}\right)^{\frac{1}{2}}$*. Then, after* k *iterations of Algorithm 1 we can generate the approximate solutions to the problems* (12) *and* (11)*, namely,* $\hat{\lambda} = y_k \in \Lambda$ *and* $\hat{p} = \sum_{i=0}^k \frac{2(i+1)}{(k+1)(k+2)}p_\nu(\lambda_i) \in \Delta_N$ *which satisfy*

$$0 \leq F(\hat{\lambda}) + G(\hat{\lambda}) - I(\hat{p},\rho) \leq \frac{4}{k+1}\sqrt{2D\log N} + \frac{16D}{(k+1)^2}. \tag{21}$$

Note that Lemma 3.12 provides an explicit error bound given in (21), also called *a priori error*. In addition this theorem predicts an approximation to the optimal input distribution (denoted by $\hat{p}$), i.e., the optimizer of the primal problem. Thus, by comparing the values of the primal and the dual optimization problem, one can also compute an *a posteriori error* which is the difference of the dual and the primal problem, namely $F(\hat{\lambda}) + G(\hat{\lambda}) - I(\hat{p},\rho)$ with $C_{\mathsf{cq},\mathrm{UB}}(\rho) := F(\hat{\lambda}) + G(\hat{\lambda})$ and $C_{\mathsf{cq},\mathrm{LB}}(\rho) := I(\hat{p},\rho)$. In practice the a posteriori error is often much smaller than the a priori error (see Section 3-A).

Remark 3.13 (Stopping criterion of Algorithm 1)**.** There are two immediate approaches to define a stopping criterion for Algorithm 1.

(i) *A priori stopping criterion*: Choose an a priori error $\varepsilon > 0$. Setting the right hand side of (21) equal to ε defines a number of iterations k_ε that has to be run in order to ensure an ε-close solution.

(ii) *A posteriori stopping criterion*: Choose an a posteriori error $\varepsilon > 0$. Choose the smoothing parameter $\nu(k_\varepsilon)$ for k_ε as defined above in the a priori stopping criterion. Fix a (small) number of iterations ℓ that are run using Algorithm 1. Compute the a posteriori error $\mathrm{e}_\ell := F(\hat{\lambda}) + G(\hat{\lambda}) - I(\hat{p},\rho)$ as given by Lemma 3.12. If $\mathrm{e}_\ell \leq \varepsilon$ terminate the algorithm otherwise continue with another ℓ iterations. Continue until the a posteriori error is below ε.

Remark 3.14 (No input cost constraint & numerical stability)**.** In the absence of an input cost constraint (i.e., $s(\cdot) = 0$), we can derive a closed form expression for $G_\nu(\lambda)$ and its gradient. Using (18) we obtain

$$G_\nu(\lambda) = \nu \log\left(\sum_{i=1}^{N} 2^{\frac{1}{\nu}(b(\lambda)-a)_i}\right) - \nu \log N$$
$$\frac{\partial G_\nu(\lambda)}{\partial \lambda_{m,\ell}} = (\nabla G_\nu(\lambda))_{m,\ell} = \frac{1}{S(\lambda)} \sum_{i=1}^{N} 2^{\frac{1}{\nu}(b(\lambda)-a)_i} (\rho_i)_{\ell,m}, \tag{22}$$

where $S(\lambda) = \sum_{i=1}^{N} 2^{\frac{1}{\nu}(b(\lambda)-a)_i}$ and we have used $\frac{\partial \mathrm{tr}[\rho\lambda]}{\partial \lambda_{m,\ell}} = \rho_{\ell,m}$ [23, Prop. 10.7.2]. Recall that as introduced above we consider $a, b(\lambda) \in \mathbb{R}^N$, such that $a_i = H(\rho_i)$ and $b_i(\lambda) = \mathrm{tr}\,[\rho_i \lambda]$. In order to achieve an ε-precise solution the smoothing factor ν has to be chosen in the order of ε, according to Lemma 3.12. A straightforward computation of $\nabla G_\nu(\lambda)$ via (22) for a small enough ν is numerically difficult. In the light of [17, p. 148], we present a numerically stable technique for computing $\nabla G_\nu(\lambda)$. By considering the functions $\mathbb{R}^M \ni \lambda \mapsto f(\lambda) = b(\lambda) - a$ and $\mathbb{R}^N \ni x \mapsto R_\nu(x) = \nu \log\left(\sum_{i=1}^{N} 2^{\frac{x_i}{\nu}}\right) \in \mathbb{R}$ it is clear that $\nabla_\lambda R_\nu(f(\lambda)) = \nabla G_\nu(\lambda)$. The basic idea is to define $\tilde{f}(\lambda) := \max_{1\le i\le N} f_i(\lambda)$ and then consider a function $g : \mathbb{R}^M \to \mathbb{R}^N$ given by $g_i(\lambda) = f_i(\lambda) - \tilde{f}(\lambda)$, such that all components of $g(\lambda)$ are non-positive. One can show that

$$\nabla_\lambda R_\nu(f(\lambda)) = \nabla_\lambda R_\nu(g(\lambda)) + \nabla \tilde{f}(\lambda),$$

where the term on the right-hand side can be computed with a small numerical error.

With the help of Lemma 3.12 we can state the main result of this section that quantifies the complexity of Algorithm 1 to compute an additive ε-close solution to the capacity of a cq-channel.

Theorem 3.15 (Complexity of Algorithm 1)**.** *Consider a cq channel with input alphabet size N and output dimension M. Then, Algorithm 1 requires $O((N \vee M)M^3 \log(N)^{1/2}\, \varepsilon^{-1})$ to compute an additive ε-close approximation to its capacity.*

Proof: Recall that a singular value decomposition of a matrix $A \in \mathbb{C}^{M\times M}$ can be done with complexity $O(M^3)$ [34, Lect. 31] which is needed for the projection operator π_Λ as explained in Proposition 3.11. A closer look at Algorithm 1 reveals that in case of no input constraint the complexity of a single iteration is $O(M^2(N \vee M))$. Lemma 3.12 implies that Algorithm 1 requires at most $4\sqrt{2D \log N}\ \varepsilon^{-1} + 4\sqrt{D/\varepsilon}$ iterations to find an ε-solution. Thus, the complexity to compute an ε-close solution using Algorithm 1 is $O((N \vee M)M^3 \log(N)^{1/2}\, \varepsilon^{-1})$. ∎

A. Simulation results

This section presents two examples to illustrate the performance of the approximation method introduced above. We consider two channels which both exhibit an analytical closed form solution for the capacity. The first example is a channel that satisfies Assumption 3.5, whereas the second one does not. To save computation time we have chosen two channels with a binary input alphabet. All the simulations in this section are performed on a 2.3 GHz Intel Core i7 processor with 8 GB RAM with Matlab.

Example 3.16. Consider a cq channel ρ with a binary input alphabet, i.e., $\mathcal{X} = \{0,1\}$, such that $0 \mapsto \rho_0 = \frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $1 \mapsto \rho_1 = \frac{1}{4}\left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. A simple calculation leads to an analytical expression of the capacity $C_{\mathsf{cq}}(\rho) = H_{\mathrm{b}}\big(\frac{16}{43}\big) - \frac{21}{43} - \frac{22}{43} H_{\mathrm{b}}\big(\frac{1}{4}\big) \approx 0.048821003204$. Note that $\operatorname{spec}(\rho_0) = \{\frac{1}{2}, \frac{1}{2}\}$ and $\operatorname{spec}(\rho_1) = \{\frac{1}{4}, \frac{3}{4}\}$, which gives $\gamma := \min_{x\in\mathcal{X}} \min \operatorname{spec}(\rho_x) = \frac{1}{4}$. As predicted by Lemma 3.12, Algorithm 1 has the following a priori error bound

$$0 \leq C_{\mathsf{cq},\mathrm{UB}}(\rho) - C_{\mathsf{cq},\mathrm{LB}}(\rho) \leq \frac{4\sqrt{2D \log N}}{k+1} + \frac{16D}{(k+1)^2},$$

where k denotes the number of iterations, $D = \frac{1}{2}(M \log\big(\gamma^{-1} \vee \mathrm{e}\big))^2 = 8$, $N = 2$, and $M = 2$. Table I shows the performance of Algorithm 1 for this example.

TABLE I

EXAMPLE 3.16 WITH $D = 8$

A priori error	10^{-1}	10^{-2}	10^{-3}	10^{-4}
$C_{\mathsf{cq},\mathrm{UB}}(\rho)$	0.049 841 307 3	0.048 972 899 3	0.048 837 263 6	0.048 822 641 1
$C_{\mathsf{cq},\mathrm{LB}}(\rho)$	0.048 820 977 3	0.048 820 982 7	0.048 821 003 3	0.048 821 003 6
A posteriori error	$1.00{\cdot}10^{-3}$	$1.52{\cdot}10^{-4}$	$1.63{\cdot}10^{-5}$	$1.64{\cdot}10^{-6}$
Time [s]	0.05	0.8	4.6	47
Iterations	167	1607	16 007	160 007

Example 3.17. Consider a cq channel ρ with a binary input alphabet, i.e., $\mathcal{X} = \{0,1\}$, such that $0 \mapsto \rho_0 = |0\rangle\langle 0| = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $1 \mapsto \rho_1 = |+\rangle\langle +| = \frac{1}{2}\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. The capacity of this channel can be computed to be $C_{\mathsf{cq}}(\rho) = H_{\mathrm{b}}\left(\frac{1}{2}(1 + \frac{1}{\sqrt{2}})\right) \approx 0.600876$. Note that $\operatorname{spec}(\rho_0) = \operatorname{spec}(\rho_1) = \{0,1\}$ which violates Assumption 3.5. As mentioned above a possible solution is to perturb the cq channel by some small parameter $\varepsilon \in (0, \frac{1}{2})$ such that Assumption 3.5 is valid. We consider the perturbed cq channel $\tilde{\rho}$ that maps $0 \mapsto \tilde{\rho}_0 = \left(\begin{smallmatrix} 1-\varepsilon & 0 \\ 0 & \varepsilon \end{smallmatrix}\right)$ and $1 \mapsto \tilde{\rho}_1 = \left(\begin{smallmatrix} \frac{1}{2}+\varepsilon & \frac{1}{2}-\varepsilon \\ \frac{1}{2}-\varepsilon & \frac{1}{2}-\varepsilon \end{smallmatrix}\right)$. By continuity of the von Neumann entropy [28], [29], when choosing ε being small we only change the value of the capacity by a small amount. More precisely, let us consider $\varepsilon = 10^{-10}$. A simple calculation gives

$$|C_{\mathsf{cq}}(\rho) - C_{\mathsf{cq}}(\tilde{\rho})| \leq 2.53474 \cdot 10^{-9}.$$

Using the triangle inequality and Lemma 3.12, we can bound the a priori error of Algorithm 1 as

$$\begin{aligned} |C_{\mathsf{cq},\mathrm{UB}}(\tilde{\rho}) - C_{\mathsf{cq}}(\rho)| &\leq |C_{\mathsf{cq},\mathrm{UB}}(\rho) - C_{\mathsf{cq}}(\tilde{\rho})| + |C_{\mathsf{cq}}(\tilde{\rho}) - C_{\mathsf{cq}}(\rho)| \\ &\leq \frac{4\sqrt{2D \log N}}{k+1} + \frac{16D}{(k+1)^2} + 2.53474 \cdot 10^{-9}, \end{aligned}$$

where k denotes the number of iterations, $D = \frac{1}{2}(M \log(\gamma^{-1} \vee \mathrm{e}))^2 \approx 2207.04$, $N = 2$, and $M = 2$. The a posteriori error is given by $C_{\mathsf{cq},\mathrm{UB}}(\tilde{\rho}) - C_{\mathsf{cq},\mathrm{LB}}(\tilde{\rho}) + 2.53474 \cdot 10^{-9}$.

4. CAPACITY OF A CONTINUOUS-INPUT CLASSICAL-QUANTUM CHANNEL

In this section we generalize the approach introduced in Section 3 to cq channels having a continuous bounded input alphabet and a finite-dimensional output. There are two major challenges compared to the discrete input alphabet setup treated in Section 3. The first difficulty is that the differential entropy is in general not bounded.

TABLE II

EXAMPLE 3.17 WITH $D \approx 2207.04$ USING A PERTURBATION PARAMETER $\varepsilon = 10^{-10}$.

A priori error	1	10^{-1}	10^{-2}
$C_{\mathrm{cq,UB}}(\tilde{\rho})$	0.600 876 033 385 197	0.600 876 033 316 571	0.600 876 033 316 571
$C_{\mathrm{cq,LB}}(\tilde{\rho})$	0.600 876 033 160 937	0.600 876 033 315 310	0.600 876 033 316 571
A posteriori error	$2.54{\cdot}10^{-9}$	$2.53{\cdot}10^{-9}$	$2.53{\cdot}10^{-9}$
Time [s]	0.1	0.8	7.9
Iterations	181	1392	13 353

This makes the smoothing step more difficult and in particular complicates the task of proving an a priori error bound. A second difficulty in the continuous input alphabet setting is the evaluation of the gradient of the Lagrange dual function which involves an integration that can only be computed approximately. Thus the robustness of the iterative protocol needs to be analyzed.[2]

Within this section, we consider cq channels of the form $\rho : \mathcal{P}(R) \to \mathcal{D}(\mathcal{H})$, $x \mapsto \rho_x$, where R is a compact subset of the non-negative real line, $\mathcal{P}(R)$ denotes the space of all probability distributions on R and $M := \dim \mathcal{H} < \infty$. In addition we consider an input constraint of the form[3]

$$\langle p, s \rangle = \int_R s(x)\, p(\mathrm{d}x) \leq S, \tag{23}$$

for $s \in \mathrm{L}^\infty(R)$ and $p \in \mathcal{P}(R)$. To properly state a formula describing the capacity of the channel ρ with an input constraint (23), we need to assume certain regularity conditions on the function s. Let $\{|e_i\rangle\}$ be an orthonormal basis in the Hilbert space $\mathcal{H}$ and $\{f_i\}$ a sequence of real numbers bounded from below. The expression

$$K\,|\psi\rangle = \sum_i f_i\, |e_i\rangle\, \langle e_i|\, \psi\rangle\,, \tag{24}$$

defines a self adjoint operator K on the dense domain

$$\mathsf{D}(K) = \left\{ \psi \in \mathcal{H} : \sum_i |f_i|^2\, |\langle e_i|\, \psi\rangle|^2 < \infty \right\}, \tag{25}$$

where f_i are the eigenvalues and $|e_i\rangle$ the corresponding eigenvectors.

Definition 4.1 ([3, Def. 11.3])**.** An operator defined on the domain (25) by the formula (24) is called *an operator of type* $\mathcal{K}$.

Assumption 4.2 (Assumptions on the input constraint function)**.** In the reminder of this section we impose the following assumption on the input constraint function $s : R \to \mathbb{R}$.

(i) There exists a self-adjoint operator K of type $\mathcal{K}$ satisfying $\mathrm{tr}\,[\exp(-\theta K)] < \infty$ for all $\theta > 0$ such that $s(x) \geq \mathrm{tr}\,[\rho_x K]$, $x \in R$.

(ii) s is lower semicontinuous and for all $k \in \mathbb{R}_{\geq 0}$ the set $\{x : s(x) \leq k\} \subset R$ is compact.

[2]This point will become especially important in Section 5.

[3]The extension to multiple average input cost constraints is straightforward.

Assumption 4.2(i) implies that $\sup_{p\in\mathcal{P}(R)} H\big(\int_R \rho_x\, p(\mathrm{d}x)\big) < \infty$ and Assumption 4.2(ii) ensures that the set $\{p \in \mathcal{P}(R) : \langle p, s\rangle \leq S\}$ is weakly compact [3, Lem. 11.14]. Under Assumption 4.2, the capacity of channel ρ is given by [3, Thm. 11.15]

$$C_{\mathsf{cq},S}(\rho) = \left\{ \begin{array}{ll} \max\limits_{p} & I(p,\rho) := H\big(\int_R \rho_x\, p(\mathrm{d}x)\big) - \langle p, H(\rho)\rangle \\ \text{s.t.} & \langle p, s\rangle \leq S \\ & p \in \mathcal{P}(R). \end{array} \right. \tag{26}$$

Proposition 4.3. *The optimization problem* (26) *is equivalent to*

$$C_{\mathsf{cq},S}(\rho) = \sup_{p\in\mathfrak{D}(R)} \big\{ I(p,\rho) \;:\; \langle p, s\rangle \leq S \big\}, \tag{27}$$

where $\mathfrak{D}(R)$ *is the space of probability densities with support* R*, i.e.,* $\mathfrak{D}(R) := \{f \in \mathrm{L}^1(R) \;:\; f \geq 0,\ \int_R f(x)\,\mathrm{d}x = 1\}$.

Proof: The proof follows by the proof of [20, Prop. 3.4] and the lower semicontinuity of the von Neumann entropy [3, Thm. 11.6]. ∎

We consider the pair of vector spaces $(\mathrm{L}^1(R), \mathrm{L}^\infty(R))$ along with the bilinear form

$$\langle f, g\rangle := \int_R f(x) g(x)\,\mathrm{d}x.$$

In the light of [35, Thm. 243G] this is a dual pair of vector spaces; we refer to [36, Sec. 3] for the details of the definition of dual pairs of vector spaces. Considering the Frobenius inner product as a bilinear form on the dual pair $(\mathrm{H}^M, \mathrm{H}^M)$, we define the linear operator $\mathcal{W} : \mathrm{H}^M \to \mathrm{L}^\infty(R)$ and its adjoint operator $\mathcal{W}^\star : \mathrm{L}^1(R) \to \mathrm{H}^M$ by

$$\mathcal{W}\lambda(x) := \mathrm{tr}\left[\rho_x \lambda\right], \qquad \mathcal{W}^\star p := \int_R \rho_x\, p(\mathrm{d}x).$$

We next derive the dual problem of (27) and show how to solve that efficiently. To this end, we introduce an additional decision variable $\sigma := \mathcal{W}^\star p$ and reformulate problem (27).

Lemma 4.4. *Let* $\mathcal{F} := \arg\max\limits_{p\in\mathfrak{D}(R)} I(p,\rho)$ *and* $S_{\max} := \min\limits_{p\in\mathcal{F}} \langle p, s\rangle$*. If* $S \geq S_{\max}$ *the optimization problem* (27) *has the same optimal value as*

$$\text{(primal problem)} \;:\; \left\{ \begin{array}{ll} \sup\limits_{p,\sigma} & H(\sigma) - \langle p, H(\rho)\rangle \\ \text{s.t.} & \sigma = \mathcal{W}^\star p \\ & p \in \mathfrak{D}(R),\ \sigma \in \mathcal{D}(\mathcal{H}). \end{array} \right.$$

If $S < S_{\max}$ *the optimization problem* (27) *has the same optimal value*

$$\text{(primal problem)} \;:\; \left\{ \begin{array}{ll} \sup\limits_{p,\sigma} & H(\sigma) - \langle p, H(\rho)\rangle \\ \text{s.t.} & \sigma = \mathcal{W}^\star p \\ & \langle p, s\rangle = S \\ & p \in \mathfrak{D}(R), \sigma \in \mathcal{D}(\mathcal{H}). \end{array} \right. \tag{28}$$

Proof: Follows by a similar argument as given in Appendix A for the finite-dimensional input setup. ∎

The Lagrange dual program to (28) is given by

$$(\text{dual problem}) \ : \ \begin{cases} \inf\limits_{\lambda} & G(\lambda)+F(\lambda) \\ \text{s.t.} & \lambda \in \mathrm{H}^M, \end{cases} \tag{29}$$

where $F, G : \mathrm{H}^M \to \mathbb{R}$ are given by

$$G(\lambda) = \begin{cases} \sup\limits_{p} & \langle p, \mathcal{W}\lambda \rangle - \langle p, H(\rho) \rangle \\ \text{s.t.} & \langle p, s \rangle = S \\ & p \in \mathfrak{D}(R) \end{cases} \quad \text{and} \quad F(\lambda) = \begin{cases} \max\limits_{\sigma} & H(\sigma) - \operatorname{tr}[\sigma\lambda] \\ \text{s.t.} & \sigma \in \mathcal{D}(\mathcal{H}) \end{cases}.$$

Note that $G(\lambda)$ is a (parametric) infinite-dimensional linear program and $F(\lambda)$ is exactly of the same form as in Section 3. According to (15) and (16) we thus have

$$F(\lambda) = \log\left(\operatorname{tr}\left[2^{-\lambda}\right]\right) \quad \text{and} \quad \nabla F(\lambda) = -\frac{2^{-\lambda}}{\operatorname{tr}\left[2^{-\lambda}\right]}. \tag{30}$$

Note that by Proposition 3.4, $\nabla F(\lambda)$ is Lipschitz continuous with respect to the Frobenius norm with Lipschitz constant 2.

Lemma 4.5. *Strong duality holds between* (28) *and* (29).

Proof: The lemma follows from the standard strong duality results of convex optimization, see [37, Thm. 6]. ■

In the remainder of this article we impose the following assumption on the cq channel.

Assumption 4.6 (Assumption on the cq channel)**.** $\gamma := \min\limits_{x \in R} \min \operatorname{spec}(\rho_x) > 0$

Lemma 4.7. *Under Assumption 4.6, the dual program* (29) *is equivalent to*

$$\min_{\lambda} \left\{ G(\lambda) + F(\lambda) \ : \ \lambda \in \Lambda \right\},$$

where $\Lambda := \left\{ \lambda \in \mathrm{H}^M \ : \ \|\lambda\|_F \leq M \log\left(\gamma^{-1} \vee \mathrm{e}\right) \right\}$.

Proof: The proof is a direct extension of the one for Lemma 3.6. ■

As a preliminary result, consider the following entropy maximization problem, with c being a continuous function, that exhibits an analytical solution

$$\begin{cases} \max\limits_{p} & h(p) + \langle p, c \rangle \\ \text{s.t.} & \langle p, s \rangle = S \\ & p \in \mathfrak{D}(R). \end{cases} \tag{31}$$

Lemma 4.8 (Entropy maximization [38, Thm. 12.1.1])**.** *Let* $p^\star(x) = 2^{\mu_1 + c(x) + \mu_2 s(x)}$, $x \in R$ *where* μ_1 *and* μ_2 *are chosen such that* $p^\star$ *satisfies the constraints in* (31)*. Then* $p^\star$ *uniquely solves* (31)*.*

The goal is to efficiently compute (29) which is not straightforward since $G(\cdot)$ is non-smooth. Similar as in Section 3 the idea is to use Nesterov's smoothing technique [17]. Therefore we consider

$$G_\nu(\lambda) = \begin{cases} \max\limits_{p} & \langle p, \mathcal{W}\lambda - H(\rho)\rangle + \nu h(p) - \nu \log(\upsilon) \\ \text{s.t.} & \langle p, s\rangle = S \\ & p \in \mathfrak{D}(R), \end{cases} \tag{32}$$

where $\upsilon := \int_R \mathrm{d}x$. Problem (32) is of the form given in Lemma 4.8 and therefore has a unique optimizer

$$p_\nu^\lambda(x) = 2^{\mu_1 + \frac{1}{\nu}(\mathrm{tr}[\rho_x \lambda] - H(\rho_x)) + \mu_2 s(x)}, \ x \in R, \tag{33}$$

where μ_1, μ_2 are chosen such that $p_\nu^\lambda \in \mathfrak{D}(R)$ and $\langle p_\nu^\lambda, s\rangle = S$. Recall that $h(p) \leq \log(\upsilon)$ for all $p \in \mathfrak{D}(R)$ and that there exists a function $\iota : \mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}$ such that

$$G_\nu(\lambda) \leq G(\lambda) \leq G_\nu(\lambda) + \iota(\nu) \quad \text{for all } \lambda \in \Lambda, \tag{34}$$

i.e., $G_\nu(\lambda)$ is a uniform approximation of the non-smooth function $G(\lambda)$. In Lemma 4.11 an explicit expression for ι is given, which implies that $\iota(\nu) \to 0$ as $\nu \to 0$.

Assumption 4.9 (Lipschitz continuity)**.**

(i) The input constraint function $s(\cdot)$ is Lipschitz continuous with constant L_s.

(ii) The function $R \ni x \mapsto \rho_x \in \mathcal{D}(\mathcal{H})$ is Lipschitz continuous with constant L with respect to the trace norm.

Lemma 4.10. *Assumption 4.9(ii) implies that the function $f_\lambda(x) := \mathcal{W}\lambda(x) - H(\rho_x)$ for $x \in R$ is Lipschitz continuous uniformly in $\lambda \in \Lambda$ with constant $L_f := L(M \log(\gamma^{-1} \vee \mathrm{e}) + \sqrt{M}\log(\frac{1}{\gamma\mathrm{e}} \vee \mathrm{e}))$.*

Proof: For $x_1, x_2 \in R$ using the triangle inequality we obtain

$$\begin{aligned} |f_\lambda(x_1) - f_\lambda(x_2)| &= \left|\langle \rho_{x_1}, \lambda\rangle_F - H(\rho_{x_1}) - \langle \rho_{x_2}, \lambda\rangle_F + H(\rho_{x_2})\right| \\ &\leq \left|\langle \rho_{x_1} - \rho_{x_2}, \lambda\rangle_F\right| + |H(\rho_{x_1}) - H(\rho_{x_2})|\,. \end{aligned} \tag{35}$$

We can bound the first term of (35) using the Cauchy-Schwarz inequality as

$$\begin{aligned} \left|\langle \rho_{x_1} - \rho_{x_2}, \lambda\rangle_F\right| &\leq \|\rho_{x_1} - \rho_{x_2}\|_F \, \|\lambda\|_F \\ &\leq \|\rho_{x_1} - \rho_{x_2}\|_{\mathrm{tr}} \, \|\lambda\|_F \\ &\leq L|x_1 - x_2| \, \|\lambda\|_F\,, \end{aligned} \tag{36}$$

where (36) follows by Assumption 4.9(ii) and by assumption $\|\lambda\|_F \leq M \log\left(\gamma^{-1} \vee \mathrm{e}\right)$. Let $J_M := \sqrt{M}\log(\frac{1}{\gamma\mathrm{e}} \vee \mathrm{e})$, using Claim F.3 and Assumption 4.6 the second term of (35) can be bounded as

$$\begin{aligned} |H(\rho_{x_1}) - H(\rho_{x_2})| &\leq J_M \, \|\rho_{x_1} - \rho_{x_2}\|_{\mathrm{tr}} \\ &\leq J_M L|x_1 - x_2|, \end{aligned} \tag{37}$$

where (37) follows again by Assumption 4.9(ii). ∎

Lemma 4.11 ([20]). *Under Assumption 4.9 a possible choice of the function ι in (34) is given by*

$$\iota(\nu) = \begin{cases} \nu\left(\log\left(\frac{T_1}{\nu} + T_2\right) + 1\right), & \nu < \frac{T_1}{1-T_2} \text{ or } T_2 > 1 \\ \nu, & \text{otherwise}, \end{cases}$$

where $T_1 := L_f \upsilon + 2L_f L_s \upsilon^2 \left(\frac{1}{-\underline{s}} \vee \frac{1}{\overline{s}}\right)$, $T_2 := L_s \upsilon(\underline{\mu} \vee \overline{\mu})$, $\underline{\mu} := \frac{2}{-\underline{s}} \log\left(\frac{2L_s\upsilon}{-\underline{s}} \vee 1\right)$, $\overline{\mu} := \frac{2}{\overline{s}} \log\left(\frac{2L_s\upsilon}{\overline{s}} \vee 1\right)$, $\upsilon := \int_R \mathrm{d}x$, $\underline{s} := -S + \min_{x\in R} s(x)$ *and* $\overline{s} := -S + \max_{x\in R} s(x)$.

Remark 4.12. In case of no input constraints, the unique optimizer to (32) is given by

$$p_\nu^\lambda(x) = \frac{2^{\frac{1}{\nu}(\mathrm{tr}[\rho_x \lambda] - H(\rho_x))}}{\int_R 2^{\frac{1}{\nu}(\mathrm{tr}[\rho_x \lambda] - H(\rho_x))}\,\mathrm{d}x},$$

whose straightforward evaluation is numerically difficult for small ν. A numerically stable technique to evaluate the above integral for small ν can be obtained by following the method presented in Remark 3.14.

Remark 4.13 ([20]). As already highlighted and discussed in Remark 3.9, in case of additional input constraints, we seek for an efficient method to find the coefficients μ_i in (33). Similarly to the finite input alphabet case the problem of finding μ_i can be reduced to the finite-dimensional convex optimization problem [32, p. 257 ff.]

$$\sup_{\mu\in\mathbb{R}^2} \left\{ \langle y, \mu\rangle - \int_R p_\nu^\lambda(x)\,\mathrm{d}x \right\}, \tag{38}$$

where $y := (1, S)$. Note that (38) is an unconstrained maximization of a concave function. However, unlike to the finite input alphabet case, the evaluation of its gradient and Hessian involves computing moments of the measure $p_\nu^\lambda(x,\mu)\,\mathrm{d}x$, which we want to avoid in view of computational efficiency. There are efficient numerical schemes known, based on semidefinite programming, to compute the gradient and Hessian (see [32, p. 259 ff.] for details).

Lemma 4.14 ([20, Lem. 3.14]). *The function $d : \mathfrak{D}(R) \to \mathbb{R}_{\geq 0}$, $p \mapsto -h(p) + \log(\upsilon)$ with $\upsilon := \int_R \mathrm{d}x$ as introduced in (32) is strongly convex with convexity parameter* 1.

Finally, we can show that the uniform approximation $G_\nu(\lambda)$ is smooth and has a Lipschitz continuous gradient with known constant. The following result is a generalization of Proposition 3.10 and follows from Theorem 5.1 in [39].

Proposition 4.15 (Lipschitz constant of ∇G_ν). *The function $G_\nu(\lambda)$ is well defined and continuously differentiable at any $\lambda \in \mathrm{H}^M$. Moreover, this function is convex and its gradient*

$$\nabla G_\nu(\lambda) = \int_R \rho_x\, p_\nu^\lambda(x)\,\mathrm{d}x$$

is Lipschitz continuous with constant $L_\nu = \frac{1}{\nu}$ with respect to the Frobenius norm.

Proof: See Appendix D. ∎

We consider the smooth, convex optimization problem

$$(\text{smoothed dual problem}) \;:\; \begin{cases} \min\limits_{\lambda} & F(\lambda) + G_\nu(\lambda) \\ \text{s.t.} & \lambda \in \Lambda, \end{cases} \tag{39}$$

whose solution can be approximated with the Algorithm 1 presented in Section 3. For the parameter $D_1 := \frac{1}{2}(M \log(\gamma^{-1} \vee \mathrm{e}))^2$ we have the following result, when running Algorithm 1 on the problem (39).

Theorem 4.16. *Let $\alpha := 2(T_1+T_2+1)$ where T_1 and T_2 are as defined in Lemma 4.11. Given a precision $\varepsilon \in (0, \frac{\alpha}{4})$, we set the smoothing parameter $\nu = \frac{\varepsilon/\alpha}{\log(\alpha/\varepsilon)}$ and number of iterations $k \geq \frac{1}{\varepsilon}\sqrt{16 D_1 \alpha}\sqrt{\log(\varepsilon^{-1}) + \log(\alpha) + \frac{1}{2}}$. Consider*

$$\hat{\lambda} = y_k \in \Lambda \qquad \text{and} \qquad \hat{p} = \sum_{i=0}^{k} \frac{2(i+1)}{(k+1)(k+2)} p_\nu^{\lambda_i} \in \mathcal{D}(R), \tag{40}$$

where y_i computed at the i^{th} iteration of Algorithm 1 and $p_\nu^{\lambda_i}$ is the analytical solution in (33). Then, $\hat{\lambda}$ and $\hat{p}$ are the approximate solutions to the problems (29) and (28), i.e.,

$$0 \leq F(\hat{\lambda}) + G(\hat{\lambda}) - I(\hat{p}, \rho) \leq \varepsilon. \tag{41}$$

Therefore, Algorithm 1 requires $O\left(\frac{1}{\varepsilon}\sqrt{\log(\varepsilon^{-1})}\right)$ iterations to find an ε-solution to the problems (28) and (29).

Proof: The proof is a minor modification of [20, Thm. 3.15]. ∎

Let us highlight that we have two different quantitative bounds for the approximation error. First, the *a priori* bound ε for which Theorem 4.16 prescribes a lower bound for the required number of iterations. Second, we have an *a posteriori* bound $F(\hat{\lambda}) + G(\hat{\lambda}) - I(\hat{p}, \rho)$ after k iterations. In practice, the a posteriori bound often approaches ε within significantly less number of iterations than predicted by Theorem 4.16. Besides, note that by (34) and Theorem 4.16

$$0 \leq F(\hat{\lambda}) + G_\nu(\hat{\lambda}) + \iota(\nu) - I(\hat{p}, \rho) \leq \iota(\nu) + \varepsilon,$$

which shows that $F(\hat{\lambda}) + G_\nu(\hat{\lambda}) + \iota(\nu)$ is an upper bound for the channel capacity with a priori error $\iota(\nu) + \varepsilon$. This bound can be particularly helpful in cases where an evaluation of $G(\lambda)$ for a given λ is hard.

Remark 4.17 (No input constraint)**.** In the absence of an input constraint we can derive an analytical expression for $G_\nu(\lambda)$ and its gradient. As derived above, the optimizer solving (32) is

$$p^\star(x) = \frac{2^{\mathrm{tr}[\rho_x \lambda] - H(\rho_x)}}{\int_R 2^{\mathrm{tr}[\rho_y \lambda] - H(\rho_y)} \, \mathrm{d}y}, \quad x \in R,$$

which gives

$$G_\nu(\lambda) = \nu \log\left(\int_R 2^{\frac{1}{\nu}(\mathrm{tr}[\rho_x \lambda] - H(\rho_x))} \, \mathrm{d}x\right) - \nu \log(\upsilon)$$

and

$$\frac{\partial G_\nu(\lambda)}{\partial \lambda_{m,\ell}} = (\nabla G_\nu(\lambda))_{m,\ell} = \frac{1}{S(\lambda)} \int_R 2^{\frac{1}{\nu}(\mathrm{tr}[\rho_x \lambda] - H(\rho_x))} (\rho_x)_{\ell,m} \, \mathrm{d}x, \tag{42}$$

with $S(\lambda) = \int_R 2^{\frac{1}{\nu}(\mathrm{tr}[\rho_x \lambda] - H(\rho_x))} \, \mathrm{d}x$. Similarly to Remark 3.14, we have used $\frac{\partial \mathrm{tr}[\rho\lambda]}{\partial \lambda_{m,\ell}} = \rho_{\ell,m}$ [23, Prop. 10.7.2].

A. Inexact first-order information

Our analysis up to now assumes availability of exact first-order information, namely we assumed that the gradients $\nabla G_\nu(\lambda)$ and $\nabla F(\lambda)$ are exactly available for any λ. However, in many cases, e.g., in the presence of an additional input cost constraint (Remark 4.13), the evaluation of those gradients requires solving another auxiliary optimization problem or a multi-dimensional integral (42), which only can be done approximately. This motivates the question of how to solve (39) in the case of inexact first-order information which indeed has been studied in detail in [40]. In our problem (39), $\nabla F(\lambda)$ has a closed form expression (30) and as such can be assumed to be known exactly. Let us assume, however, that we only have an oracle providing an approximation $\nabla \tilde{G}_\nu(\lambda)$, which satisfies $\|\nabla \tilde{G}_\nu(\lambda) - \nabla G_\nu(\lambda)\|_{\mathrm{op}} \leq \delta$ for any $\lambda \in \Lambda$ and some $\delta > 0$. Recall that π_Λ, as defined in Proposition 3.11, denotes the projection operator onto the set Λ, defined in Lemma 4.7, that is the Frobenius norm ball with radius $r := M \log\left(\gamma^{-1} \vee \mathrm{e}\right)$.

Algorithm 2: Scheme for inexact first-order information

Choose some $\lambda_0 \in \mathrm{H}^M$

For $m \geq 0$ **do***

Step 1: Compute $\nabla F(\lambda_m) + \nabla \tilde{G}_\nu(\lambda_m)$

Step 2: $\lambda_{m+1} = \pi_\Lambda\left(-\frac{1}{L_\nu}\left(\nabla F(\lambda_m) + \nabla \tilde{G}_\nu(\lambda_m)\right) + \lambda_m\right)$

[*The stopping criterion is explained in Remark 4.19]

Lemma 4.18. *For every $\nu \in \mathbb{R}_{>0}$, after k iterations of Algorithm 2*

$$F(\lambda_k) + G(\lambda_k) - C_{\mathsf{cq},S}(\rho) \leq \frac{(2+\frac{1}{\nu})D^2}{2k} + \iota(\nu) + 2\delta D, \tag{43}$$

where $\iota(\nu)$ is given in Lemma 4.11 and $D := M \log\left(\gamma^{-1} \vee \mathrm{e}\right)$.

Proof: We denote the optimum value to (39) by $C_{\nu,\mathsf{cq},S}(\rho)$. According to [40], for every $\nu \in \mathbb{R}_{>0}$, after k iterations of Algorithm 2

$$F(\lambda_k) + G_\nu(\lambda_k) - C_{\nu,\mathsf{cq},S}(\rho) \leq \frac{(2+\frac{1}{\nu})D^2}{2k} + 2\delta D. \tag{44}$$

By recalling (34), which leads to $C_{\nu,\mathsf{cq},S}(\rho) \leq C_{\mathsf{cq},S}(\rho)$ the statement can be refined to

$$F(\lambda_k) + G(\lambda_k) - C_{\mathsf{cq},S}(\rho) \leq \frac{(2+\frac{1}{\nu})D^2}{2k} + \iota(\nu) + 2\delta D.$$

■

Remark 4.19 (Stopping criterion of Algorithm 2)**.** In case of no average power constraint the following explicit formulas can be used as a stopping criterion of Algorithm 2. Choose an a priori error $\varepsilon > 0$. For $\beta := 1 + \frac{\log \mathrm{e}}{\mathrm{e}}$ and $\alpha := \log T_1 + 1$, where T_1 is as in Lemma 4.11, consider $\nu \leq \frac{\varepsilon}{3\beta(\alpha + \log(3\beta\varepsilon^{-1}))}$, $k \geq \frac{3(M\log(\gamma^{-1}\vee \mathrm{e}))^2(2\varepsilon + 3\beta(\alpha+\log(3\beta\varepsilon^{-1})))}{2\varepsilon^2}$ and $\delta \leq \frac{\varepsilon}{6M\log(\gamma^{-1}\vee \mathrm{e})}$. For this choice Algorithm 2 guarantees an ε-close solution, i.e., the right hand side of (43) is upper bounded by ε. This analysis follows by Lemma E.1 that is given in Appendix E.

5. Approximating the Holevo Capacity

In this section it is shown how ideas developed in the previous sections for cq channels can be extended to quantum channels with a quantum mechanical input and output, also known as qq channels. Let $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ be a quantum channel, where $\mathcal{B}(\mathcal{H})$ denotes the space of bounded linear operators on some Hilbert space $\mathcal{H}$ that are equipped with the trace norm. The classical capacity describing the maximal amount of classical information that can be sent on average, asymptotically reliable over the channel Φ per channel use, has proven to be [4], [5]

$$C(\Phi) = \lim_{k\to\infty} \frac{1}{k} C_{\mathcal{X}}(\Phi^{\otimes k}), \tag{45}$$

where

$$C_{\mathcal{X}}(\Phi) = \sup_{\{p_i,\rho_i\}} H\left(\sum_i p_i \Phi(\rho_i)\right) - \sum_i p_i H(\Phi(\rho_i))\,, \tag{46}$$

denotes the Holevo capacity. It is immediate to verify that $C(\Phi) \geq C_{\mathcal{X}}(\Phi)$ for all quantum channels Φ. In [11], the existence of channels satisfying $C(\Phi) > C_{\mathcal{X}}(\Phi)$ has been proven which implies that the limit in (45) which is called *regularization* is necessary. Due to the regularization, a direct approximation of $C(\Phi)$ seems difficult.

In this section, we present an approximation scheme for the Holevo capacity based on the method explained in Section 4. It has been shown that the supremum in (46) is attained on an ensemble consisting of no more than N^2 pure states, where $N := \dim \mathcal{H}_A$ [3, Cor. 8.5]. The Holevo capacity is in general hard to compute since (46) is a non-convex optimization problem as the objective function is concave in $\{p_i\}$ for fixed $\{\rho_i\}$ and convex in $\{\rho_i\}$ for fixed $\{p_i\}$ [2, Thms. 12.3.5 and 12.3.6]. Furthermore, Beigi and Shor showed that computing the Holevo capacity is NP-hard [12]. Their proof also implies that it is NP-hard to compute the Holevo capacity up to $\frac{1}{\mathrm{poly}(N)}$ accuracy. Based on a stronger complexity assumption, Harrow and Montanaro improved this result by showing that the Holevo capacity is in general hard to approximate even up to a constant accuracy [13]. However, this does not preclude the existence of classes of channels for which the Holevo capacity can be computed efficiently.

Using a universal encoder, which is a mapping translating a classical state into a quantum state, we can compute the Holevo capacity of a quantum channel by calculating the cq capacity of a channel having a continuous, bounded input alphabet (see Figure 2). A universal encoder is defined as the mapping $\mathsf{E} : R \ni r \mapsto |r\rangle\langle r| =: \rho_r \in \mathcal{D}(\mathcal{H}_A)$. From an optimization point of view, by adding the universal encoder we map a finite-dimensional non-convex optimization problem (of the form (46)) into an infinite-dimensional convex optimization problem (of the form (27)), which we know how to approximate as discussed in Section 4. To represent an N-dimensional pure state we need $2N-2$ real bounded variables.[4] As an example, for $N = 2$ a possible universal encoder is $\mathsf{E} : [0,\pi]\times[0,2\pi] \ni (\phi,\theta) \mapsto |v\rangle\langle v| \in \mathbb{C}^{2\times 2}$, with $|v\rangle = (\cos\theta, \sin\theta\, e^{\mathrm{i}\phi})^\top$. A possible universal encoder for a general N-dimensional setup is discussed in Remark 5.1.

As explained in Figure 2, using the idea of the universal encoder gives $C_{\mathsf{cq}}(\rho) = C_{\mathcal{X}}(\Phi)$, i.e., we can approximate $C_{\mathcal{X}}(\Phi)$ by approximating $C_{\mathsf{cq}}(\rho)$. This can be done as explained in Section 4. For an approximation error $\varepsilon > 0$,

[4]We need to describe an N-dimensional complex vector, where one real parameter can be removed since the global phase is irrelevant. A second parameter is determined as the vector must have unit length.

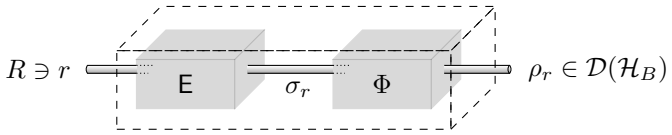

Fig. 2. **How to embed a qq into a cq channel.** A universal encoder is a mapping $\mathsf{E} : R \ni r \mapsto |r\rangle\langle r| =: \sigma_r \in \mathcal{D}(\mathcal{H}_A)$ that translates a classical state r into a quantum state σ_r. It can be used to embed the qq channel $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ 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, leading to $C_{\mathsf{cq}}(\rho) = C_{\mathcal{X}}(\Phi)$.

Theorem 4.16 gives a minimal number of iterations k and a smoothing parameter $\nu > 0$ such that after k iterations Algorithm 1 generates a lower and upper bound $C_{\mathcal{X},\mathrm{LB}}(\Phi) \leq C_{\mathcal{X}}(\Phi) \leq C_{\mathcal{X},\mathrm{UB}}(\Phi)$ to the Holevo capacity such that

$$0 \leq C_{\mathcal{X},\mathrm{UB}}(\Phi) - C_{\mathcal{X},\mathrm{LB}}(\Phi) \leq \varepsilon.$$

We note that in the limit $k \to \infty$, where k denotes the number of iterations, Theorem 4.16 ensues that the capacity achieving input distribution for the induced cq channel, i.e. $\rho : R \ni r \mapsto (\Phi \circ \mathsf{E})(r) \in \mathcal{D}(\mathcal{H}_B)$ converges to a discrete probability distribution which then defines an ensemble that achieves the Holevo capacity of Φ. This is in agreement with the observations made in [26, Thm. 2].

Remark 5.1 (Universal encoder)**.** For a channel $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ with $N = \dim \mathcal{H}_A$ a possible universal encoder can be derived using spherical coordinates as

$$\begin{aligned}\mathsf{E} : R = [0,\pi] \times \ldots \times [0,\pi] \times [0,2\pi] \times [0,\pi] \times \ldots \times [0,\pi] &\to \mathbb{C}^{N\times N}\\ (\theta_1,\ldots,\theta_{N-2},\theta_{N-1},\phi_1,\ldots,\phi_{N-1}) &\mapsto |v\rangle\langle v|\end{aligned}$$

with

$$\begin{aligned}|v\rangle = (&\cos\theta_1, \sin\theta_1\cos\theta_2 e^{\mathrm{i}\phi_1}, \sin\theta_1\sin\theta_2\cos\theta_3 e^{\mathrm{i}\phi_2}, \ldots, \sin\theta_1\ldots\sin\theta_{N-2}\cos\theta_{N-1}e^{\mathrm{i}\phi_{N-2}},\\ &\sin\theta_1\ldots\sin\theta_{N-2}\sin\theta_{N-1}e^{\mathrm{i}\phi_{N-1}})^\top.\end{aligned}$$

It can be verified immediately that the Lebesgue measure of the set R is equal to $2\pi^{2N-2}$ for this setup.

A. Computational complexity

Let $\{\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)\}_{N,M}$ be a family of quantum channels with $N := \dim \mathcal{H}_A$ and $M := \dim \mathcal{H}_B$. For such a family, we derive the complexity of our method presented in this chapter to ensure an ε-close solution. Suppose the family of channels $\{\Phi\}_{N,M}$ satisfies the following assumption.

Assumption 5.2 (Regularity)**.** $\gamma_M := \min_{\rho\in\mathcal{D}(\mathcal{H}_A)} \min \operatorname{spec} \Phi(\rho) > 0$

To simplify notation, define the function $\mathbb{R}_{\geq 0} \ni M \mapsto \mathrm{p}(M) := \log\left(\gamma_M^{-1}\right) \in \mathbb{R}_{\geq 0}$. We will discuss later in Remark 5.9 how Assumption 5.2 can be removed at the cost of computational complexity proportional to $\varepsilon^{-1}\log\varepsilon^{-1}$ where ε is the preassigned approximation error, i.e., considering ε as a constant Assumption 5.2 can be

automatically satisfied. As detailed in the preceding section and summarized in Algorithm 1, for the approximation of the Holevo capacity one requires to efficiently evaluate the gradient $\nabla G_\nu(\lambda)$ for an arbitrary $\lambda \in \Lambda$ given by (42), which involves two integrations over R.

Definition 5.3 (Gradient oracle complexity)**.** Given a family of channels $\{\Phi\}_{N,M}$, the computational complexity for Algorithm $\mathscr{A}$ to provide an estimate $\nabla \tilde{G}_\nu(\lambda)$ for any $\lambda \in \Lambda$ of the form

$$\mathbb{P}\left[\left\|\nabla G_\nu(\lambda) - \nabla \tilde{G}_\nu(\lambda)\right\|_{\mathrm{op}} \geq \delta\right] \leq \eta$$

is denoted (when it exists) by $\mathscr{C}_{\Phi,\mathscr{A}}(N, M, \delta^{-1}, \eta^{-1})$.[5]

In Section 5-B, we discuss two candidates for $\mathscr{A}$ and derive their complexity as defined in Definition 5.3.

Theorem 5.4 (Complexity of Algorithm 2)**.** *Let $\{\Phi\}_{N,M}$ be a family of quantum channels satisfying Assumption 5.2. Then, Algorithm 2 together with $\mathscr{A}$ require*

$$O\Big(\varepsilon^{-2} M^4 \mathrm{p}(M)^2 \big(N + \log(M\mathrm{p}(M)) + \log(\varepsilon^{-1})\big) \\ \mathscr{C}_{\Phi,\mathscr{A}}\big(N, M, \varepsilon^{-1} M\mathrm{p}(M), \xi^{-1}\varepsilon^{-2} M^2 \mathrm{p}(M)^2 (N + \log(M\mathrm{p}(M)) + \log(\varepsilon^{-1}))\big)\Big)$$

to compute an additive ε-close solution to the Holevo capacity with probability $1 - \xi$.

Remark 5.5. Theorem 5.4 establishes a link in terms of computational complexity from the main objective of this section, the Holevo capacity of a family of quantum channels $\{\Phi\}_{N,M}$ under Assumption 5.2, to the computation of $\nabla G_\nu(\lambda)$ for a given $\lambda \in \Lambda$, the task of Algorithm $\mathscr{A}$ in Definition 5.3. That is, if $\mathscr{C}(N, M, \delta^{-1}, \eta^{-1})$ for δ^{-1} and η^{-1} given in Theorem 5.4 is polynomial (resp. sub-exponential) in (N, ε^{-1}), then the complexity of the proposed scheme to approximate the Holevo capacity is polynomial (resp. sub-exponential) in (N, ε^{-1}).

To prove Theorem 5.4 one requires a few preparatory lemmas. First we need an explicit a priori error bound in a similar fashion as in Section 4 given that the function $f_{\lambda,M}(x) := \mathrm{tr}\left[\Phi(\mathsf{E}(x))\lambda\right] - H(\Phi(\mathsf{E}(x)))$ is Lipschitz continuous uniformly in $\lambda \in \Lambda$. The following lemma shows that this readily follows from Assumption 5.2.

Lemma 5.6. *Let $\{\Phi\}_{N,M}$ be a family of channels satisfying Assumption 5.2. The function $f_{\lambda,M}(x) := \mathrm{tr}\left[\Phi(\mathsf{E}(x))\lambda\right] - H(\Phi(\mathsf{E}(x)))$ for $x \in R$ is Lipschitz continuous uniformly in $\lambda \in \Lambda$ with respect to the ℓ^1-norm with constant $L_{N,M} = 2N\sqrt{N}\left(M \log(\frac{1}{\gamma_M} \vee \mathrm{e}) + \sqrt{M}\log(\frac{1}{\gamma_M \mathrm{e}} \vee \mathrm{e})\right)$.*

Proof: See Appendix F. ∎

Lemma 5.7. *Let $\eta \in [0,1]$ and $n \in \mathbb{N}$. Then $1 - (1-\eta)^n \leq n\eta$.*

Proof: For a fixed $n \in \mathbb{N}$ the function $[0,1] \ni \eta \mapsto f(\eta) := 1 - (1-\eta)^n - n\eta$ is concave since $\frac{\mathrm{d}^2 f(\eta)}{\mathrm{d}\eta} = -n(n-1)(1-\eta)^{n-2} \leq 0$. Solving $\frac{\mathrm{d}f(\eta)}{\mathrm{d}\eta} = 0$, gives $\eta^\star = 0$. As $f(0) = 0$ and $f(1) = 1 - n \leq 0$ this proves that $f(\eta) \leq 0$ for all $n \in \mathbb{N}$ and $\eta \in [0,1]$. ∎

[5]Note that $\mathscr{C}_{\Phi,\mathscr{A}}(N, M, \delta^{-1}, \eta^{-1})$ is increasing in all its components.

Proof of Theorem 5.4: Recall that according to Lemma 4.18, after k iterations of Algorithm 2, where the gradient $\nabla G_\nu(\lambda_i)$ in each iteration i is approximated with $\nabla \tilde{G}_\nu(\lambda_i)$ using Algorithm $\mathscr{A}$ as introduced in Definition 5.3, we get

$$F(\lambda_k) + G(\lambda_k) - C_{\mathcal{X}}(\Phi) \leq \frac{(2+\frac{1}{\nu})D^2}{2k} + \iota(\nu) + 2\delta D, \tag{47}$$

where the function $\iota(\cdot)$ is given in (48).

As ensured by Definition 5.3 with probability $1-\eta$ the numerically evaluated gradient $\nabla \tilde{G}_\nu(\lambda)$ is close to its exact value $\nabla G_\nu(\lambda)$ or more precisely with probability at least $1-\eta$, $\nabla \tilde{G}_\nu(\lambda) \in \mathcal{A}$, where $\mathcal{A} := \{X \in \mathbb{C}^{n\times n} : \|\nabla G_\nu(\lambda) - X\|_{\mathrm{op}} < \delta\}$ denotes a confidence region. We first derive the complexity of finding an ε-close solution to $C_{\mathcal{X}}(\Phi)$ given that in every iteration step the numerically evaluated gradient lies in the confidence region $\mathcal{A}$. Afterwards we justify that the probability that the gradient in all iteration steps is evaluated approximately correctly, i.e., such that its value lies inside the confidence region, is high.

Recall that for our setup the function $\iota(\cdot)$ in (47) has the form

$$\iota(\nu) = \begin{cases} \nu \log\left(\frac{L_{N,M} 2\pi^{2N-2}}{\nu}\right) + \nu, & \nu < L_{N,M}(2\pi^{2N-2}) \\ \nu, & \text{otherwise,} \end{cases} \tag{48}$$

as given in Lemma 4.11 with $L_{N,M}$ defined in Lemma 5.6. Note that we use a universal encoder as introduced in Remark 5.1 which gives $\upsilon = \int_R \mathrm{d}x = 2\pi^{2N-2}$.

According to Remark 4.19 and (48) we define $\beta = 1 + \frac{\log \mathrm{e}}{\mathrm{e}}$ and $\alpha := \log(L_{N,M}) + (2N-2)\log(2\pi) + 1$, which by Lemma 5.6 scales as $\alpha = O(N + \log(N^{3/2} M \mathrm{p}(M)))$. Following Remark 4.19 the number of iterations k and the gradient approximation accuracy δ are chosen such that

$$k = O\Big(\varepsilon^{-2} M^2 \mathrm{p}(M)^2 \left(N + \log(M\mathrm{p}(M)) + \log(\varepsilon^{-1})\right)\Big). \tag{49}$$

$$\delta \leq \tfrac{\varepsilon}{6M\log(\gamma^{-1}\vee \mathrm{e})} = O\left(\frac{\varepsilon}{M\mathrm{p}(M)}\right). \tag{50}$$

As shown in Remark 4.19, for these two parameters with a smoothing parameter $\nu \leq \frac{\varepsilon}{3\beta(\alpha+\log(3\beta\varepsilon^{-1}))}$ after k iterations of Algorithm 2 we obtain an ε-close solution. The total complexity for an ε-solution is k times the complexity of a single iteration which is

$$\begin{aligned} & k\, O\big(M^2 \mathscr{C}_{\Phi,\mathscr{A}}(N, M, \delta^{-1}, \eta^{-1})\big) \\ & \quad = k\, O\big(M^2 \mathscr{C}_{\Phi,\mathscr{A}}(N, M, \varepsilon^{-1} M \log(\mathrm{p}(M)), \eta^{-1})\big) \\ & \quad = O\big(\varepsilon^{-2} M^4 \mathrm{p}(M)^2 \left(N + \log(M\mathrm{p}(M)) + \log(\varepsilon^{-1})\right) \mathscr{C}_{\Phi,\mathscr{A}}(N, M, \varepsilon^{-1} M \log(\mathrm{p}(M)), \eta^{-1})\big), \end{aligned}$$

where we used (49) and (50).

We next show that the randomized scheme is reliable with probability $1-\xi$. As mentioned in Definition 5.3 each evaluation of the gradient $\nabla \tilde{G}_\nu(\lambda)$ is confident with a probability not smaller than $(1-\eta)$. The scheme is successful if the gradient evaluation lies inside the confidence region in each iteration step. Thus the probability that the approximation scheme fails can be bounded by

$$\mathbb{P}[\text{scheme fails}] \leq 1 - (1-\eta)^k \leq k\eta = O(\varepsilon^{-2} M^2 \mathrm{p}(M)^2 \left(N + \log(M\mathrm{p}(M)) + \log(\varepsilon^{-1})\right) \eta),$$

where the second inequality is due to Lemma 5.7 and (49). Therefore for $\eta^{-1} = k\,\xi^{-1}$ the scheme is reliable with probability $1-\xi$.

■

Proposition 5.8 (Continuity of the Holevo capacity [41, Cor. 11])**.** *Let $\Phi_1, \Phi_2 : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ be two quantum channels with $M = \dim \mathcal{H}_B$ such that $\|\Phi_1 - \Phi_2\|_\diamond \leq \varepsilon$ for $\varepsilon \geq 0$, then*

$$|C_\mathcal{X}(\Phi_1) - C_\mathcal{X}(\Phi_2)| \leq 8\varepsilon \log(M) + 4H_\mathrm{b}(\varepsilon).$$

Remark 5.9 (Removing Assumption 5.2)**.** The continuity of the Holevo capacity can be used to remove Assumption 5.2. Let $\{\Phi_1\}_{N,M}$ be a family of quantum channels that violates Assumption 5.2. Consider the family $\{\Phi_2\}_{N,M} := \{(1-\xi_{N,M})\Phi_1 + \xi_{N,M}\Theta\}_{N,M}$ for $\xi_{N,M} \in (0,1)$ with $\Theta(\rho) = \mathrm{tr}\,[\rho]\,\frac{\mathbb{1}}{M}$. Using the triangle inequality we find for each member of the two families

$$\|\Phi_1 - \Phi_2\|_\diamond = \|\xi_{N,M}(\Theta - \Phi_1)\|_\diamond \leq \xi_{N,M}(\|\Theta\|_\diamond + \|\Phi_1\|_\diamond) \leq 2\xi_{N,M}, \tag{51}$$

where the final inequality uses the fact that the trace norm of a channel is always upper bounded by one. Note that the family $\{\Phi_2\}$ as defined above clearly satisfies Assumption 5.2 as $\Phi_2(\rho) \geq \xi_{N,M}\frac{\mathbb{1}}{M}$ for all $\rho \in \mathcal{D}(\mathcal{H}_A)$. Hence, Proposition 5.8 in conjunction with the analysis of Lemma E.1 shows that Assumption 5.2 is not restrictive in the sense that one can always suggest a family of channel satisfying Assumption 5.2 that is ε-close to the original channel in terms of diamond norm at the cost of $O(\varepsilon^{-1}\log\varepsilon^{-1})$.

B. Gradient approximation

As shown in the previous section, the crucial element for our approximation method is Algorithm $\mathscr{A}$ to approximate the gradient $G_\nu(\lambda)$ that is given in (42). In this section we propose two candidates and discuss their corresponding complexity function $\mathscr{C}_{\Phi,\mathscr{A}}$. The main idea is to approximate $\nabla G_\nu(\lambda)$ via a probabilistic method.

First approach: uniform sampling: This approach relies on a simple randomized algorithm generating independent samples from a uniform distribution. Consider

$$\nabla\tilde{G}_\nu(\lambda) := \frac{\sum_{i=1}^n 2^{\frac{1}{\nu}(\mathrm{tr}[\Phi(\mathsf{E}(X_i))\lambda] - H(\Phi(\mathsf{E}(X_i))))}\Phi(\mathsf{E}(X_i))}{\sum_{i=1}^n 2^{\frac{1}{\nu}(\mathrm{tr}[\Phi(\mathsf{E}(X_i))\lambda] - H(\Phi(\mathsf{E}(X_i))))}}, \tag{52}$$

where $\{X_i\}_{i=1}^n$ are i.i.d. random variables uniformly distributed on R. In Lemma 5.10 we derive a measure concentration bound to quantify the approximation error. As above, we denote by $L_{N,M}$ the Lipschitz constant of the function $f_{\lambda,M}(x) := \mathrm{tr}\,[\Phi(\mathsf{E}(x))\lambda] - H(\Phi(\mathsf{E}(x)))$ with respect to the ℓ^1-norm.

Lemma 5.10. *For every $0 \leq \delta \leq 2^{\frac{-\sqrt{N}L_{N,M}}{\nu} - 1}$*

$$\mathbb{P}\left[\left\|\nabla G_\nu(\lambda) - \nabla\tilde{G}_\nu(\lambda)\right\|_{\mathrm{op}} \geq \delta\right] \leq M\exp\left(-\delta^2 n K_{N,M}\right) =: \eta$$

for $K_{N,M} := \frac{1}{576}2^{\frac{-4\sqrt{N}L_{N,M}}{\nu}}$.

Proof: See Appendix G. ■

Corollary 5.11. *Let $\{\Phi\}_{N,M}$ be a family of channels and $\varepsilon > 0$. With high probability, using Algorithm 2 with a uniform sampling method as explained in Lemma 5.10, the complexity for an ε-close solution to the Holevo capacity is*

$$O\left(M^6 \log(M\log M)^4 \Big(N + \log\big(M\log(M\log M)\big)\Big) 2^{c(N^{3/2}+N^{1/2}\log(N^{3/2}M\log(M\log M)))L_{N,M}}\right),$$

where $c > 0$ is a constant.

Proof: See Appendix H. ∎

Corollary 5.12 (Subexponential or polynomial running time)**.** *Let $\varepsilon > 0$. Given a family of channels $\{\Phi\}_{N,M}$ with $M = \mathrm{poly}(N)$ such that*

(i) $\frac{1}{L_{N,M}} = \Omega(N^{3/2})$. Then the method described in this section, using an integration method explained in Lemma 5.10, provides with high probability an ε-approximation to the Holevo capacity with a complexity $O\big(M^6 \log(M\log M)^4 (N + \log(M\log(M\log M)))\big) = \mathrm{poly}(N)$.

(ii) $\frac{1}{L_{N,M}} = \Omega(N^{1/2+\alpha})$ for $\alpha > 0$. Then the method described in this section, using an integration method explained in Lemma 5.10, provides with high probability an ε-approximation to the Holevo capacity with a complexity $O\big(M^6 \log(M\log M)^4 (N + \log(M\log(M\log M))) \, 2^{cN^{1-\alpha}}\big) = \mathrm{subexp}(N)$ for a constant $c > 0$.

Proof: Follows directly from Corollary 5.11. ∎

The following example presents families of channels $\{\Phi\}_{N,M}$ with an arbitrarily scaling Lipschitz constant $L_{N,M}$.

Example 5.13 (Family of channels with an arbitrary Lipschitz constant)**.** Consider the family of channels $\{\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)\}_{N,M}$ that maps $\rho \mapsto (1-\phi(N,M))\frac{\mathbf{1}}{M} + \phi(N,M)\Theta(\rho)$, where $\Theta : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ denotes an arbitrary cptp map and $\phi(N,M) \geq 0$. Following the lines of the proof of Lemma 5.6 using that $\|\Phi(\rho_1) - \Phi(\rho_2)\|_{\mathrm{tr}} = \phi(N,M)\,\|\Theta(\rho_1) - \Theta(\rho_2)\|_{\mathrm{tr}} \leq \phi(N,M)\,\|\rho_1 - \rho_2\|_{\mathrm{tr}}$ it follows that the Lipschitz constant $L_{N,M}$ with respect to the ℓ^1-norm of the function $f_{\lambda,M}$ as defined in Lemma 5.6 if given by $L_{N,M} = (2M\sqrt{M}(\log(\frac{1}{\gamma_M} \vee \mathrm{e})) + 2M(\log(\frac{1}{\gamma_M \mathrm{e}} \vee \mathrm{e})))\phi(N,M)$.

Second approach: importance sampling: The second approach invokes a non-trivial sampling method, known as *importance sampling* [42]. Define the function $f_\lambda(x) := \mathrm{tr}\left[\Phi(\mathsf{E}(x))\lambda\right] - H(\Phi(\mathsf{E}(x)))$ such that the gradient of $G_\nu(\lambda)$, given in (42), can be expressed as

$$\nabla G_\nu(\lambda) = \frac{\int_R 2^{\frac{1}{\nu} f_\lambda(x)} \Phi(\mathsf{E}(x))\,\mathrm{d}x}{\int_R 2^{\frac{1}{\nu} f_\lambda(x)}\,\mathrm{d}x} = \mathbb{E}^Q[\Phi(\mathsf{E}(x))]\,,$$

where the expectation is with respect to the probability density $Q(x) = \frac{2^{\frac{1}{\nu} f_\lambda(x)}}{\int_R 2^{\frac{1}{\nu} f_\lambda(x)}\,\mathrm{d}x}$. Consider i.i.d. random variables $\{X_i\}_{i=1}^n$ according to the density Q and define the random variable $Z_n := \frac{1}{n}\sum_{i=1}^n \Phi(\mathsf{E}(X_i))$.

Lemma 5.14. *For every $t \geq 0$ and $n \in \mathbb{N}$, $\mathbb{P}\Big[\|\nabla G_\nu(\lambda) - Z_n\|_{\mathrm{op}} \geq t\Big] \leq M \exp\left(\frac{-t^2 n}{32}\right)$.*

Proof: The function defined as $R^n \ni x \mapsto f(x_1,\dots,x_n) := \frac{1}{n}\sum_{i=1}^n \Phi(\mathsf{E}(x_i))$ satisfies the following bounded difference assumption

$$\left\|(f(x_1,\dots,x_i,\dots,x_n) - f(x_1,\dots,x_{i-1},x_{i'},x_{i+1},\dots,x_n))^2\right\|_{\rm op} \leq \left(\frac{1}{n}(\Phi(\mathsf{E}(x_i)) - \Phi(\mathsf{E}(x_{i'})))\right)^2 \tag{53}$$

$$\leq \frac{4}{n^2}, \tag{54}$$

where (53) follows from $\left\|(B-C)^2\right\|_{\rm op} = \left\|B^2 - BC - CB - C^2\right\|_{\rm op} \leq \left\|B^2\right\|_{\rm op} + \|BC\|_{\rm op} + \|CB\|_{\rm op} + \left\|C^2\right\|_{\rm op} \leq \|B\|_{\rm op}^2 + 2\,\|B\|_{\rm op}\,\|C\|_{\rm op} + \|C\|_{\rm op}^2 = (\|B\|_{\rm op} + \|C\|_{\rm op})^2$ which uses the submultiplicative property of the operator norm. Inequality (54) is due to the fact that $\Phi(\mathsf{E}(x))$ are density operators for all $x \in R$. Hence, by the matrix McDiarmid inequality [18, Cor. 7.5], we get the concentration bound

$$\mathbb{P}\Big[\|\nabla G_\nu(\lambda) - Z_n\|_{\rm op} \geq t\Big] \leq M \exp\left(\frac{-t^2 n}{32}\right).$$

■

The main difficulty in this approach is how to obtain samples $\{X_i\}_{i=1}^n$ according to the density Q given above and in particular quantifying its computational complexity. It is well known that if the density Q has a particular structure this samples can be drawn efficiently, e.g., if Q is a log-concave density in polynomial time [43]. Providing assumptions on the channel Φ such that sampling according to Q can be done efficiently is a topic of further research.

Remark 5.15. Let $\mathscr{S}(N,M)$ denote the computational cost of drawing one sample according to the density Q. Then, Lemma 5.14 shows that the computational complexity the gradient approximation given in Definition 5.3 using the importance sampling algorithm is $\mathscr{C}_{\Phi,\mathscr{A}}(N,M,\delta^{-1},\eta^{-1}) = \mathscr{S}(N,M)\frac{32}{\delta^2}\ln\left(\frac{M}{\eta}\right)$.

C. Simulation results

The following three examples show the performance of our method to compute the Holevo capacity. In the first example we compute the classical capacity of a depolarizing channel. In the second example we demonstrate how to compute the classical capacity of an arbitrary qubit Pauli channel. As a third example, we have chosen a random qubit-input qubit-output channel for which the Holevo capacity is unknown.

The Choi-Jamiolkowski representation ensures that every quantum channel $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ can be written as

$$\sigma_B = \Phi(\rho_A) = N\,\mathrm{tr}_A((\mathcal{T}_A(\rho_A)\otimes \mathrm{id}_B)\,\tau_{AB}),$$

where $\mathcal{T}_A(\cdot)$ is the transpose mapping and τ_{AB} denotes a density operator that fully characterizes the quantum channel and that satisfies $\mathrm{tr}_B(\tau_{AB}) = \frac{1}{N}\mathbf{1}$. For the following examples we use this representation of the channel.

Note that our method works for arbitrary quantum channels having a finite input dimension. The reason we have chosen qubit channels is to save computation time. All the simulations in this section are performed on a 2.3 GHz Intel Core i7 processor with 8 GB RAM with Matlab. For the evaluation of the gradient ∇G_ν that involves the computation of an integral over the domain $[0,\pi]\times[0,2\pi]$ we used a trapezoidal method with a grid having 100×200 points.

Example 5.16 (Qubit depolarizing channel)**.** We consider the depolarizing channel with input and ouput dimension 2, that can be described by the map $\rho_A \to (1-p)\rho_A + p\frac{1}{2}\mathbf{1}$, for $p \in [0,1]$. Its Choi state is given by $\tau_{AB} = (1-p)\left|\omega\right\rangle\!\left\langle\omega\right| + \frac{p}{4}\mathbf{1}$, where $\left|\omega\right\rangle$ denotes a maximally entangled state. The Holevo capacity of the depolarizing channel can be computed analytically being [2, Thm. 19.4.2]

$$C_{\mathcal{X}}(p) = 1 + \left(1-\frac{p}{2}\right)\log\left(1-\frac{p}{2}\right) + \frac{p}{2}\log\left(\frac{p}{2}\right) = 1 - H_{\mathrm{b}}\left(\frac{p}{2}\right). \tag{55}$$

Table III shows the performance of our algorithm for the task of approximating the Holevo capacity for the depolarizing channel with parameter $p = \frac{1}{3}$. According to (55) the precise value of the Holevo capacity is $C_{\mathcal{X}}(p = \frac{1}{4}) = 1 - H_{\mathrm{b}}(\frac{1}{6}) \approx 0.3499775784$.

TABLE III
HOLEVO CAPACITY OF A DEPOLARIZING CHANNEL WITH $p = \frac{1}{3}$.

Iterations	10	10^2	10^3
ν	0.1602	0.0174	0.0018
$C_{\mathcal{X},\mathrm{UB}}$	0.3603	0.3500	0.3500
$C_{\mathcal{X},\mathrm{LB}}$	0.3500	0.3500	0.3500
A posteriori error	$1.029{\cdot}10^{-2}$	$3.401{\cdot}10^{-5}$	$8.019{\cdot}10^{-6}$
Time [s]	414	4144	41578

Example 5.17 (Qubit Pauli channel)**.** Consider the general Pauli channel Φ for an input and output dimension 2, which can be described by the map $\rho_A \to (1-p_X-p_Y-p_Z)\rho_A + p_X X\rho_A X + p_Y Y\rho_A Y + p_Z Z\rho_A Z$, where X,Y,Z denote the Pauli matrices and $p_X, p_Y, p_Z \in [0,1]$ such that $p_X + p_Y + p_Z \in [0,1]$. The Choi state τ_{AB} representing this channel can be computed to be

$$\tau_{AB} = \frac{1}{2}\begin{pmatrix} 1-p_X-p_Y & 0 & 0 & 1-p_X-p_Y-2p_Z \\ 0 & p_X+p_Y & p_X-p_Y & 0 \\ 0 & p_X-p_Y & p_X+p_Y & 0 \\ 1-p_X-p_Y-2p_Z & 0 & 0 & 1-p_X-p_Y \end{pmatrix}.$$

King proved that the Holevo capacity is additive for product channels, under the condition that one of the channels is a *unital* qubit channel, with the other completely arbitrary [44].[6] As Pauli channels are unital channels, the Holevo capacity is therefore equal to the classical capacity for arbitrary Pauli qubit channels. Due to their symmetry properties it is possible to derive a close-form expression for the classical capacity of an arbitrary Pauli channel (as discussed e.g., in [45]). Let $\alpha := 1-2p_Y-2p_Z$, $\beta := 1-2p_X-2p_Z$ and $\gamma := 1-2p_Y-2p_Z$, then

$$C(\Phi) = C_{\mathcal{X}}(\Phi) = 1 - H_{\mathrm{b}}\left(\frac{1+(|\alpha| \vee |\beta| \vee |\gamma|)}{2}\right). \tag{56}$$

Our method introduced above allows us to approximate the Holevo capacity. To demonstrate this we compute upper and lower bounds for the Holevo capacity of a qubit Pauli channel with $p_X = \frac{1}{7}$, $p_Y = \frac{1}{10}$ and $p_Z = \frac{1}{4}$ as shown in Table IV. According to (56) for this setup we have $C(\Phi) = C_{\mathcal{X}}(\Phi) = 1 - H_{\mathrm{b}}(\frac{53}{70}) \approx 0.2002405887$.

[6]Unital channels are channels that map the identity to the identity, i.e., $\Phi(\mathrm{id}) = \mathrm{id}$.

TABLE IV

HOLEVO CAPACITY OF A QUBIT PAULI CHANNEL WITH $p_X = \frac{1}{7}$, $p_Y = \frac{1}{10}$ AND $p_Z = \frac{1}{4}$.

Iterations	10	10^2	10^3
ν	0.1265	0.0138	0.0014
$C_{\mathcal{X},\mathrm{UB}}$	0.2026	0.2002	0.2002
$C_{\mathcal{X},\mathrm{LB}}$	0.1399	0.1894	0.1983
A posteriori error	$6.267{\cdot}10^{-2}$	$1.087{\cdot}10^{-2}$	$1.940{\cdot}10^{-3}$
Time [s]	409	3919	40154

Example 5.18 (Random qubit channel)**.** We consider a random qubit-input qubit-output channel $\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ with $N = \dim(\mathcal{H}_A) = d_B = \dim(\mathcal{H}_B) = 2$. More precisely, we consider the Choi state of Φ, which is given by

$$\tau_{AB} = \frac{1}{N}(\rho_A^{-\frac{1}{2}} \otimes \mathrm{id}_B)\, \rho_{AB}\, (\rho_A^{-\frac{1}{2}} \otimes \mathrm{id}_B),$$

where ρ_{AB} is a random density matrix.[7] To demonstrate the performance of our method, let

$$\tau_{AB} = \begin{pmatrix} 0.2041 & -0.1145 - 0.0926\mathrm{i} & 0.0590 - 0.0187\mathrm{i} & 0.0721 + 0.0487\mathrm{i} \\ -0.1145 + 0.0926\mathrm{i} & 0.2959 & -0.0861 - 0.0928\mathrm{i} & -0.0590 + 0.00187\mathrm{i} \\ 0.0590 + 0.0187\mathrm{i} & -0.0861 + 0.0928\mathrm{i} & 0.2350 & -0.1296 + 0.0128\mathrm{i} \\ 0.0721 - 0.0487\mathrm{i} & -0.0590 - 0.0187\mathrm{i} & -0.1296 - 0.0128\mathrm{i} & 0.2650 \end{pmatrix}. \tag{57}$$

Table V shows the performance of the presented algorithm to approximate the Holevo capacity of this random qubit channel.

TABLE V

HOLEVO CAPACITY OF A RANDOM QQ-CHANNEL DESCRIBED BY ITS CHOI STATE GIVEN IN (57).

Iterations	10	10^2	10^3
ν	0.2575	0.0280	0.0028
$C_{\mathcal{X},\mathrm{UB}}$	0.3928	0.2648	0.2573
$C_{\mathcal{X},\mathrm{LB}}$	0.0900	0.2032	0.2522
A posteriori error	$3.028{\cdot}10^{-1}$	$6.156{\cdot}10^{-2}$	$5.061{\cdot}10^{-3}$
Time [s]	421	4025	41630

6. DISCUSSION

Due to its operational significance, knowing the capacity of a channel is of fundamental importance. As in general no closed form expression to the capacity is known, this motivates the study of approximation methods. In particular as the channel dimension increases the computational complexity of the approximation scheme becomes

[7]There are different methods to generate random density matrices which is however not relevant for this work. The interested reader might consider [46] for further information.

important. Numerical results (see Section 3-A and Section 5-C) show that the theoretical work presented in this article performs well in practice. The optimization problem characterizing the Holevo capacity of a qq channel has been shown to be NP-hard [12] and also difficult to approximate [13]. However, this does not preclude the existence of certain classes of channels for which the Holevo capacity can be approximated efficiently. Our approach via its smoothed dual version allows us to reduce the original Holevo capacity problem to a multi-dimensional integration — a problem that has been well-studied in the literature and oftentimes can be solved efficiently [42].

Recall that the classical capacity of a quantum channel $\Phi : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is given by its regularized Holevo capacity, i.e.,

$$C(\Phi) = \lim_{k\to\infty} \frac{1}{k} C_{\mathcal{X}}(\Phi^{\otimes k}). \tag{58}$$

The regularization required in (58) makes the classical capacity of a quantum channel difficult to compute. If for some channel Φ the Holevo capacity is additive, i.e., $C_{\mathcal{X}}(\Phi \otimes \Theta) = C_{\mathcal{X}}(\Phi) + C_{\mathcal{X}}(\Theta)$ for an arbitrary channel Θ, this implies that $C(\Phi) = C_{\mathcal{X}}(\Phi)$ making the classical capacity a lot simpler to compute and proves that entangled states at the encoder do not help to improve the rate. For a while there existed a conjecture that the Holevo capacity is additive for all quantum channels. In 2009 using techniques from measure concentration, Hastings disproved the conjecture by constructing high-dimensional random quantum channels whose Holevo capacity is provably not additive [11]. However, it remains unsolved whether there exist explicit low-dimensional quantum channels whose Holevo capacity is not additive. Our approximation scheme can be used to check the additivity of the Holevo capacity for channels with low dimensions.

The number of iterations the presented approximation scheme requires for an additive ε-solution highly depends on the Lipschitz constant estimate of the objective's gradient. Recently there has been some work motivating an adaptive estimate of the local Lipschitz constant that has been shown to be very efficient in practice (up to three orders of magnitude reduction of computation time), while preserving the worst-case complexity [47]. This may help to achieve a faster convergence for our algorithm, i.e., a smaller number of iterations would be required to achieve a certain approximation error. Another idea to reduce the computation time of the approximation scheme is to make use of possible symmetry properties the channel might have. More precisely, certain symmetry properties could enable us to restrict the set R over which one has to integrate in order to evaluate the gradient ∇G_ν. This would speed up the computational cost per iteration considerably.

We believe that the presented framework can be employed 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 [48], the *quantum rate distortion function* describing the maximal compression rate up to a certain distortion [49], the *channel coherent information* which is the best generic lower bound to the quantum capacity characterizing the highest possible rate at which quantum information can be transmitted reliably over a quantum channel [3], and the *channel private information* giving a lower bound on how much information can be securely and reliably transmitted over a channel which is of importance for example in quantum key distribution (QKD) [50], [51]. The proposed framework in this article has proven useful to approximate the capacity of classical channels whose value is unknown, e.g., the capacity of

a discrete-time Poisson channel [20].

APPENDIX A
PROOF OF LEMMA 3.2

This proof follows a very similar structure as the proof of Lemma 2.1 in [20]. Adding the constraint $\sigma := \sum_{i=1}^{N} p_i \rho_i$ gives $I(p,\rho) = H(\sigma) - \sum_{i=1}^{N} p_i H(\rho_i)$. Since $p \in \Delta_N$ and $\rho_i \in \mathcal{D}(\mathcal{H})$ for all $1 \leq i \leq N$ it follows that $\sigma \in \mathcal{D}(\mathcal{H})$.

By definition of $S_{\max}$ it is clear that the constraint $\langle p, s \rangle \leq S$ is inactive if $S \geq S_{\max}$ proving (10). It remains to show that for $S < S_{\max}$ the optimization problems (8) and (11) are equivalent. To keep notation simple, let $C_{\mathsf{cq}}(S) := C_{\mathsf{cq},S}(\rho)$ for some fixed cq channel ρ. We next prove that $C_{\mathsf{cq}}(S)$ is concave in S for $S \in [0, S_{\max}]$. Let $S^{(1)}, S^{(2)} \in [0, S_{\max}]$, $\lambda \in [0,1]$ and let $p^{(i)}$ be capacity achieving input distribution for $C_{\mathsf{cq}}(S^{(i)})$ with $i \in \{1,2\}$. Let $p^{(\lambda)} := \lambda p^{(1)} + (1-\lambda) p^{(2)}$, which gives

$$\begin{aligned} \left\langle s, p^{(\lambda)} \right\rangle &= \lambda \left\langle s, p^{(1)} \right\rangle + (1-\lambda) \left\langle s, p^{(2)} \right\rangle \\ &\leq \lambda S^{(1)} + (1-\lambda) S^{(2)} \\ &=: S^{(\lambda)} \in [0, S_{\max}]. \end{aligned}$$

Using the fact that $p \mapsto I(p,\rho)$ is concave[8] we obtain

$$\begin{aligned} \lambda C_{\mathsf{cq}}(S^{(1)}) + (1-\lambda) C_{\mathsf{cq}}(S^{(2)}) &= \lambda I\left(p^{(1)}, \rho\right) + (1-\lambda) I\left(p^{(2)}, \rho\right) \\ &\leq I\left(p^{(\lambda)}, \rho\right) \\ &\leq C_{\mathsf{cq}}(S^{(\lambda)}), \end{aligned}$$

where the final inequality follows from (8).

$C_{\mathsf{cq}}(S)$ is clearly non-degreasing in S as enlarging S relaxes the input cost constraint. We next show that $C_{\mathsf{cq}}(S)$ is even strictly increasing in $S \in [0, S_{\max}]$. We first prove that for all $\varepsilon > 0$,

$$C_{\mathsf{cq}}(S_{\max} - \varepsilon) < C_{\mathsf{cq}}(S_{\max}). \tag{59}$$

Suppose $C_{\mathsf{cq}}(S_{\max} - \varepsilon) = C_{\mathsf{cq}}(S_{\max})$ and denote $C_{\mathsf{cq}}^{\star} = \max_{p \in \Delta_N} I(p,\rho)$. This implies that there exists a $\bar{p} \in \Delta_N$ such that $I(\bar{p},\rho) = C_{\mathsf{cq}}^{\star}$ and $\langle \bar{p}, s \rangle = S_{\max} - \varepsilon$, which contradicts the definition of $S_{\max}$. Thus by concavity of $C_{\mathsf{cq}}(S)$ together with the the non-decreasing property and (59) imply that $C_{\mathsf{cq}}(S)$ is strictly increasing in S.

Finally, assume that $C_{\mathsf{cq}}(S)$ is achieved for $p^{\star} \in \Delta_N$ such that $\langle p^{\star}, s \rangle = \bar{S} < S$. For

$$C_{\mathsf{cq}}(\bar{S}) := \left\{ \begin{array}{ll} \max\limits_{p} & I(p,\rho) \\ \text{s.t.} & \langle p, s \rangle \leq \bar{S} \\ & p \in \Delta_N, \end{array} \right.$$

we then have $C_{\mathsf{cq}}(\bar{S}) = I(p^{\star},\rho) = C_{\mathsf{cq}}(S)$, which is a contradiction as $C_{\mathsf{cq}}(S)$ is strictly increasing in $S \in [0, S_{\max}]$. □

[8]This follows directly from the well known fact that $p \mapsto H(p)$ is concave.

APPENDIX B
PROOF OF LEMMA 3.6

The proof is extending the ideas used to prove [20, Lem. 2.4]. Consider the following two optimization problems

$$\mathsf{P}_\beta : \begin{cases} \max\limits_{p,\sigma,\varepsilon} & H(\sigma) - \sum_{i=1}^N p_i H(\rho_i) - \beta\varepsilon \\ \text{s.t.} & \left\| \sum_{i=1}^N p_i\rho_i - \sigma \right\|_{\text{op}} \leq \varepsilon \\ & \left\langle p, s \right\rangle = S \\ & p \in \Delta_N, \sigma \in \mathcal{D}(\mathcal{H}), \varepsilon \in \mathbb{R}_{\geq 0} \end{cases} \quad \text{and} \quad \mathsf{D}_\beta : \begin{cases} \min\limits_{\lambda} & F(\lambda) + G(\lambda) \\ \text{s.t.} & \|\lambda\|_{\text{tr}} \leq \beta \\ & \lambda \in \mathrm{H}^M. \end{cases}$$

Claim B.1. *Strong duality holds between* P_β *and* D_β.

Proof: According to the identity $\left\| \sum_{i=1}^N p_i\rho_i - \sigma \right\|_{\text{op}} = \max_{\|\lambda\|_{\text{tr}} \leq 1} \left\langle \lambda, \sum_{i=1}^N p_i\rho_i - \sigma \right\rangle_F$ [3, p. 7] the optimization problem P_β can be rewritten as

$$\mathsf{P}_\beta : \begin{cases} \max\limits_{p,\sigma} & H(\sigma) - \sum_{i=1}^N p_i H(\rho_i) + \min\limits_{\|\lambda\|_{\text{tr}} \leq \beta} \left\langle \lambda, \sum_{i=1}^N p_i\rho_i - \sigma \right\rangle_F \\ \text{s.t.} & \left\langle p, s \right\rangle = S \\ & p \in \Delta_N, \sigma \in \mathcal{D}(\mathcal{H}), \end{cases}$$

whose dual program, where strong duality holds according to [22, Prop. 5.3.1, p. 169] is given by

$$\begin{cases} \min\limits_{\|\lambda\|_{\text{tr}} \leq \beta} \max\limits_{p,\sigma} & H(\sigma) - \sum_{i=1}^N p_i H(\rho_i) + \left\langle \lambda, \sum_{i=1}^N p_i\rho_i - \sigma \right\rangle_F \\ \text{s.t.} & \left\langle p, s \right\rangle = S \\ & p \in \Delta_N, \sigma \in \mathcal{D}(\mathcal{H}), \end{cases}$$

which clearly is equivalent to D_β with $F(\cdot)$ and $G(\cdot)$ as given in (13). ∎

We denote by $\varepsilon^\star(\beta)$ the optimizer of P_β with the respective optimal value $J_\beta^\star$. Note that for

$$J(\varepsilon) := \begin{cases} \max\limits_{p,\sigma} & H(\sigma) - \sum_{i=1}^N p_i H(\rho_i) \\ \text{s.t.} & \left\| \sum_{i=1}^N p_i\rho_i - \sigma \right\|_{\text{op}} \leq \varepsilon \\ & \left\langle p, s \right\rangle = S \\ & p \in \Delta_N, \sigma \in \mathcal{D}(\mathcal{H}) \end{cases}, \tag{60}$$

the mapping $\varepsilon \mapsto J(\varepsilon)$, the so-called perturbation function, is concave [52, p. 268]. In a next step we write the optimization problem (60) in another equivalent form

$$J(\varepsilon) = \begin{cases} \max\limits_{p,v} & -\sum_{i=1}^N p_i H(\rho_i) + H\left(\sum_{i=1}^N p_i\rho_i + \varepsilon v \right) \\ \text{s.t.} & \|v\|_{\text{op}} \leq 1 \\ & \left\langle p, s \right\rangle = S \\ & p \in \Delta_N,\ v \in \mathrm{H}^M. \end{cases} \tag{61}$$

The main idea of the proof is to show that for a sufficiently large β, which we will quantify in the following, the optimizer $\varepsilon^\star(\beta)$ of P_β is equal to zero. That is, in light of the duality relations, the constraint $\|\lambda\|_{\text{tr}} \leq \frac{\beta}{2}$ in D_β

is inactive and as such D_β is equivalent to (12). By using Taylor's theorem, there exists a $y_\varepsilon \in [0,\varepsilon]$ such that the entropy term in the objective function of (61) can be bounded as

$$\begin{aligned} H\left(\sum_{i=1}^N p_i\rho_i + \varepsilon v\right) &= H\left(\sum_{i=1}^N p_i\rho_i\right) - \left\langle \log\left(\sum_{i=1}^N p_i\rho_i\right) + \tfrac{1}{\ln 2}\mathbf{1}, v\right\rangle_F \varepsilon \\ &\quad - \left\langle \left(\sum_{i=1}^N p_i\rho_i + y_\varepsilon v\right)^{-1}, v^2\right\rangle_F \varepsilon^2 \tfrac{1}{\ln 2} \\ &\leq H\left(\sum_{i=1}^N p_i\rho_i\right) - \left\langle \log\left(\sum_{i=1}^N p_i\rho_i\right) + \tfrac{1}{\ln 2}\mathbf{1}, v\right\rangle_F \varepsilon + \frac{M}{\gamma \ln 2}\varepsilon^2. \end{aligned} \tag{62}$$

Thus, the optimal value of problem P_β can be expressed as

$$\begin{aligned} J_\beta^\star &= \max_\varepsilon \{J(\varepsilon) - \beta\varepsilon\} \\ &\leq \max_\varepsilon \left\{ \max_{p,v} \left[-\sum_{i=1}^N p_i H(\rho_i) + H\left(\sum_{i=1}^N p_i\rho_i\right) \right.\right. \\ &\qquad \left.\left. - \left\langle \log\left(\sum_{i=1}^N p_i\rho_i\right) + \tfrac{1}{\ln 2}\mathbf{1}, v\right\rangle_F \varepsilon \;:\; \langle p, s\rangle = S \right] + \frac{M}{\gamma \ln 2}\varepsilon^2 - \beta\varepsilon \right\} \qquad (63) \\ &\leq \max_\varepsilon \left\{ \max_{p,v} \left[-\sum_{i=1}^N p_i H(\rho_i) + H\left(\sum_{i=1}^N p_i\rho_i\right) \;:\; \langle p, s\rangle = S \right] \right. \\ &\qquad \left. + (\rho - \beta)\varepsilon + \frac{M}{\gamma \ln 2}\varepsilon^2 \right\} \qquad (64) \\ &= J(0) + \max_\varepsilon \left\{ (\rho - \beta)\varepsilon \; + \frac{M}{\gamma \ln 2}\varepsilon^2 \right\}, \qquad (65) \end{aligned}$$

where $\rho = M\left(\log(\gamma^{-1}) \vee \frac{1}{\ln 2}\right)$. Note that (63) follows from (61) and (62). The equation (64) uses the fact that $-\left\langle \log\left(\sum_{i=1}^N p_i\rho_i\right) + \frac{1}{\ln 2}\mathbf{1}, v\right\rangle_F \leq M\left(\log(\gamma^{-1}) \vee \frac{1}{\ln 2}\right)$. Thus, for $\beta > \rho$ and $\varepsilon_1 = \frac{N\gamma}{M}(\rho - \beta)$, we get $\max_{\varepsilon \leq \varepsilon_1}\left\{(\rho - \beta)\varepsilon + \frac{M}{\gamma \ln 2}\varepsilon^2\right\} = 0$. Therefore, (65) together with the concavity of ε implies that $J(0)$ is the global optimum of $J(\varepsilon)$ and as such $\varepsilon^\star(\beta) = 0$ for $\beta > \rho$, indicating that P_β is equivalent to (11) in the sense that $J_\beta^\star = J_0^\star$. By strong duality this implies that the constraint $\|\lambda\|_{\mathrm{tr}} \leq \beta$ in D_β is inactive. Finally, $\|\lambda\|_F \leq \|\lambda\|_{\mathrm{tr}}$ concludes the proof. □

Appendix C
Proof of Proposition 3.10

The proof follows directly from the proof of Theorem 1 and Lemma 3 in [17] together with the following analysis. Consider the operator $\mathcal{W} : \mathcal{H}^* \to \mathbb{R}^N$ by $\mathcal{W}\lambda := \left(\langle \rho_1, \lambda\rangle_F, \ldots, \langle \rho_N, \lambda\rangle_F\right)^\top$. Its operator norm can be bounded as

$$\begin{aligned} \|\mathcal{W}\|_{\mathrm{op}} &= \max_{\lambda \in \mathrm{H}^M,\; p \in \Delta_N} \left\{ \langle p, \mathcal{W}\lambda\rangle \;:\; \|\lambda\|_F = 1,\; \|p\|_1 = 1 \right\} \\ &\leq \max_{\lambda \in \mathrm{H}^M,\; p \in \Delta_N} \left\{ \left| \sum_{i=1}^N \langle \rho_i, \lambda\rangle_F p_i \right| \;:\; \|\lambda\|_F = 1,\; \|p\|_1 = 1 \right\} \\ &\leq \max_{\lambda \in \mathrm{H}^M,\; p \in \Delta_N} \left\{ \sum_{i=1}^N \left|\langle \rho_i, \lambda\rangle_F\right| p_i \;:\; \|\lambda\|_F = 1,\; \|p\|_1 = 1 \right\} \end{aligned} \tag{66}$$

$$\leq \max_{p\in\Delta_N} \left\{ \sum_{i=1}^{N} \|\rho_i\|_F \, p_i \;\; : \|\lambda\|_F = 1, \;\; \|p\|_1 = 1 \right\} \tag{67}$$

$$\leq 1,$$

where (66) follows from the triangle inequality, (67) from Cauchy Schwarz and the last step is due to the fact that

$$\|\rho_i\|_F \leq \|\sqrt{\rho_i}\|_F \|\sqrt{\rho_i}\|_F \tag{68}$$

$$= \sqrt{\mathrm{tr}\left[\sqrt{\rho_i}\sqrt{\rho_i}^\dagger\right]}\sqrt{\mathrm{tr}\left[\sqrt{\rho_i}\sqrt{\rho_i}^\dagger\right]}$$

$$= \sqrt{\mathrm{tr}\left[\sqrt{\rho_i}\sqrt{\rho_i^\dagger}\right]}\sqrt{\mathrm{tr}\left[\sqrt{\rho_i}\sqrt{\rho_i^\dagger}\right]} \tag{69}$$

$$= \sqrt{\mathrm{tr}\left[\rho_i\right]}\sqrt{\mathrm{tr}\left[\rho_i\right]} \tag{70}$$

$$= 1, \tag{71}$$

where (68) is due to the submultiplicative property of the Frobenius norm and (69) follows from the fact that ρ_i is positive semi-definite. Finally, (70) and (71) follow since ρ_i is a density operator. □

APPENDIX D
PROOF OF PROPOSITION 4.15

It is known, according to Theorem 5.1 in [39], that $G_\nu(\lambda)$ is well defined and continuously differentiable at any $\lambda \in Q$ and that this function is convex and its gradient $\nabla G_\nu(\lambda) = \mathcal{W}^\star p_\nu^\lambda$ is Lipschitz continuous with constant $L_\nu = \frac{1}{\nu}\|\mathcal{W}\|^2$, where we have also used Lemma 4.14. The operator norm can be simplified to

$$\|\mathcal{W}\|_{\mathrm{op}} := \sup_{\lambda\in \mathrm{H}^M,\, p\in \mathrm{L}^1(R)} \left\{ \langle p, \mathcal{W}\lambda\rangle \;\; : \;\; \|\lambda\|_F = 1, \;\; \|p\|_1 = 1 \right\}$$

$$\leq \sup_{\lambda\in \mathrm{H}^M,\, p\in \mathrm{L}^1(R)} \left\{ \left| \int_R \mathrm{tr}\left[\rho_x \lambda\right] \, p(x)\,\mathrm{d}x \right| : \;\; \|\lambda\|_F = 1, \;\; \|p\|_1 = 1 \right\}$$

$$\leq \sup_{\lambda\in \mathrm{H}^M,\, p\in \mathrm{L}^1(R)} \left\{ \int_R \left|\mathrm{tr}\left[\rho_x \lambda\right]\right| \, p(x)\,\mathrm{d}x : \;\; \|\lambda\|_F = 1, \;\; \|p\|_1 = 1 \right\} \tag{72}$$

$$\leq \sup_{\lambda\in \mathrm{H}^M,\, p\in \mathrm{L}^1(R)} \left\{ \int_R \|\rho_x\|_F \, p(x)\,\mathrm{d}x : \;\; \|p\|_1 = 1 \right\} \tag{73}$$

$$\leq \sup_{p\in \mathrm{L}^1(R)} \left\{ \int_R p(x)\,\mathrm{d}x : \;\; \|p\|_1 = 1 \right\} \tag{74}$$

$$\leq 1,$$

where (72) follows from the triangle inequality, (73) from Cauchy-Schwarz and (74) is due to (71). □

APPENDIX E
JUSTIFICATION OF REMARK 4.19

Lemma E.1. *For $\alpha \in \mathbb{R}_{\geq 0}$, consider the function $\mathbb{R}_{>0} \ni \nu \mapsto \iota(\nu) := \nu\left(\log \nu^{-1} + \alpha\right) \in \mathbb{R}$. For all $\varepsilon \in \left(0, 2^\alpha\left(1 + \frac{\log \mathrm{e}}{\mathrm{e}}\right)\right)$ if $\nu \leq \frac{\varepsilon}{\left(1+\frac{\log \mathrm{e}}{\mathrm{e}}\right)\left(\alpha+\log\left(\left(1+\frac{\log \mathrm{e}}{\mathrm{e}}\right)\varepsilon^{-1}\right)\right)}$, then $\iota(\nu) \leq \varepsilon$.*

Proof: Note that for all $\bar{\varepsilon} \in (0,1)$

$$\iota\left(\frac{2^{\alpha}\bar{\varepsilon}}{\log \bar{\varepsilon}^{-1}}\right) = 2^{\alpha}\bar{\varepsilon}\left(1+\frac{\log\log \bar{\varepsilon}^{-1}}{\log \bar{\varepsilon}^{-1}}\right) \leq 2^{\alpha}\bar{\varepsilon}\left(1+\frac{\log \mathrm{e}}{\mathrm{e}}\right),$$

where the last step is due to the fact that $\frac{\log x}{x} \leq \frac{\log \mathrm{e}}{\mathrm{e}}$ for all $x \in \mathbb{R}_{>0}$ is used. It then suffices to consider $\varepsilon := 2^{\alpha}\left(1+\frac{\log \mathrm{e}}{\mathrm{e}}\right)\bar{\varepsilon}$. ∎

APPENDIX F
PROOF OF LEMMA 5.6

Claim F.1. *The function $R \ni r \mapsto |r\rangle \in \mathbb{C}^N$ as given in Remark 5.1 satisfies $\||r_1\rangle - |r_2\rangle\|_1 \leq N \|r_1 - r_2\|_1$.*

Proof: Using the simple fact that if $f, g : \mathbb{R} \to [0,1]$ are two Lipschitz continuous function with constant L_g and L_f then $f(\cdot)+g(\cdot)$ is Lipschitz continuous with constant $L_f + L_g$ we get

$$\||r_1\rangle - |r_2\rangle\|_1 = \sum_{i=1}^{N} \big||r_1\rangle_i - |r_2\rangle_i\big| \leq N \|r_1 - r_2\|_1 . \tag{75}$$

∎

Claim F.2. *The function $\Delta_n \ni x \mapsto f(x) = x\,x^{\top} \in \mathbb{R}^{n\times n}_{\geq 0}$ satisfies $\|f(x) - f(y)\|_{\mathrm{tr}} \leq 2\sqrt{n}\,\|x-y\|_1$.*

Proof: Let $x, y \in \Delta_n$, then by Cauchy-Schwarz we find

$$\begin{aligned}
\|f(x) - f(y)\|_F^2 &= \|x\,x^{\top} - y\,y^{\top}\|_F^2 \\
&= \|x\|_2^4 + \|y\|_2^4 - 2\left\langle x, y\right\rangle^2 \\
&\leq \|x\|_2^4 + \|y\|_2^4 - 2\left\langle x, y\right\rangle^2 + 2\|x\|_2^2\|y\|_2^2 - 2\left\langle x, y\right\rangle^2 \\
&= \left(\|x\|_2^2 + \|y\|_2^2\right)^2 - \left(2\left\langle x, y\right\rangle\right)^2 \\
&= \left(\|x\|_2^2 + \|y\|_2^2 + 2\left\langle x, y\right\rangle\right)\left(\|x\|_2^2 + \|y\|_2^2 - 2\left\langle x, y\right\rangle\right) \\
&= \left(\|x\|_2^2 + \|y\|_2^2 + 2\left\langle x, y\right\rangle\right)\|x-y\|_2^2 \qquad (76) \\
&\leq 4\,\|x-y\|_2^2 , \qquad (77)
\end{aligned}$$

where (76) uses the parallelogram identity and (77) follows since by assumption we have $\|x\|_2 \leq \|x\|_1 = 1$ and $\|y\|_2 \leq \|y\|_1 = 1$. For a matrix $A \in \mathbb{R}^{n\times n}$ the equivalence of the Frobenius and the trace norm [23], i.e., $\|A\|_F \leq \|A\|_{\mathrm{tr}} \leq \sqrt{n}\,\|A\|_F$ and the equivalence for vector norms, i.e., $\|x\|_2 \leq \|x\|_1 \leq \sqrt{n}\,\|x\|_2$ for $x \in \mathbb{R}^n$ finally proves the assertion. ∎

Claim F.3. *Let $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H})$ with $m = \dim \mathcal{H}$ and $c := \min_{i\in\{1,2\}} \min \operatorname{spec} \rho_i > 0$. Then $|H(\rho_1) - H(\rho_2)| \leq L_m \|\rho_1 - \rho_2\|_{\mathrm{tr}}$ with $L_m := \sqrt{m}(\log(\frac{1}{ce}) \vee \mathrm{e}))$.*

Proof: Consider the function $(0,1] \ni x \mapsto f(x) = -x\log x \in \mathbb{R}_{\geq 0}$. Note that $\frac{\partial f}{\partial x} = \log(\frac{1}{xe})$. As $f(\cdot)$ is a concave function we have for all $1 \geq x_1 \geq x_2 > 0$, $f(x_1) - f(x_2) \leq \frac{\partial f}{\partial x}(x_1)(x_2 - x_1)$. Thus it follows that

$|f(x_1)-f(x_2)| \leq \max_{i\in\{1,2\}} |\frac{\partial f}{\partial x}(x_i)||x_1-x_2|$ for all $x_1, x_2 \in (0,1]$, which then implies that for all $x_1, x_2 \in (0,1]$ and $c \in (0,1)$

$$|f(x_1) - f(x_2)| \leq \left(\log(\tfrac{1}{ce}) \vee \log(e)\right) |x_1 - x_2|. \tag{78}$$

For $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H})$, let $\operatorname{spec}(\rho_1) = \{\lambda_1^{(1)}, \lambda_1^{(2)}, \ldots, \lambda_1^{(m)}\}$ and $\operatorname{spec}(\rho_2) = \{\lambda_2^{(1)}, \lambda_2^{(2)}, \ldots, \lambda_2^{(m)}\}$. Using the triangle inequality then gives

$$\begin{aligned}
|H(\rho_1) - H(\rho_2)| &= \left|\sum_{i=1}^{m} -\lambda_1^{(i)} \log(\lambda_1^{(i)}) + \lambda_2^{(i)} \log(\lambda_2^{(i)})\right| \\
&\leq \sum_{i=1}^{m} \left|-\lambda_1^{(i)} \log(\lambda_1^{(i)}) + \lambda_2^{(i)} \log(\lambda_2^{(i)})\right| \\
&= \sum_{i=1}^{m} \left|f(\lambda_1^{(i)}) - f(\lambda_2^{(i)})\right| \\
&\leq \left(\log\left(\frac{1}{ce}\right) \vee \log(\mathrm{e})\right) \sum_{i=1}^{m} \left|\lambda_1^{(i)} - \lambda_2^{(i)}\right| && (79) \\
&\leq \left(\log\left(\frac{1}{ce} \vee e\right)\right) \sqrt{m} \left(\sum_{i=1}^{m} \left|\lambda_1^{(i)} - \lambda_2^{(i)}\right|^2\right)^{1/2} && (80) \\
&\leq \left(\log\left(\frac{1}{ce} \vee \mathrm{e}\right)\right) \sqrt{m} \left\|\rho_1 - \rho_2\right\|_F && (81) \\
&\leq \left(\log\left(\frac{1}{ce} \vee \mathrm{e}\right)\right) \sqrt{m} \left\|\rho_1 - \rho_2\right\|_{\mathrm{tr}}, && (82)
\end{aligned}$$

where (79) follows by assumption together with (78). Inequality (80) uses the equivalence of the one and two vector norm and that the logarithm is monotonic. Inequality (81) uses the Hoffman-Wielandt inequality [53, p. 56]. Finally, (82) follows from the equivalence of the Frobenius and the trace norm. ■

For $x_1, x_2 \in R$, the triangle inequality gives

$$\begin{aligned}
|f_{\lambda,M}(x_1) - f_{\lambda,M}(x_2)| &= |\operatorname{tr}\left[\Phi(\mathsf{E}(x_1))\lambda\right] - H(\Phi(\mathsf{E}(x_1))) - \operatorname{tr}\left[\Phi(\mathsf{E}(x_2))\lambda\right] + H(\Phi(\mathsf{E}(x_2)))| \\
&\leq \left|\left\langle \Phi(\mathsf{E}(x_1)), \lambda\right\rangle_F - \left\langle \Phi(\mathsf{E}(x_2)), \lambda\right\rangle_F\right| + |H(\Phi(\mathsf{E}(x_1))) - H(\Phi(\mathsf{E}(x_2)))|. && (83)
\end{aligned}$$

Using Cauchy-Schwarz and the linearity of quantum channels we can bound the first part of (83) as

$$\begin{aligned}
\left|\left\langle \Phi(\mathsf{E}(x_1)), \lambda\right\rangle - \left\langle \Phi(\mathsf{E}(x_2)), \lambda\right\rangle_F\right| &= \left|\left\langle \Phi(\mathsf{E}(x_1) - \mathsf{E}(x_2)), \lambda\right\rangle_F\right| \\
&\leq \left\|\Phi(\mathsf{E}(x_1) - \mathsf{E}(x_2))\right\|_F \left\|\lambda\right\|_F \\
&\leq \left\|\Phi(\mathsf{E}(x_1) - \mathsf{E}(x_2))\right\|_{\mathrm{tr}} \left\|\lambda\right\|_F && (84) \\
&\leq \left\|\mathsf{E}(x_1) - \mathsf{E}(x_2)\right\|_{\mathrm{tr}} \left\|\lambda\right\|_F && (85) \\
&\leq 2N\sqrt{N} \left\|x_1 - x_2\right\|_1 \left\|\lambda\right\|_F, && (86)
\end{aligned}$$

where (84) uses the equivalence of the Frobenius and the trace norm [23] and inequality (85) is a direct consequence of the contractivity property under the trace norm of quantum channels [54, Thm. 8.16]. Inequality (86) follows from Claims F.1 and F.2.

Recall that $\|\lambda\|_F \leq M \log\left(\gamma_M^{-1} \vee \mathrm{e}\right)$ as by definition $\lambda \in \Lambda$.

With the help of Claim F.3 and Assumption 5.2 we can also bound the second part of (83). Let $J_M := \sqrt{M}(\log(\frac{1}{\gamma_M \mathrm{e}} \vee \mathrm{e}))$ we then have

$$\begin{aligned} |H(\Phi(\mathsf{E}(x_1))) - H(\Phi(\mathsf{E}(x_2)))| &\leq J_M \left\|\Phi(\mathsf{E}(x_1)) - \Phi(\mathsf{E}(x_2))\right\|_{\mathrm{tr}} \\ &= J_M \left\|\Phi(\mathsf{E}(x_1) - \mathsf{E}(x_2))\right\|_{\mathrm{tr}} \\ &\leq J_M \left\|\mathsf{E}(x_1) - \mathsf{E}(x_2)\right\|_{\mathrm{tr}} \qquad (87) \\ &\leq 2N\sqrt{N} J_M \left\|x_1 - x_2\right\|_1 , \qquad (88) \end{aligned}$$

where (87) again uses the contractivity property under the trace norm of quantum channels [54, Thm. 8.16] and (88) follows from Claims F.1 and F.2. □

APPENDIX G
PROOF OF LEMMA 5.10

Within this proof we use the notation $\rho_x := \Phi(\mathsf{E}(x))$. We define the functions $R \ni x \mapsto f_\lambda(x) := \mathcal{W}\lambda(x) - H(\rho_x) = \mathrm{tr}\left[\rho_x \lambda\right] - H(\rho_x) \in \mathbb{R}$ and $R \ni x \mapsto g_\lambda(x) := f_\lambda(x) - \bar{f}_\lambda \in \mathbb{R}_{\leq 0}$, where $\bar{f}_\lambda := \max_{x \in R} f_\lambda(x) = f_\lambda(x^\star)$. Then, by following Remark 3.14, we have

$$\nabla G_\nu(\lambda) = \frac{1}{\bar{S}(\lambda)} \int_R 2^{\frac{1}{\nu} g_\lambda(x)} (\rho_x^\top - \rho_{x^\star}^\top)\, \mathrm{d}x + \rho_{x^\star}^\top ,$$

where

$$\bar{S}(\lambda) = \int_R 2^{\frac{1}{\nu} g_\lambda(x)}\, \mathrm{d}x$$

and we have used $\frac{\partial \mathrm{tr}[\rho\lambda]}{\partial \lambda_{k,\ell}} = \rho_{\ell,k}$ [23, Prop. 10.7.2]. Consider i.i.d. random variables $\{X_i\}_{i=1}^n$ taking values in R. Define the random variable $\bar{S}_n(\lambda) := \frac{1}{n} \sum_{i=1}^n 2^{\frac{1}{\nu} g_\lambda(X_i)}$. Then, invoking the non-positivity of $g_\lambda(\cdot)$, Mc Diarmid's inequality [55, Thm. 2.2.2] leads to the following concentration bound

$$\mathbb{P}\left[\left|\bar{S}(\lambda) - \bar{S}_n(\lambda)\right| \geq t\right] \leq 2 \exp\left(-2t^2 n\right). \qquad (89)$$

Next, we approximate $T(\lambda) := \int_R 2^{\frac{1}{\nu} g_\lambda(x)} (\rho_x^\top - \rho_{x^\star}^\top)\, \mathrm{d}x$. Consider i.i.d. random variables $\{X_i\}_{i=1}^n$ taking values in R and define a function $R^n \ni x \mapsto f(x_1, \ldots, x_n) := \frac{1}{n} \sum_{i=1}^n 2^{\frac{1}{\nu} g_\lambda(x_i)} (\rho_{x_i}^\top - \rho_{x^\star}^\top) \in \mathrm{H}^M$.

Claim G.1. *The function f satisfies the bounded difference assumption*

$$\sup_{x_1, \ldots, x_n, x_i'} \left(f(x_1, \ldots, x_i, \ldots, x_n) - f(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_n)\right)^2 \preccurlyeq \mathsf{diag}(\tfrac{3}{n}, \ldots, \tfrac{3}{n})^2 \text{ for all } i = 1, \ldots, n.$$

Proof:

$$\begin{aligned} &f(x_1, \ldots, x_i, \ldots, x_n) - f(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_n) \\ &= \frac{1}{n} \left(2^{\frac{1}{\nu} g_\lambda(x_i)} (\rho_{x_i}^\top - \rho_{x^\star}^\top) - 2^{\frac{1}{\nu} g_\lambda(x_i')} (\rho_{x_i'}^\top - \rho_{x^\star}^\top)\right) \\ &= \frac{1}{n} \rho_{x^\star}^\top \left(2^{\frac{1}{\nu} g_\lambda(x_i')} - 2^{\frac{1}{\nu} g_\lambda(x_i)}\right) + \frac{1}{n} \left(2^{\frac{1}{\nu} g_\lambda(x_i)} \rho_{x_i}^\top - 2^{\frac{1}{\nu} g_\lambda(x_i')} \rho_{x_i'}^\top\right) \end{aligned}$$

$$= \frac{1}{n}\left(\rho_{x^\star}^\top (b_{x_i'} - b_{x_i}) + b_{x_i}\rho_{x_i}^\top - b_{x_i'}\rho_{x_i'}^\top\right) =: (\star),$$

where $b_y := 2^{\frac{1}{\nu}g_\lambda(y)}$. Now,

$$\begin{aligned}
\lambda_{\max}\left((\star)^2\right) &= \left\|(\star)^2\right\|_{\mathrm{op}} \\
&\le \left(\left|\frac{b_{x_i}}{n} - \frac{b_{x_i'}}{n}\right| \left\|\rho_{x^\star}^\top\right\|_{\mathrm{op}} + \left\|\frac{b_{x_i'}}{n}\rho_{x_i'}^\top - \frac{b_{x_i}}{n}\rho_{x_i}^\top\right\|_{\mathrm{op}}\right)^2 && (90)\\
&\le \left(\frac{1}{n}\left|b_{x_i} - b_{x_i'}\right| \left\|\rho_{x^\star}\right\|_{\mathrm{op}} + \frac{1}{n}\left|b_{x_i'}\right| \left\|\rho_{x_i'}\right\|_{\mathrm{op}} + \frac{1}{n}\left|b_{x_i}\right| \left\|\rho_{x_i}\right\|_{\mathrm{op}}\right)^2 && (91)\\
&\le \frac{9}{n^2}, && (92)
\end{aligned}$$

where (90) follows from $\left\|(B-C)^2\right\|_{\mathrm{op}} = \left\|B^2 - BC - CB - C^2\right\|_{\mathrm{op}} \le \left\|B^2\right\|_{\mathrm{op}} + \|BC\|_{\mathrm{op}} + \|CB\|_{\mathrm{op}} + \left\|C^2\right\|_{\mathrm{op}} \le \|B\|_{\mathrm{op}}^2 + 2\|B\|_{\mathrm{op}}\|C\|_{\mathrm{op}} + \|C\|_{\mathrm{op}}^2 = (\|B\|_{\mathrm{op}} + \|C\|_{\mathrm{op}})^2$ which uses the submultiplicative property of the operator norm. Equation (91) is due to the triangle inequality and (92) uses the non-positivity of the function g_λ and the property of density operators. ■

Define the random variable $T_n(\lambda) := \frac{1}{n}\sum_{i=1}^n 2^{\frac{1}{\nu}g_\lambda(X_i)}(\rho_{X_i}^\top - \rho_{x^\star}^\top)$

Claim G.2. $\mathbb{P}\left[\left\|T_n(\lambda) - T(\lambda)\right\|_{\mathrm{op}} \ge t\right] \le M\exp\left(\frac{-t^2 n}{72}\right)$

Proof: By the matrix McDiarmid inequality [18, Cor. 7.5], we get the concentration bound

$$\mathbb{P}[\lambda_{\max}(T_n(\lambda) - T(\lambda)) \ge t] \le M\exp\left(\frac{-t^2 n}{72}\right).$$

Furthermore, as pointed out in [18, Rmk. 3.10], $\lambda_{\min}(X) = -\lambda_{\max}(-X)$. As such following similar lines as above one can derive

$$\mathbb{P}[\lambda_{\min}(T_n(\lambda) - T(\lambda)) \le -t] \le M\exp\left(\frac{-t^2 n}{72}\right).$$

■

Claim G.3. *Let $A, B \in \mathbb{R}$, $\xi_1, \xi_2 \ge 0$, $B > \xi_2$, $\hat{A} \in [A-\xi_1, A+\xi_1]$ and $\hat{B} \in [B-\xi_2, B+\xi_2]$. Then for $Z := \frac{A}{B}$ and $\hat{Z} := \frac{\hat{A}}{\hat{B}}$ we have*

$$\left|Z - \hat{Z}\right| \le \max\left\{\frac{A}{B} - \frac{A-\xi_1}{B+\xi_2}, \frac{A+\xi_1}{B-\xi_2} - \frac{A}{B}\right\}.$$

Proof: Define

$$\hat{Z}_{\min} := \frac{A-\xi_1}{B+\xi_2} \quad \text{and} \quad \hat{Z}_{\max} := \frac{A+\xi_1}{B-\xi_2}$$

such that $\hat{Z}_{\min} \le \hat{Z} \le \hat{Z}_{\max}$. The inequality $|Z - \hat{Z}| \le \max\{Z - \hat{Z}_{\min}, \hat{Z}_{\max} - Z\}$ finally proves the assertion. ■

According to Claim G.3, Equation (89) together with Claim G.2 give

$$\mathbb{P}\left[\left\|\nabla G(\lambda) - \nabla\tilde{G}(\lambda)\right\|_{\mathrm{op}} \ge \varphi(t)\right] \le M\exp\left(\frac{-t^2 n}{72}\right), \tag{93}$$

where $\varphi(t) := \max\left\{\frac{(\|T(\lambda)\|_{\mathrm{op}} + \bar{S}(\lambda))t}{\bar{S}(\lambda)(\bar{S}(\lambda) - t)}, \frac{(\|T(\lambda)\|_{\mathrm{op}} + \bar{S}(\lambda))t}{\bar{S}(\lambda)(\bar{S}(\lambda) + t)}\right\}$. We next show that $\bar{S}(\lambda)$ is uniformly away from zero and restrict values of t to an interval such that φ well defined. Recall that $x^\star \in R$ is such that $g_\lambda(x^\star) = 0$. Therefore

$$\bar{S}(\lambda) = \int_R 2^{\frac{1}{\nu}g_\lambda(x)}\,\mathrm{d}x \ge \int_{\mathsf{B}_\varepsilon(x^\star)\cap R} 2^{\frac{1}{\nu}g_\lambda(x)}\,\mathrm{d}x \ge \int_{\mathsf{B}_\varepsilon(x^\star)\cap R} 2^{\frac{-\sqrt{N}L_{N,M}\varepsilon}{\nu}}\,\mathrm{d}x \ge 2^{\frac{-\sqrt{N}L_{N,M}\varepsilon}{\nu}}\varepsilon^N, \tag{94}$$

where we have used the Lipschitz continuity of g_λ given by Lemma 5.6 with respect to the ℓ_∞-norm and considered the ball $\mathsf{B}_\varepsilon(x^\star)$, centered at $x^\star$ with radius ε with respect to the ℓ_∞-norm. By choosing $\varepsilon = 1$, one gets

$$\bar{S}(\lambda) \geq 2^{\frac{-\sqrt{N}L_{N,M}}{\nu}},$$

which is strictly away from zero for any finite N. Moreover, the inequality (93) holds for all $t \in (0, 2^{\frac{-\sqrt{N}L_{N,M}}{\nu}})$.

Claim G.4. *For* $t \in [0, \frac{\bar{S}(\lambda)}{2}]$ *and* $\min_{\lambda\in\Lambda} \frac{\bar{S}(\lambda)^4}{576} \geq \frac{1}{576} 2^{\frac{-4\sqrt{N}L_{N,M}}{\nu}} =: K_{N,M}$

$$\mathbb{P}\left[\left\|\nabla G(\lambda) - \nabla\tilde{G}(\lambda)\right\|_{\mathrm{op}} \geq t\right] \leq M \exp\left(-K_{N,M} t^2 n\right),$$

Proof: Define $\alpha_\varepsilon := \frac{\|T(\lambda)\|_{\mathrm{op}}+\bar{S}(\lambda)}{\bar{S}(\lambda)(\bar{S}(\lambda)-\varepsilon)}$ and $\beta_\varepsilon := \frac{\|T(\lambda)\|_{\mathrm{op}}+\bar{S}(\lambda)}{\bar{S}(\lambda)(\bar{S}(\lambda)+\varepsilon)}$. It can be seen that $\alpha_\varepsilon \geq \beta_\varepsilon$ for any $\varepsilon \in [0, \bar{S}(\lambda))$ and as such

$$\varphi(t) \leq \alpha_\varepsilon t = \frac{2(\|T(\lambda)\|_{\mathrm{op}}+\bar{S}(\lambda))}{\bar{S}(\lambda)^2} t =: \alpha t \quad \text{for all } t \in [0, \varepsilon], \tag{95}$$

where we have chosen $\varepsilon = \frac{\bar{S}(\lambda)}{2}$. By (93) this gives

$$\mathbb{P}\left[\left\|\nabla G(\lambda) - \nabla\tilde{G}(\lambda)\right\|_{\mathrm{op}} \geq \alpha t\right] \leq M \exp\left(\frac{-t^2 n}{72}\right),$$

which shows that $K_{N,M} \geq \frac{\bar{S}(\lambda)^4}{288(\|T(\lambda)\|_{\mathrm{op}}+\bar{S}(\lambda))^2}$. Using $\|T(\lambda)\|_{\mathrm{op}} \leq 1$ and $\bar{S}(\lambda) \leq 1$ completes the proof. ■

□

APPENDIX H
PROOF OF COROLLARY 5.11

This proof uses the same notation as the proof of Theorem 5.4. For a fixed accuracy $\varepsilon > 0$, Remark 5.9 implies that without loss of generality we can assume that $\log(\frac{1}{\gamma_M}) = \log(M \log M) =: \mathrm{p}(M)$. Recall that as explained in the proof of Theorem 5.4 the smoothing parameter ν is chosen as $\nu \leq \frac{\varepsilon}{3\beta(\alpha+\log(3\beta\varepsilon^{-1}))}$ for $\beta := 1 + \frac{\log \mathrm{e}}{\mathrm{e}}$ and $\alpha := \log(L_{N,M}) + (2N-2)\log(2\pi) + 1$. It can be verified immediately that $\nu^{-1} = \Omega(N + \log(N^{3/2} M \mathrm{p}(M)))$. Let $\delta = O(\frac{1}{M\mathrm{p}(M)} 2^{c\frac{\sqrt{N}}{\nu}L_{N,M}})$ for some constant $c > 0$. According to Lemma 5.10, to ensure that $\eta^{-1} = \Omega(M^2 \mathrm{p}(M)^2 (N + \log(M\mathrm{p}(M))))$ we have to choose the number of samples as

$$n = O\left(M^2 \mathrm{p}(M)^2 2^{c'\frac{\sqrt{N}}{\nu}L_{N,M}}\right) = O\left(M^2 \mathrm{p}(M)^2 2^{c'(N^{3/2}+N^{1/2}\log(N^{3/2}M\mathrm{p}(M)))L_{N,M}}\right), \tag{96}$$

for some constant $c' > 0$. Note that the complexity to generate n i.i.d. uniformly distributed samples $\{X_i\}_{i=1}^n$ is $O(n)$. The total complexity to ensure an ε-close solution is then $k\, M^2 n$ with k being the number of iterations that is given in (49). Recalling that $\mathrm{p}(M) := \log(M \log M)$ then proves the assertion. □

ACKNOWLEDGMENTS

We would like to thank Omar Fawzi, Norbert Lütkenhaus, John Lygeros, Stefan Richter, and Marco Tomamichel for helpful discussions and pointers to references. We also thank Aram Harrow and Ashley Montanaro for sharing with us their vision and discernment on [13].

REFERENCES

[1] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948. [Online]. Available: http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[2] M. Wilde, *Quantum Information Theory*. Cambridge University Press, June 2013.

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

[4] ——, "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 269–273, 1998.

[5] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A*, vol. 56, pp. 131–138, Jul 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.56.131

[6] R. E. Blahut, "Computation of channel capacity and rate-distortion functions," *IEEE Transactions on Information Theory*, vol. 18, no. 4, pp. 460–473, 1972.

[7] S. Arimoto, "An algorithm for computing the capacity of arbitrary discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 14–20, 1972.

[8] G. Matz and P. Duhamel, "Information geometric formulation and interpretation of accelerated Blahut-Arimoto-type algorithms," *Proceedings Information Theory Workshop (ITW)*, pp. 66–70, 2004.

[9] H. Nagaoka, "Algorithms of Arimoto-Blahut type for computing quantum channel capacity," *Proceedings IEEE International Symposium on Information Theory (ISIT)*, pp. 354–, Aug 1998.

[10] H. Nagaoka and S. Osawa, "Algorithms of Arimoto-Blahut type for computing quantum channel capacity," *Proceedings of the second QIT*, p. 107112, 1999.

[11] M. B. Hastings, "Superadditivity of communication capacity using entangled inputs," *Nature Physics*, vol. 5, no. 4, pp. 255–257, 2009.

[12] S. Beigi and P. Shor, "On the complexity of computing zero-error and holevo capacity of quantum channels," 2008, available at arXiv:0709.2090.

[13] A. W. Harrow and A. Montanaro, "Testing product states, quantum Merlin-Arthur games and tensor optimization," *J. ACM*, vol. 60, no. 1, pp. 3:1–3:43, February 2013. [Online]. Available: http://doi.acm.org/10.1145/2432622.2432625

[14] P. W. Shor, "Capacities of quantum channels and how to find them," *Mathematical Programming*, vol. 97, no. 1-2, pp. 311–335, 2003. [Online]. Available: http://dx.doi.org/10.1007/s10107-003-0446-y

[15] S. Osawa and H. Nagaoka, "Numerical experiments on the capacity of quantum channel with entangled input states," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E84, no. 10, pp. 2583–2590, October 2001, available at arXiv:ph/0007115v4.

[16] M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai, and T. Shimono, "Qubit channels which require four inputs to achieve capacity: Implications for additivity conjectures," *Quantum Information and Computation*, vol. 5, no. 1, pp. 13–31, January 2005. [Online]. Available: http://dl.acm.org/citation.cfm?id=2011608.2011610

[17] Y. Nesterov, "Smooth minimization of non-smooth functions," *Mathematical Programming*, vol. 103, no. 1, pp. 127–152, 2005. [Online]. Available: http://dx.doi.org/10.1007/s10107-004-0552-5

[18] J. A. Tropp, "User-friendly tail bounds for sums of random matrices," *Foundations of Computational Mathematics*, vol. 12, no. 4, pp. 389–434, 2012. [Online]. Available: http://dx.doi.org/10.1007/s10208-011-9099-z

[19] S. Boucheron, G. Lugosi, and P. Massart, *Concentration inequalities*. Oxford University Press, Oxford, 2013, a nonasymptotic theory of independence.

[20] T. Sutter, D. Sutter, P. M. Esfahani, and J. Lygeros, "Efficient approximation of channel capacities," *IEEE Transactions on Information Theory*, vol. 61, no. 4, pp. 1649–1666, April 2015.

[21] E. T. Jaynes, "Information theory and statistical mechanics. ii," *Physical Review*, vol. 108, pp. 171–190, Oct 1957. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRev.108.171

[22] D. P. Bertsekas, *Convex Optimization Theory*, ser. Athena Scientific optimization and computation series. Athena Scientific, 2009.

[23] D. S. Bernstein, *Matrix Mathematics*, 2nd ed. Princeton University Press, 2009.

[24] M. Ohya, D. Petz, and N. Watanabe, "On capacities of quantum channels," *Probability and Mathematical Statistics*, vol. 17, pp. 179 – 196, 1997.

[25] B. Schumacher and M. D. Westmoreland, "Optimal signal ensembles," *Phys. Rev. A*, vol. 63, p. 022308, Jan 2001. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.63.022308

[26] M. Tomamichel and V. Y. Tan, "Second-order asymptotics for the classical capacity of image-additive quantum channels," *Communications in Mathematical Physics*, vol. 338, no. 1, pp. 103–137, 2015. [Online]. Available: http://dx.doi.org/10.1007/s00220-015-2382-0

[27] S. Kakade, S. Shalev-Shwartz, and A. Tewari, "On the duality of strong convexity and strong smoothness: Learning applications and matrix regularization," Tech. Rep., 2009. [Online]. Available: http://www.cs.huji.ac.il/~shais/papers/KakadeShalevTewari09.pdf

[28] M. Fannes, "A continuity property of the entropy density for spin lattice systems," *Communications in Mathematical Physics*, vol. 31, no. 4, pp. 291–294, 1973. [Online]. Available: http://dx.doi.org/10.1007/BF01646490

[29] K. M. R. Audenaert, "A sharp continuity estimate for the von neumann entropy," *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 28, p. 8127, 2007. [Online]. Available: http://stacks.iop.org/1751-8121/40/i=28/a=S18

[30] R. Alicki and M. Fannes, "Continuity of quantum conditional information," *Journal of Physics A: Mathematical and General*, vol. 37, no. 5, pp. L55–L57, 2004-02-06T00:00:00. [Online]. Available: http://www.ingentaconnect.com/content/iop/jphysa/2004/00000037/00000005/art00l01

[31] Y. Nesterov, *Introductory Lectures on Convex Optimization: A Basic Course*, ser. Applied Optimization. Springer, 2004.

[32] J. B. Lasserre, *Moments, Positive Polynomials and Their Applications*, ser. Imperial College Press optimization series. Imperial College Press, 2009.

[33] S. Richter, "Computational complexity certification of gradient methods for real-time model predictive control," *PhD thesis, ETH Zurich*, 2012, available at http://dx.doi.org/10.3929/ethz-a-007587480.

[34] L. N. Trefethen and D. Bau, *Numerical Linear Algebra*. Siam, 1997.

[35] D. H. Fremlin, *Measure theory. Vol. 2*. Torres Fremlin, Colchester, 2010, broad foundations, Second edition January 2010.

[36] E. J. Anderson and P. Nash, *Linear programming in infinite-dimensional spaces: theory and applications*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley, 1987.

[37] S. K. Mitter, "Convex optimization in infinite dimensional spaces," in *Recent advances in learning and control*, ser. Lecture Notes in Control and Inform. Sci. Springer, London, 2008, vol. 371, pp. 161–179. [Online]. Available: http://dx.doi.org/10.1007/978-1-84800-155-8_12

[38] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley Interscience, 2006.

[39] O. Devolder, F. Glineur, and Y. Nesterov, "Double smoothing technique for large-scale linearly constrained convex optimization," *SIAM Journal on Optimization*, vol. 22, no. 2, pp. 702–727, 2012.

[40] ——, "First-order methods of smooth convex optimization with inexact oracle," *Mathematical Programming*, pp. 1–39, 2013. [Online]. Available: http://dx.doi.org/10.1007/s10107-013-0677-5

[41] D. Leung and G. Smith, "Continuity of quantum channel capacities," *Communications in Mathematical Physics*, vol. 292, no. 1, pp. 201–215, 2009. [Online]. Available: http://dx.doi.org/10.1007/s00220-009-0833-1

[42] C. Robert and G. Casella, *Monte Carlo Statistical Methods*, ser. Springer Texts in Statistics. Springer, 2004.

[43] L. Lovász and S. Vempala, "The geometry of logconcave functions and sampling algorithms," *Random Struct. Algorithms*, vol. 30, no. 3, pp. 307–358, May 2007. [Online]. Available: http://dx.doi.org/10.1002/rsa.v30:3

[44] C. King, "Additivity for unital qubit channels," *Journal of Mathematical Physics*, vol. 43, no. 10, pp. 4641–4653, 2002. [Online]. Available: http://scitation.aip.org/content/aip/journal/jmp/43/10/10.1063/1.1500791

[45] K. Brádler, E. Castro-Ruiz, and E. Nahmad-Achar, "Quantum and classical capacity boosted by a Lorentz transformation," *Phys. Rev. A*, vol. 90, p. 022308, Aug 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.90.022308

[46] K. Zyczkowski, K. A. Penson, I. Nechita, and B. Collins, "Generating random density matrices," *Journal of Mathematical Physics*, vol. 52, no. 6, pp. –, 2011. [Online]. Available: http://scitation.aip.org/content/aip/journal/jmp/52/6/10.1063/1.3595693

[47] M. Baes and M. Bürgisser, "An acceleration procedure for optimal first-order methods," *Optimization Methods and Software*, vol. 29, no. 3, pp. 610–628, 2014. [Online]. Available: http://dx.doi.org/10.1080/10556788.2013.835812

[48] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, 1996. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.54.3824

[49] H. Barnum, "Quantum rate-distortion coding," *Phys. Rev. A*, vol. 62, p. 042309, Sep 2000. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.62.042309

[50] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, no. 4, pp. 318–336, 2004. [Online]. Available: http://dx.doi.org/10.1007/s11122-005-0002-x

[51] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, 2005. [Online]. Available: http://dx.doi.org/10.1109/TIT.2004.839515

[52] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge: Cambridge University Press, 2004, sixth printing with corrections, 2008.

[53] T. Tao, *Topics in Random Matrix Theory*. Graduate Studies in Mathematics, 2012, vol. 132.

[54] M. Wolf, *Quantum Channels & Operations*, 2012, available at http://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf.

[55] M. Raginsky and I. Sason, "Concentration of measure inequalities in information theory, communications, and coding," *Foundations and Trends in Communications and Information Theory*, vol. 10, no. 1-2, pp. 1–246, 2013.