Louisiana State University

LSU Digital Commons

Faculty Publications

Department of Physics & Astronomy

1-1-2019

Quantum channel capacities per unit cost

Dawei Ding
Stanford University

Dmitri S. Pavlichin
Stanford University

Mark M. Wilde
Louisiana State University

Follow this and additional works at: https://digitalcommons.lsu.edu/physics_astronomy_pubs

Recommended Citation
Ding, D., Pavlichin, D., & Wilde, M. (2019). Quantum channel capacities per unit cost. *IEEE Transactions on Information Theory, 65* (1), 418-435. https://doi.org/10.1109/TIT.2018.2854747

This Article is brought to you for free and open access by the Department of Physics & Astronomy at LSU Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of LSU Digital Commons. For more information, please contact ir@lsu.edu.

Quantum Channel Capacities per Unit Cost

Dawei Ding, Dmitri S. Pavlichin, and Mark M. Wilde, *Senior Member, IEEE*

***Abstract*— Communication over a noisy channel is often conducted in a setting in which different input symbols to the channel incur a certain cost. For example, for bosonic quantum channels, the cost associated with an input state is the number of photons, which is proportional to the energy consumed. In such a setting, it is often useful to know the maximum amount of information that can be reliably transmitted per cost incurred. This is known as the capacity per unit cost. In this paper, we generalize the capacity per unit cost to various communication tasks involving a quantum channel, such as classical communication, entanglement-assisted classical communication, private communication, and quantum communication. For each task, we define the corresponding capacity per unit cost and derive a formula for it analogous to that of the usual capacity. Furthermore, for the special and natural cases in which there is a zero-cost state, we obtain expressions in terms of an optimized relative entropy involving the zero-cost state. For each communication task, we construct an explicit pulse-position-modulation coding scheme that achieves the capacity per unit cost. Finally, we compute capacities per unit cost for various bosonic Gaussian channels and introduce the notion of a blocklength constraint as a proposed solution to the long-standing issue of infinite capacities per unit cost. This motivates the idea of a blocklength-cost duality on which we elaborate in depth.**

***Index Terms*— Capacity per unit cost, bosonic Gaussian channels, quantum communication, blocklength-cost duality.**

I. Introduction

THE main concerns of information theory are determining limitations on information processing and how to attain them [1]. In the task of communication over a noisy channel, for example, the usual goal is to compute the capacity of the channel, which is informally defined as the maximum number of bits that can be reliably transmitted over the channel divided by the total number of channel uses. As the number of channel uses is often directly proportional to the overall transmission time, the capacity measures the maximum rate of information transmission per unit time. Hence, the capacity is a limit to communication when given a certain *time constraint*.

Manuscript received June 12, 2017; revised April 13, 2018; accepted June 28, 2018. Date of publication July 10, 2018; date of current version December 19, 2018. D. Ding was supported by the Stanford Graduate Fellowship Program. D. S. Pavlichin was supported by the Army Research Office under Grant W911NF-16-1-0086. M. M. Wilde was supported in part by the U.S. National Science Foundation and in part by the Office of Naval Research.

D. Ding is with the Stanford Institute for Theoretical Physics, Stanford University, Stanford, CA 94305 USA (e-mail: dding@stanford.edu).

D. S. Pavlichin is with the Department of Applied Physics, Stanford University, Stanford, CA 94305 USA.

M. M. Wilde is with the Hearne Institute for Theoretical Physics, the Department of Physics and Astronomy, and the Center for Computation and Technology, Louisiana State University, Baton Rouge, LA 70803 USA.

Communicated by S. Watanabe, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2018.2854747

However, we need not restrict ourselves to time constraints. We can seek limits to communication with respect to other types of constraints, and in some practical settings these other constraints are more relevant. For example, we can imagine a setting in which a satellite deep in space is transmitting information back to Earth [2]. In this case, the amount of time taken to transmit the information is not as much of a concern as is the finite amount of battery energy. Given the time and money taken to get the satellite deep into space, the receivers on Earth can afford to wait; but once the batteries are consumed, the satellite is no longer useful in the absence of an external energy source, as is often the case when deep in space. Hence, in this case, what is relevant here is an *energy constraint*. This would also be relevant for deep sea communication, or in general, communication with a remote probe in a location difficult to reach. These were classic motivating examples for studying cost constraints in classical information theory, but they also naturally motivate studying cost constraints in quantum information theory. For instance, if the satellite is transmitting quantum information, a recently realized technology [3], [4], we would like to develop theory for optimizing information transmission with respect to that cost.

In general, we would like to consider constraints with respect to a certain *cost* associated with transmission. In classical information theory, communication limits with respect to costs other than time were first considered in [5]–[9]. Such ideas have appeared in quantum settings as well, most notably for quantum bosonic channels [10]–[13] where the relevant cost is the photon number. Now, just as the communication limit to a time constraint is the capacity, the corresponding communication limit to a general cost constraint should, informally, be the maximum amount of information that can be reliably transmitted divided by the total cost incurred in transmission. This is the *capacity per unit cost*, which was introduced and extensively studied for classical channels in [14]. After the development of quantum information theory, capacity per unit cost was extended to channels with classical binary inputs and quantum outputs [15].

Capacity per unit cost is relevant in many different settings, primarily when one is concerned with constraints other than time, as in the satellite setting mentioned above. However, it is also relevant even when one is still concerned with a time constraint. This is when *input states have different time durations*. This was pointed out in [5] and [6]. Indeed, the notion of cost is very general and can appear in many different settings — it can even be relevant for questions in quantum gravity. For instance, we could give a limit to the amount of quantum information transmitted via Hawking

0018-9448 © 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

radiation emitted from a black hole using bounds on the mass-energy of the black hole. This would involve quantum channel capacity per unit cost, with mass-energy as the relevant cost.

In this paper, we generalize the capacity per unit cost to various communication tasks involving quantum channels, including classical communication, entanglement-assisted classical communication, private communication, and quantum communication. To do so, we first recall from classical information theory where cost was quantified with a *cost function*, used in [14], which associates to each input symbol a non-negative real number. In the quantum case, we employ a *cost observable* $G \geq 0$, considered for cost-constrained capacities in [16] and [17], in order to quantify the cost of transmitting a quantum state. Hence, any cost that can be described by a positive semidefinite observable can be considered in our framework. As mentioned above, we could consider channel uses, energy, photon number, or even a linear combination of these if that is what one is interested in, as is often the case with many practical optimization problems. The cost observable is a very natural generalization of the cost function, as it preserves two key properties. One is positive semidefiniteness, which we enforce by requiring $G \geq 0$. Another is additivity across channel uses. This was implicit in the definition of the classical cost function, that the total cost incurred across multiple channel uses is the sum of the costs incurred in individual channel uses. We can enforce this by defining the cost observable for an input state to n channel uses to be

$$G_n \equiv \sum_{j=1}^{n} I^{\otimes j-1} \otimes G \otimes I^{\otimes n-j}. \tag{1}$$

By inspection, the total cost will be additive across the channel uses. Note that the classical cost function can be embedded into a cost observable by letting the spectrum of the latter be the image of the former.

Using this prescription, we can then generalize the results in [14] to classical communication over quantum channels by giving a formula for the capacity per unit cost of the form

$$\sup_{\{p_X, \rho_A(x)\}} \frac{I(X;B)_\rho}{\mathrm{tr}[G\bar{\rho}_A]}, \tag{2}$$

where A, B denote quantum systems, $\bar{\rho}_A \equiv \sum_x p_X(x)\rho_A(x)$, and the mutual information $I(X;B)$ is evaluated with respect to a classical–quantum state ρ_{XB} associated with the channel. For simplicity, we focus on channels with a single-letter cost-constrained classical capacity, including entanglement-breaking channels for example [18]–[20], but the developments easily generalize beyond this case and we discuss this point later on. The formula in eq. (2) is derived via the known formula [17] for the cost-constrained classical capacity, also known as the classical capacity cost function, of a quantum channel. This is the capacity with an average cost constraint over all the channel uses. Hence, the ratio of the cost-constrained capacity to the average cost constraint is achievable as a capacity per unit cost. Conversely, this is the highest possible rate per unit cost since any higher rate would imply that we could achieve a higher rate per channel use than the cost-constrained capacity. We can then write the cost-constrained capacity as an optimized mutual information, and thus eq. (2) follows. Note that the formula reduces to the regular capacity when G is the identity operator. This is intuitive since in this case the cost is the number of channel uses, and so every quantum state incurs unit cost.

Now, more interesting results come about in the special case in which there is a zero-cost quantum state, that is, some state ψ^0 such that $\mathrm{tr}[G\psi^0] = 0$. This is a natural setting to consider, given that transmitting a zero-cost state often physically corresponds to not actively sending anything through the channel. For example, for a bosonic channel, the zero-cost state is the vacuum. Now, by the positive semi-definiteness of G, without loss of generality we can take ψ^0 to be pure. In this case, we find that the capacity per unit cost reduces to the following expression:

$$\sup_{\psi \neq \psi^0} \frac{D(\mathcal{N}(\psi) \| \mathcal{N}(\psi^0))}{\langle \psi | G | \psi \rangle}, \tag{3}$$

where D denotes the quantum relative entropy [21] and the supremum is with respect to pure states ψ. The above expression is intuitive given the fact that pulse-position-modulation (PPM) protocols achieve the capacity per unit cost when there is a zero-cost state [14]. Such PPM protocols encode information into the position of a ψ-pulse amidst a baseline of zero-cost ψ^0 states. Hence, for these protocols, we expect the relevant variables for computing the capacity per unit cost to be the distinguishability of the states $\mathcal{N}(\psi)$ and $\mathcal{N}(\psi^0)$ in addition to the cost of ψ. We then extend these results to various other communication tasks over a quantum channel, such as entanglement-assisted, private, or quantum communication. See Sections IV, V, and VI for details. We apply these formulas to various quantum Gaussian channels in section VII. In section VIII we introduce the notion of a blocklength-constrained capacity per unit cost, analogous to that of a cost-constrained capacity, and we derive a formula for it. We find that a blocklength constraint can ensure that the capacity per unit cost is finite and thus can play a similar role to a cost constraint for the usual capacity. This motivates the notion of a *blocklength-cost duality*, which we develop with various examples and concepts.

Related Work

After deriving many of the results in this paper and while drafting this manuscript, a related work appeared on the quant-ph arXiv [22]. In [22], Jarzyna considers classical capacity per unit cost for particular channels that accept a general classical input symbol and output a quantum state (known as classical–quantum channels in the literature), thus generalizing the approach in [15]. In particular, a cost function is considered to quantify the cost of classical input symbols. We note here that our paper generalizes this setup to the fully quantum case in which there is a cost observable and the channels considered have quantum inputs and quantum outputs.

II. Preliminaries

For simplicity, we restrict our developments to finite-dimensional Hilbert spaces, with the exception of Section VII,

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

which applies to quantum Gaussian channels. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ denote finite-dimensional Hilbert spaces, and let $\mathcal{L}(\mathcal{H}_A)$ and $\mathcal{L}(\mathcal{H}_B)$ denote spaces of linear operators acting on those respective Hilbert spaces. We denote by $\mathcal{N}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ a quantum channel, defined to be a completely positive and trace-preserving map. By Stinespring's dilation theorem [23], [24], $\mathcal{N}_{A\to B}$ can be extended to an isometric channel $\mathcal{U}_{A\to BE} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_E)$, where $\mathcal{H}_E$ is some other finite-dimensional Hilbert space and $\mathcal{N}_{A\to B} = \mathrm{tr}_E \circ \mathcal{U}_{A\to BE}$.

Now, let $G \in \mathcal{L}(\mathcal{H}_A)$ be a positive semi-definite operator acting on $\mathcal{H}_A$. Throughout, we refer to G as the *cost observable*. This is the standard cost constraint used in applications of quantum Shannon theory (see, for instance, [16], [17], [20], [25]). As mentioned above, this is also a quantum generalization of a classical cost function [14], which is a map from the input alphabet to the non-negative reals. However, note that unlike in the classical case, we can use quantum codewords that are not eigenstates of the cost observable. This might even be necessary to achieve the capacity of a quantum channel. For example, for single-mode phase-insensitive bosonic Gaussian channels, the relevant cost observable is the photon number operator, but it is known that coherent states, not number states, achieve the classical capacity [26]–[28].

Lastly, given two quantum states $\rho, \sigma \in \mathcal{S}(\mathcal{H}_A)$, where $\mathcal{S}(\mathcal{H}_A) \subsetneq \mathcal{L}(\mathcal{H}_A)$ denotes the set of positive semi-definite operators with unit trace, a quantum hypothesis test with N copies is a binary positive-operator valued measure (POVM) $\{\Lambda_N, I - \Lambda_N\}$ that distinguishes between N copies of the two states. The two states to be distinguished are called the null and alternative hypotheses, respectively. Now, there are two possible errors that can occur. Taking Λ_N to be the measurement result that declares the state to be $\rho^{\otimes N}$, the error probabilities are given by

$$\alpha_N(\Lambda_N) \equiv \mathrm{tr}[(I - \Lambda_N)\rho^{\otimes N}], \tag{4}$$

$$\beta_N(\Lambda_N) \equiv \mathrm{tr}[\Lambda_N \sigma^{\otimes N}]. \tag{5}$$

The errors are called the Type I and Type II errors, respectively. Then, for some $\varepsilon \in (0, 1)$, we can define the following quantity:

$$\beta_N^*(\varepsilon) \equiv \inf_{\Lambda_N} \{\beta_N(\Lambda_N) | \alpha_N(\Lambda_N) \le \varepsilon\}. \tag{6}$$

That is, it is the lowest Type II error possible, given that the Type I error does not exceed ε. By Quantum Stein's Lemma [29], [30], for all $\varepsilon \in (0, 1)$,

$$\lim_{N\to\infty} -\frac{1}{N} \log_2 \beta_N^*(\varepsilon) = D(\rho\|\sigma), \tag{7}$$

where the quantum relative entropy $D(\rho\|\sigma)$ is defined as [21]

$$D(\rho\|\sigma) \equiv \mathrm{tr}[\rho(\log_2 \rho - \log_2 \sigma)] \tag{8}$$

whenever $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$ and it is equal to $+\infty$ otherwise.

III. Classical Communication

We first consider the case of unassisted classical communication over a quantum channel $\mathcal{N}$. Let $n, M \in \mathbb{N}$, $\nu \in \mathbb{R}_{>0}$, and $\varepsilon \in [0, 1]$. We denote an (n, M, ν, ε) code as one with blocklength n and number of messages M. Furthermore, denoting the quantum codewords as the density operators $\rho_{A^n}(1), \ldots, \rho_{A^n}(M) \in \mathcal{S}(\mathcal{H}_A^{\otimes n})$, each quantum codeword satisfies

$$\mathrm{tr}[G_n \rho_{A^n}(x)] \le \nu. \tag{9}$$

Finally, given that the decoder uses a POVM $\{\Pi_1, \ldots, \Pi_M\}$ to guess the message, the average error probability over the possible messages cannot exceed ε, i.e.,

$$\frac{1}{M} \sum_{m=1}^{M} \mathrm{tr}[(I^{\otimes n} - \Pi_m)\mathcal{N}^{\otimes n}(\rho_{A^n}(m))] \le \varepsilon. \tag{10}$$

We recall the definition for the cost-constrained classical capacity of a quantum channel [16], [17]:

Definition 1: Given $\varepsilon \in [0, 1)$, *and* $\beta > 0$, *a non-negative number* R *is an* ε*-achievable rate with average cost not exceeding* β *if for all* $\delta > 0$, $\exists n_0 \in \mathbb{N}$ *such that if* $n \ge n_0$, *then* $\exists$ *an* $(n, M, n\beta, \varepsilon)$ *code such that* $\frac{\log_2 M}{n} > R - \delta$. *Then,* R *is called achievable if it is* ε*-achievable for all* $\varepsilon \in (0, 1)$. *The supremum of all achievable rates with average cost not exceeding* β *is denoted* $C(\mathcal{N}, \beta)$, *the classical capacity cost function.*

For simplicity, for the rest of the section we will consider channels with additive Holevo information at all cost constraints, i.e.,

$$\forall \beta \ge 0, n \in \mathbb{N}, \quad \chi(\mathcal{N}^{\otimes n}, n\beta) = n\chi(\mathcal{N}, \beta), \tag{11}$$

where

$$\chi(\mathcal{N}^{\otimes n}, n\beta) \equiv \sup_{\substack{\{p_X, \rho_{A^n}(x)\} \\ \mathrm{tr}[G_n \bar{\rho}_{A^n}] \le n\beta}} I(X; B^n)_\rho \tag{12}$$

and

$$\rho_{XB^n} = \sum_x p_X(x)|x\rangle\langle x|_X \otimes \mathcal{N}^{\otimes n}(\rho_{A^n}(x)), \tag{13}$$

$$\bar{\rho}_{A^n} = \sum_x p_X(x)\rho_{A^n}(x). \tag{14}$$

Similar to the classical case [14], the classical capacity cost function can be computed as an optimization of a mutual information with respect to input ensembles that satisfy the cost constraint:

Theorem 2 [16], [17], [31], [32]: For a channel with additive Holevo information at all cost constraints, the classical capacity cost function is given by

$$C(\mathcal{N}, \beta) = \chi(\mathcal{N}, \beta) \equiv \sup_{\substack{\{p_X, \rho_A(x)\} \\ \mathrm{tr}[G\bar{\rho}_A] \le \beta}} I(X; B)_\rho. \tag{15}$$

We now give the definition of the classical capacity per unit cost.

Definition 3: Given $\varepsilon \in [0, 1)$, *a non-negative number* $\boldsymbol{R}$ *is an* ε*-achievable rate per unit cost if for every* $\delta > 0$, $\exists \nu_0 > 0$ *such that if* $\nu \ge \nu_0$, $\exists$ *an* (n, M, ν, ε) *code such that* $\log_2 M > \nu\ (\boldsymbol{R} - \delta)$. $\boldsymbol{R}$ *is achievable if it is achievable for all* $\varepsilon \in (0, 1)$ *and the capacity per unit cost is the supremum of all achievable rates per unit cost, denoted as* $\boldsymbol{C}(\mathcal{N})$.

Observe that the above definition is similar to that of the usual capacity, except that we replace the blocklength n by the cost ν. In fact, we can also give an expression for the

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

classical capacity per unit cost in terms of an optimized mutual information:

Theorem 4: The capacity per unit cost for a channel with additive Holevo information at all cost constraints is given by

$$\boldsymbol{C}(\mathcal{N}) = \sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta} = \sup_{\{p_X,\rho_A(x)\}} \frac{I(X;B)_\rho}{\operatorname{tr}[G\bar{\rho}_A]}. \tag{16}$$

The proof of Theorem 4 is based on [14] and follows from the achievability and converse for the cost-constrained classical capacity. In general it is sufficient to prove the coding theorem for the cost-constrained capacity in order to establish a coding theorem for the capacity per unit cost.

Proof of Theorem 4: We first show the achievability statement $\boldsymbol{C}(\mathcal{N}) \geq \sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta}$. Let $\beta > 0$. Let R be an achievable rate per channel use with average cost not exceeding β. We claim that R/β is an achievable rate per unit cost. This is clear for $R = 0$, and so we can assume $R > 0$. To see the claim, let $\varepsilon \in (0,1)$ and fix some $\delta > 0$. Then, by definition $\exists n_0$ such that for all $n \geq n_0$ there is an $(n, M, n\beta, \varepsilon)$ code such that

$$\frac{\log_2 M}{n} > R - \frac{\beta\delta}{2}. \tag{17}$$

This same code is an $(n, M, n\beta, \varepsilon)$ code such that

$$\frac{\log_2 M}{n\beta} > \frac{R}{\beta} - \frac{\delta}{2}. \tag{18}$$

Now, let $\nu_0 = \max\left\{(n_0+1)\beta, \frac{2R}{\delta}\right\}$ and $\nu \geq \nu_0$. If $\nu = n\beta$ for some $n \in \mathbb{N}$, then $n \geq n_0$, and so the above $(n, M, n\beta, \varepsilon)$ code satisfies the necessary requirements. If instead $n\beta < \nu < (n+1)\beta$ for some $n \in \mathbb{N}$, then we note

$$n + 1 > \frac{\nu}{\beta} \geq \frac{\nu_0}{\beta} \geq \frac{2R}{\delta\beta}, \tag{19}$$

and so

$$\left(\frac{R}{\beta} - \frac{\delta}{2}\right)\frac{n\beta}{\nu} > \left(\frac{R}{\beta} - \frac{\delta}{2}\right)\frac{n}{n+1} \tag{20}$$

$$= \left(\frac{R}{\beta} - \frac{\delta}{2}\right)\left(1 - \frac{1}{n+1}\right) \tag{21}$$

$$> \left(\frac{R}{\beta} - \frac{\delta}{2}\right)\left(1 - \frac{\delta\beta}{2R}\right) \tag{22}$$

$$> \frac{R}{\beta} - \delta. \tag{23}$$

Now, $(n+1)\beta > \nu \geq \nu_0$, so $n \geq n_0$. Hence, the above $(n, M, n\beta, \varepsilon)$ code is a (n, M, ν, ε) code such that

$$\frac{\log_2 M}{\nu} > \left(\frac{R}{\beta} - \frac{\delta}{2}\right)\frac{n\beta}{\nu} > \frac{R}{\beta} - \delta. \tag{24}$$

Hence we have shown achievability.

We next show the converse statement $\boldsymbol{C}(\mathcal{N}) \leq \sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta}$. Suppose $\mathcal{N}$ has an (n, M, ν, ε) code. By a standard data-processing argument and entropy continuity bound [25], [33], [34], we have

$$\log_2 M \leq \chi(\mathcal{N},\nu) + f(M,\varepsilon). \tag{25}$$

where $f(M,\varepsilon) = \varepsilon \log_2 M + (\varepsilon+1)\log_2(\varepsilon+1) - \varepsilon\log_2\varepsilon$, so that $\lim_{\varepsilon\to 0} f(M,\varepsilon) = 0$. Thus,

$$\frac{\log_2 M}{\nu} \leq \frac{\chi(\mathcal{N},\nu)}{\nu} + \frac{f(M,\varepsilon)}{\nu} \tag{26}$$

$$= \frac{1}{\nu} \sup_{\substack{\{p_X,\rho_A(x)\}\\ \operatorname{tr}[G\bar{\rho}_A]\leq\nu}} I(X;B)_\rho + \frac{f(M,\varepsilon)}{\nu} \tag{27}$$

$$\leq \sup_{\beta>0} \frac{1}{\beta} \sup_{\substack{\{p_X,\rho_A(x)\}\\ \operatorname{tr}[G\bar{\rho}_A]\leq\beta}} I(X;B)_\rho + \frac{f(M,\varepsilon)}{\nu} \tag{28}$$

$$= \sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta} + \frac{f(M,\varepsilon)}{\nu}. \tag{29}$$

Thus, for any ε-achievable rate per unit cost $\boldsymbol{R}$, for any $\delta > 0$ there exists ν_0 such that for $\nu \geq \nu_0$,

$$\boldsymbol{R} - \delta < \sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta} + \frac{f(M,\varepsilon)}{\nu}. \tag{30}$$

Hence, for all $\delta > 0$,

$$\boldsymbol{R} - \delta < \liminf_{\nu\to\infty}\left(\sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta} + \frac{f(M,\varepsilon)}{\nu}\right). \tag{31}$$

Hence, if $\boldsymbol{R}$ is an achievable rate per unit cost, then

$$\boldsymbol{R} \leq \sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta}. \tag{32}$$

This establishes the first equality in Theorem 4.

To show the second equality, we first argue

$$\sup_{\beta>0} \frac{C(\mathcal{N},\beta)}{\beta} = \sup_{\beta>0} \frac{1}{\beta} \sup_{\substack{\{p_X,\rho_A(x)\}\\ \operatorname{tr}[G\bar{\rho}_A]\leq\beta}} I(X;B)_\rho \tag{33}$$

$$\leq \sup_{\beta>0} \sup_{\substack{\{p_X,\rho_A(x)\}\\ \operatorname{tr}[G\bar{\rho}_A]\leq\beta}} \frac{1}{\operatorname{tr}[G\bar{\rho}_A]} I(X;B)_\rho \tag{34}$$

$$= \sup_{\{p_X,\rho_A(x)\}} \frac{I(X;B)_\rho}{\operatorname{tr}[G\bar{\rho}_A]}. \tag{35}$$

Note that the inequality is trivial if for some ensemble $\operatorname{tr}[G\bar{\rho}_A] = 0$ and $I(X;B)_\rho > 0$. Now, this is also an achievable rate per unit cost since for any $\{p_X, \rho_A(x)\}$, we can achieve a rate per channel use $I(X;B)_\rho$ using cost-constrained Holevo-Schumacher-Westmoreland (HSW) coding [16], [17], [25], [31], [32]. The average cost per channel use is then exactly $\operatorname{tr}[G\bar{\rho}_A]$, and so we achieve a capacity per unit cost equal to

$$\frac{I(X;B)_\rho}{\operatorname{tr}[G\bar{\rho}_A]}. \tag{36}$$

This concludes the proof. □

Now, suppose that we have a state ψ^0 with zero cost, i.e., $\operatorname{tr}[G\psi^0] = 0$. As mentioned above, without loss of generality, ψ^0 can be taken pure since otherwise we can spectrally decompose it and conclude that all of its eigenstates must have zero cost since $G \geq 0$. In this special case, the capacity per unit cost is given by the following simple expression:

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

Theorem 5: If there is a state ψ^0 with zero cost, then the capacity per unit cost of a channel with additive Holevo information at all cost constraints is

$$\boldsymbol{C}(\mathcal{N}) = \sup_{\psi \neq \psi^0} \frac{D(\mathcal{N}(\psi) \| \mathcal{N}(\psi^0))}{\langle \psi | G | \psi \rangle}, \tag{37}$$

where ψ is pure.

Just as was found in [14], the expression for the capacity per unit cost is arguably simpler than that for the capacity cost function given in eq. (15). The latter requires an optimization over ensembles on the input space while the former only requires an optimization over the input space itself.

We now give a proof of Theorem 5.

Proof: Without loss of generality, ψ^0 is the unique zero-cost state. Otherwise, let $\phi^0 \neq \psi^0$ be a zero-cost state. If $\mathcal{N}(\phi^0) \neq \mathcal{N}(\psi^0)$, the capacity per unit cost is infinite since we can send a binary message with zero cost. If on the other hand $\mathcal{N}(\phi^0) = \mathcal{N}(\psi^0)$, then ϕ^0 is the same as ψ^0 for the purposes of communicating over $\mathcal{N}$.

We first prove the direct part. To begin with, we note that the possibility of time-sharing (interpolation between two different protocols) implies that $C(\mathcal{N}, \beta)$ is concave in β. Furthermore, we have a zero-cost state and so $C(\mathcal{N}, \beta)/\beta$ is monotone non-increasing on $(0, +\infty)$. We conclude that

$$\boldsymbol{C}(\mathcal{N}) = \lim_{\beta \searrow 0} \frac{C(\mathcal{N}, \beta)}{\beta}. \tag{38}$$

Now, let $\beta \in (0, \langle \psi | G | \psi \rangle)$ and consider the following classical-quantum state:

$$\rho^\beta_{XA} = \left(1 - \frac{\beta}{\langle \psi | G | \psi \rangle}\right) |0\rangle\langle 0| \otimes \psi^0 + \frac{\beta}{\langle \psi | G | \psi \rangle} |1\rangle\langle 1| \otimes \psi, \tag{39}$$

where $\psi \neq \psi^0$. By Theorem 4, we can achieve the following rate per unit cost:

$$\frac{I(X; B)_{\rho^\beta}}{\beta}. \tag{40}$$

Now, recall the following identity, which holds for a classical-quantum state $\rho_{XB} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes \rho^x_B$ [25], [35] where for all x, $p_X(x) > 0$:

$$\begin{aligned} I(X; B)_\rho &= D(\rho_{XB} \| \rho_X \otimes \rho_B) \\ &= \sum_x p_X(x) D(\rho^x_B \| \rho_B). \end{aligned} \tag{41}$$

This expression is well defined because $\text{supp}(\rho^x_B) \subseteq \text{supp}(\rho_B)$ for all x. Hence by eq. (41) and non-negativity of quantum relative entropy when evaluated on quantum states, we obtain

$$\frac{I(X; B)_{\rho^\beta}}{\beta} \geq \frac{D(\mathcal{N}(\psi) \| \rho^\beta_B)}{\langle \psi | G | \psi \rangle}. \tag{42}$$

So by the lower semicontinuity of the relative entropy [25],

$$\begin{aligned} \boldsymbol{C}(\mathcal{N}) &= \lim_{\beta \searrow 0} \frac{C(\mathcal{N}, \beta)}{\beta} && (43) \\ &\geq \lim_{\beta \searrow 0} \frac{I(X; B)_{\rho^\beta}}{\beta} && (44) \\ &\geq \liminf_{\beta \searrow 0} \frac{D(\mathcal{N}(\psi) \| \rho^\beta_B)}{\langle \psi | G | \psi \rangle} && (45) \\ &\geq \frac{D(\mathcal{N}(\psi) \| \mathcal{N}(\psi^0))}{\langle \psi | G | \psi \rangle}. && (46) \end{aligned}$$

This holds for all $\psi \neq \psi^0$, and so we obtain the direct part

$$\boldsymbol{C}(\mathcal{N}) \geq \sup_{\psi \neq \psi^0} \frac{D(\mathcal{N}(\psi) \| \mathcal{N}(\psi^0))}{\langle \psi | G | \psi \rangle}. \tag{47}$$

For the converse, we start with

$$\begin{aligned} I(X; B)_\rho &= \inf_{\sigma_B \in \mathcal{S}(\mathcal{H}_B)} D(\rho_{XB} \| \rho_X \otimes \sigma_B) && (48) \\ &\leq D(\rho_{XB} \| \rho_X \otimes \mathcal{N}(\psi^0)) && (49) \\ &= \sum_x p_X(x) D(\mathcal{N}(\rho^x) \| \mathcal{N}(\psi^0)). && (50) \end{aligned}$$

The first equality is a well known identity [33, Exercise 11.8.2]. Note that if any of the relative entropies are infinite, then the bound is trivial. Therefore, $\forall \beta > 0$, (51)–(57) hold, as shown at the top of the next page, where eq. (52) follows since pure state ensembles maximize the Holevo information (even with a cost constraint), and we can divide by $\langle \psi^x | G | \psi^x \rangle$ in eq. (55) since we assumed ψ^0 is the unique zero-cost state. □

A. Pulse-Position-Modulation Scheme for Classical Communication

We can also directly prove the achievability part of Theorem 5 without going through the cost-constrained capacity, as was done in [14] for the classical case. This follows by using a PPM scheme along the following lines.

Encoding: Let $\psi \neq \psi^0$ be a pure state and fix $M, N \in \mathbb{N}$. For a message $m \in [1 : M]$, the sender transmits the following length-MN sequence of states:

$$\left[(\psi^0)^{\otimes N}\right]^{\otimes m-1} \otimes \psi^{\otimes N} \otimes \left[(\psi^0)^{\otimes N}\right]^{\otimes M-m}. \tag{58}$$

That is, the message is encoded in the position of a ψ-"pulse" amidst a baseline of zero-cost states. Note that the cost of each codeword is $N \langle \psi | G | \psi \rangle$.

Decoding: Let $\varepsilon \in (0, 1)$. The receiver obtains the state

$$\left[\mathcal{N}(\psi^0)^{\otimes N}\right]^{\otimes m-1} \otimes \mathcal{N}(\psi)^{\otimes N} \otimes \left[\mathcal{N}(\psi^0)^{\otimes N}\right]^{\otimes M-m}. \tag{59}$$

Then, the receiver uses a quantum hypothesis test to deduce the position of the pulse. Specifically, he performs M independent binary hypothesis tests with N copies where the null hypothesis is $\mathcal{N}(\psi)$ and the alternative hypothesis is $\mathcal{N}(\psi^0)$. If the receiver obtains a test result of the form eq. (59) for some $\hat{m}$, then $\hat{m}$ is declared. Otherwise an error is declared.

Error Analysis: Let A_{iN}, for $i \in [1 : M]$, denote the POVM of the ith hypothesis test, and let $\alpha_{iN}(A_{iN})$ and $\beta_{iN}(A_{iN})$ denote the Type I and Type II errors, respectively. Now, the error probability p_e is independent of the message by symmetry, so we can fix some message index i. Furthermore, since

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

$$\frac{C(\mathcal{N},\beta)}{\beta} = \frac{1}{\beta} \sup_{\substack{\{p_X,\rho^x\}\\ \mathrm{tr}[G\bar{\rho}]\le\beta}} I(X;B) \tag{51}$$
$$= \frac{1}{\beta} \sup_{\substack{\{p_X,\psi^x\}\\ \mathrm{tr}[G\bar{\psi}]\le\beta}} I(X;B) \tag{52}$$
$$\le \frac{1}{\beta} \sup_{\substack{\{p_X,\psi^x\}\\ \frac{1}{\beta}\mathrm{tr}[G\bar{\psi}]\le 1}} \sum_x p_X(x) D(\mathcal{N}(\psi^x)\|\mathcal{N}(\psi^0)) \tag{53}$$
$$= \frac{1}{\beta} \sup_{\substack{\{p_X,\psi^x\},\psi^x\neq\psi^0\\ \frac{1}{\beta}\mathrm{tr}[G\bar{\psi}]\le 1}} \sum_x p_X(x) D(\mathcal{N}(\psi^x)\|\mathcal{N}(\psi^0)) \tag{54}$$
$$= \sup_{\substack{\{p_X,\psi^x\},\psi^x\neq\psi^0\\ \frac{1}{\beta}\mathrm{tr}[G\bar{\psi}]\le 1}} \sum_x p_X(x) \frac{D(\mathcal{N}(\psi^x)\|\mathcal{N}(\psi^0))}{\langle\psi^x|\,G\,|\psi^x\rangle} \frac{\langle\psi^x|\,G\,|\psi^x\rangle}{\beta} \tag{55}$$
$$\le \sup_{\psi\neq\psi^0} \frac{D(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0))}{\langle\psi|\,G\,|\psi\rangle} \sup_{\substack{\{p_X,\psi^x\},\psi^x\neq\psi^0\\ \frac{1}{\beta}\mathrm{tr}[G\bar{\psi}]\le 1}} \sum_x p_X(x) \frac{\langle\psi^x|\,G\,|\psi^x\rangle}{\beta} \tag{56}$$
$$\le \sup_{\psi\neq\psi^0} \frac{D(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0))}{\langle\psi|\,G\,|\psi\rangle}, \tag{57}$$

each POVM acts on independent size-N blocks, we can apply the classical union bound as follows:

$$p_e \le \alpha_{iN} + (M-1)\beta_{iN}. \tag{60}$$

By eq. (7), for $\varepsilon \in (0,1)$,

$$\lim_{N\to\infty} -\frac{1}{N}\log_2 \beta^*_{iN}(\varepsilon/2) = D(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0)). \tag{61}$$

Using the test A_{iN} that achieves $\beta^*_{iN}(\varepsilon/2)$ and given $\delta > 0$, for sufficiently large N, the probability of error is bounded by

$$p_e \le \frac{\varepsilon}{2} + (M-1)2^{-ND(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0))+N\delta}. \tag{62}$$

Hence, if

$$\frac{\log_2 M}{N\,\langle\psi|\,G\,|\psi\rangle} < \frac{D(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0))}{\langle\psi|\,G\,|\psi\rangle} - \frac{2\delta}{\langle\psi|\,G\,|\psi\rangle}, \tag{63}$$

then $p_e < \varepsilon$ for sufficiently large N. Therefore, $\frac{D(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0))}{\langle\psi|G|\psi\rangle}$ is an achievable rate per unit cost.

IV. Entanglement-Assisted Communication

We now consider the case of communication with unlimited entanglement assistance. We define an (n, M, ν, ε) code in the same way as in the unassisted case, with the exception that the sender and receiver are allowed to share an arbitrary quantum state of arbitrary dimension before communication begins and they can use this resource in the encoding and decoding. The entanglement-assisted capacity cost function $C_{\mathrm{EA}}(\mathcal{N},\beta)$ is defined similarly but again takes into account the entanglement assistance.

Let A and A' denote quantum systems with isomorphic Hilbert spaces. Define for a bipartite state $\varphi_{AA'}$

$$\varphi_{AB} \equiv (\mathrm{id}_A \otimes \mathcal{N}_{A'\to B})(\varphi_{AA'}). \tag{64}$$

We recall the following theorem:

Theorem 6 [16]: The entanglement-assisted capacity cost function for a quantum channel $\mathcal{N}_{A'\to B}$ is given by

$$C_{\mathrm{EA}}(\mathcal{N},\beta) = \max_{\substack{\varphi_{AA'}\\ \mathrm{tr}[G\varphi_{A'}]\le\beta}} I(A;B)_\varphi, \tag{65}$$

where $\varphi_{AA'}$ is a pure bipartite state.

We define the entanglement-assisted capacity per unit cost $\boldsymbol{C}_{\mathrm{EA}}(\mathcal{N})$ in the same manner and obtain an expression for it in the same way as in the unassisted case (i.e., as done in Theorem 4).

Theorem 7: The entanglement-assisted capacity per unit cost for a quantum channel $\mathcal{N}_{A'\to B}$ is given by

$$\boldsymbol{C}_{\mathrm{EA}}(\mathcal{N}) = \sup_{\beta>0} \frac{C_{\mathrm{EA}}(\mathcal{N},\beta)}{\beta} = \sup_{\varphi_{AA'}} \frac{I(A;B)_\varphi}{\mathrm{tr}[G\varphi_{A'}]}. \tag{66}$$

Now suppose that we have a zero-cost pure state ψ^0. Similar to the unassisted case, we obtain the expression for the entanglement-assisted capacity per unit cost given in Theorem 8. Note that, like the mutual information, the quantity to be optimized is only a function of the input state $\varphi_{A'}$ and not of the specific purification. Also note that, unlike the unassisted case, $\boldsymbol{C}_{\mathrm{EA}}$ is ostensibly as difficult to calculate as C_{EA}.

Theorem 8: If there is a state ψ^0 with zero cost, then the entanglement-assisted capacity per unit cost of a channel $\mathcal{N}_{A'\to B}$ is given by

$$\boldsymbol{C}_{\mathrm{EA}}(\mathcal{N}) = \sup_{\varphi_{AA'}} \boldsymbol{C}_{\mathrm{EA},\psi^0}(\mathcal{N},\varphi), \tag{67}$$

where

$$\boldsymbol{C}_{\mathrm{EA},\psi^0}(\mathcal{N},\varphi) = \begin{cases} \frac{D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'}))}{\mathrm{tr}[G\varphi_{A'}]} & D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'}))>0\\ 0 & \textit{otherwise}. \end{cases} \tag{68}$$

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

Proof: The proof proceeds much like in the unassisted case. Suppose that $\varphi^0 \neq \psi^0$ has zero cost. Now, if $D(\varphi^0_{AB}\|\varphi^0_A\otimes\mathcal{N}(\psi^0_{A'})) > 0$, we clearly have infinite $\boldsymbol{C}_{\text{EA}}(\mathcal{N})$ since we can send a distinguishable binary message (using the entangled state $\varphi^0_{AA'}$) with zero cost. Hence it is sufficient to assume that $D(\varphi^0_{AB}\|\varphi^0_A\otimes\mathcal{N}(\psi^0_{A'})) = 0$.

We now prove achievability. By concavity of $C_{\text{EA}}(\mathcal{N},\beta)$ with respect to β and the existence of a zero-cost state,

$$\boldsymbol{C}_{\text{EA}}(\mathcal{N}) = \lim_{\beta\searrow 0}\frac{C_{\text{EA}}(\mathcal{N},\beta)}{\beta}. \tag{69}$$

Consider some $\varphi_{AA'}$. Since we can trivially achieve zero rate, suppose that $\varphi_{A'}$ has positive cost. Then, define the following state:

$$\rho^{\beta}_{XAA'} \equiv \left(1-\frac{\beta}{\operatorname{tr}[G\varphi_{A'}]}\right)|0\rangle\langle 0|_X\otimes\varphi_A\otimes\psi^0_{A'} + \frac{\beta}{\operatorname{tr}[G\varphi_{A'}]}|1\rangle\langle 1|_X\otimes\varphi_{AA'}, \tag{70}$$

where $\beta \in (0,\operatorname{tr}[G\varphi_{A'}])$. By Theorem 7 and the data-processing inequality for mutual information, we obtain the following entanglement-assisted rate per unit cost for the mixed state $\rho^{\beta}_{XAB} \equiv (\text{id}_{XA}\otimes\mathcal{N}_{A'\to B})(\rho^{\beta}_{XAA'})$:

$$\frac{I(XA;B)_{\rho^{\beta}}}{\beta}. \tag{71}$$

Now, we can write the mutual information of any classical-quantum state

$$\rho_{XAB} = \sum_x p_X(x)|x\rangle\langle x|_X\otimes\rho^x_{AB} \tag{72}$$

as the following convex sum of relative entropies:

$$\begin{aligned} I(XA;B)_{\rho} &= \operatorname{tr}\left[\rho_{XAB}\left(\log_2\rho_{XAB}-\log_2\rho_{XA}\otimes\rho_B\right)\right] \\ &= \sum_x p_X(x)\operatorname{tr}_{AB}\left[\rho^x_{AB}\left(\log_2\rho^x_{AB}-\log_2\rho^x_A\otimes\rho_B\right)\right] \\ &= \sum_x p_X(x) D(\rho^x_{AB}\|\rho^x_A\otimes\rho_B). \end{aligned} \tag{73}$$

Thus, by the non-negativity of quantum relative entropy when evaluated on quantum states,

$$\frac{I(XA;B)_{\rho^{\beta}}}{\beta} \geq \frac{D\left(\varphi_{AB}\|\varphi_A\otimes\rho^{\beta}_B\right)}{\operatorname{tr}[G\varphi_{A'}]}. \tag{74}$$

Hence, again by the lower semicontinuity of the relative entropy,

$$\begin{aligned} \boldsymbol{C}_{\text{EA}}(\mathcal{N}) &= \lim_{\beta\searrow 0}\frac{C_{\text{EA}}(\mathcal{N},\beta)}{\beta} & (75)\\ &\geq \lim_{\beta\searrow 0}\frac{I(XA;B)_{\rho^{\beta}}}{\beta} & (76)\\ &\geq \liminf_{\beta\searrow 0}\frac{D\left(\varphi_{AB}\|\varphi_A\otimes\rho^{\beta}_B\right)}{\operatorname{tr}[G\varphi_{A'}]} & (77)\\ &\geq \frac{D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'}))}{\operatorname{tr}[G\varphi_{A'}]}. & (78) \end{aligned}$$

For the converse, we have for any pure input state $\varphi_{AA'}$,

$$\begin{aligned} I(A;B)_{\varphi} &= \inf_{\sigma_B} D(\varphi_{AB}\|\varphi_A\otimes\sigma_B) & (79)\\ &\leq D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'})). & (80) \end{aligned}$$

Note again that if the relative entropy is infinite, then the bound is trivial. Hence,

$$\frac{C_{\text{EA}}(\mathcal{N},\beta)}{\beta} \leq \sup_{\substack{\varphi_{AA'} \\ \operatorname{tr}[G\varphi_{A'}]\leq\beta}}\frac{D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'}))}{\beta}. \tag{81}$$

Now, we assumed that for any zero-cost state φ^0, $D(\varphi_{AB}\|\varphi^0_A\otimes\mathcal{N}(\psi^0_{A'})) = 0$. Thus we can take the supremum over non-zero cost states. If there are not any, then eq. (81) implies that the upper bound is 0, which would conclude the converse. Otherwise, we can argue

$$\begin{aligned} \frac{C_{\text{EA}}(\mathcal{N},\beta)}{\beta} &\leq \sup_{\substack{\varphi_{AA'} \\ \frac{1}{\beta}\operatorname{tr}[G\varphi_{A'}]\leq 1}}\frac{D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'}))}{\operatorname{tr}[G\varphi_{A'}]}\frac{\operatorname{tr}[G\varphi_{A'}]}{\beta} & (82)\\ &\leq \sup_{\varphi_{AA'}}\frac{D(\varphi_{AB}\|\varphi_A\otimes\mathcal{N}(\psi^0_{A'}))}{\operatorname{tr}[G\varphi_{A'}]}. & (83) \end{aligned}$$

This concludes the proof. □

A. Pulse-Position-Modulation Scheme for Entanglement-Assisted Classical Communication

We propose a PPM scheme that achieves the rate given in eq. (67), thereby providing an alternative proof of the direct part of Theorem 8. This will be much like the scheme in the unassisted case except with the greater discriminatory power that entanglement assistance provides.

Encoding: Let $\varphi_{A'}$ be a positive-cost state and fix $M, N \in \mathbb{N}$. The sender and receiver share MN copies of a pure state $\varphi_{AA'}$, where A' is at the sender and A is at the receiver, where we have N copies for each message in $[1:M]$. Hence the overall shared state is

$$\bigotimes_{i=1}^{M}\left(\varphi_{A_iA'_i}\right)^{\otimes N}. \tag{84}$$

For a message $m \in [1:M]$, the sender transmits a $\varphi_{A'}$-pulse amidst a zero-cost state baseline by using the following sequence of states:

$$\bigotimes_{i=1}^{m-1}\left(\psi^0_{A'_i}\right)^{\otimes N}\otimes\left(\varphi_{A'_m}\right)^{\otimes N}\otimes\bigotimes_{j=m+1}^{M}\left(\psi^0_{A'_j}\right)^{\otimes N}. \tag{85}$$

That is, the sender transmits the zero-cost state, but at every mth block of length N, he sends his shares of the corresponding copies of $\varphi_{AA'}$. Note that the cost of each codeword is $N\operatorname{tr}[G\varphi_{A'}]$.

Decoding: Let $\varepsilon \in (0,1)$. Now, since $\varphi_{AA'}$ purifies $\varphi_{A'}$, whenever the sender transmits ψ^0, the receiver obtains a

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

product state $\varphi_A \otimes \mathcal{N}(\psi^0)$. Hence, the receiver now has the state

$$\bigotimes_{i=1}^{m-1} \left(\varphi_{A_i} \otimes \mathcal{N}(\psi^0_{A'_i})\right)^{\otimes N} \otimes \ (\mathrm{id}_A \otimes \mathcal{N})(\varphi_{A_m A'_m})^{\otimes N} \otimes \bigotimes_{j=m+1}^{M} \left(\varphi_{A_j} \otimes \mathcal{N}(\psi^0_{A'_j})\right)^{\otimes N}. \quad (86)$$

Then, the receiver uses quantum hypothesis testing along with his shares of the entangled states to deduce the position of the pulse. He performs M independent binary hypothesis tests with N copies where the null hypothesis is $\varphi_{AB} \equiv (\mathrm{id}_A \otimes \mathcal{N}_{A' \to B})(\varphi_{AA'})$ and the alternative hypothesis is $\varphi_A \otimes \mathcal{N}(\psi^0_{A'})$. If the receiver obtains a test result of the form eq. (86) for some $\hat{m}$, then $\hat{m}$ is declared. Otherwise an error is declared.

Error Analysis: The error analysis follows in exactly the same way as the unassisted case. We conclude that we can obtain vanishing error in transmission provided that, for some $\delta > 0$,

$$\frac{\log_2 M}{N \,\mathrm{tr}[G\varphi_{A'}]} < \frac{D(\varphi_{AB} \| \varphi_A \otimes \mathcal{N}(\psi^0_{A'}))}{\mathrm{tr}[G\varphi_{A'}]} - \frac{\delta}{\mathrm{tr}[G\varphi_{A'}]}. \quad (87)$$

Hence we achieve the entanglement-assisted rate per unit cost $\frac{D(\varphi_{AB} \| \varphi_A \otimes \mathcal{N}(\psi^0_{A'}))}{\mathrm{tr}[G\varphi_{A'}]}$.

Similar to the position-based coding scheme for entanglement-assisted classical communication [36], this scheme does not consume all the entanglement needed to implement the encoding. This follows from the gentle-measurement lemma [37], [38]: the entangled states that were not transmitted but measured by the decoder will only be negligibly disturbed, given that the decoding measurement succeeds with high probability. Now, the natural measure of rate of entanglement consumption in this setting is entanglement consumed per unit cost, and in this scheme it can be expressed in terms of the entanglement entropy of $\varphi_{AA'}$ as follows:

$$\frac{N S(A)_\varphi}{N \,\mathrm{tr}[G\varphi_{A'}]} = \frac{S(A)_\varphi}{\mathrm{tr}[G\varphi_{A'}]}. \quad (88)$$

V. Private Communication

We now consider private communication over a quantum channel. This was first studied in [39], [40] when there is no cost constraint and recently in [41] when there is a cost constraint. Given a noisy channel $\mathcal{N}_{A\to B}$, let $\mathcal{U}_{A\to BE}$ denote an isometric channel extending it and let $\mathcal{N}^c_{A\to E} = \mathrm{tr}_B \circ \mathcal{U}_{A\to BE}$ denote the induced complementary channel. A channel $\mathcal{N}_{A\to B}$ is degradable if there exists a degrading channel $\mathcal{D}_{B\to E}$ such that $\mathcal{N}^c_{A\to E} = \mathcal{D}_{B\to E} \circ \mathcal{N}_{A\to B}$ [54].

The formulation here is based on [42], but note that here we use a definition of a private code with the privacy based on trace distance [33], [41], [43]. Namely, we define an $(n, M, \nu, \varepsilon, \zeta)$ private code as having blocklength $n \in \mathbb{N}$, number of messages $M \in \mathbb{N}$, total cost at most $\nu \in \mathbb{R}_{>0}$, and probability of error of the receiver's decoding at most $\varepsilon \in [0, 1]$. The quantity $\zeta \in [0, 1]$ bounds the privacy error for each message: for each message, we demand that the eavesdropper's state is approximately independent of the message. Specifically, for all $m \in [1 : M]$, we require that

$$\frac{1}{2}\left\| \left(\mathcal{N}^c_{A\to E}\right)^{\otimes n} (\rho_{A^n}(m)) - \sigma_{E^n} \right\|_1 \le \zeta, \quad (89)$$

where $\rho_{A^n}(m)$ are the codewords and σ_{E^n} is some fixed state independent of m.

We can now establish some definitions.

Definition 9 [41]: Given $\beta > 0$, R_p is an achievable private communication rate with average cost not exceeding β if for all $\varepsilon, \zeta \in (0, 1)$ and $\delta > 0$, $\exists\, n_0$ such that $\forall n \ge n_0$, there is an $(n, M, n\beta, \varepsilon, \zeta)$ code for which

$$\frac{\log_2 M}{n} > R_p - \delta. \quad (90)$$

The supremum of all achievable rates with average cost not exceeding β as a function of β is the private capacity cost function $P(\mathcal{N}, \beta)$.

We recall the formula for $P(\mathcal{N}, \beta)$ when $\mathcal{N}$ is a degradable channel:

Theorem 10 [41]: The private capacity cost function for a degradable channel $\mathcal{N}_{A\to B}$ is given by

$$P(\mathcal{N}, \beta) = \sup_{\substack{\{p_X, \psi_A(x)\} \\ \mathrm{tr}[G\bar{\psi}_A] \le \beta}} I(X; B)_\rho - I(X; E)_\rho, \quad (91)$$

where each state $\psi_A(x)$ is pure,

$$\rho_{XBE} = \sum_x |x\rangle\langle x|_X \otimes \mathcal{U}_{A\to BE}(\psi_A(x)), \quad (92)$$

and $\bar{\psi}_A = \sum_x p_X(x)\psi_A(x)$ is the average input state.

Now we give the definition for the private capacity per unit cost.

Definition 11: $\boldsymbol{R}_p$ is an achievable private communication rate per unit cost if for all $\varepsilon, \zeta \in (0, 1)$ and $\delta > 0$, there $\exists\, \nu_0 > 0$ such that $\forall \nu \ge \nu_0$, there is an $(n, M, \nu, \varepsilon, \zeta)$ code for which

$$\log_2 M > \nu(\boldsymbol{R}_p - \delta). \quad (93)$$

The private capacity per unit cost is equal to the supremum of all achievable private communication rates per unit cost, denoted by $\boldsymbol{P}(\mathcal{N})$.

We can obtain an expression for the private capacity per unit cost via the private capacity cost function. A proof of this follows from the achievability and converse of the cost-constrained private capacity per channel use [41], just as in the proof of Theorem 4.

Theorem 12: The private capacity per unit cost of a degradable channel $\mathcal{N}_{A\to B}$ is given by

$$\boldsymbol{P}(\mathcal{N}) = \sup_{\beta > 0} \frac{P(\mathcal{N}, \beta)}{\beta} = \sup_{\{p_X, \psi_A(x)\}} \frac{I(X; B)_\rho - I(X; E)_\rho}{\mathrm{tr}[G\bar{\psi}_A]}, \quad (94)$$

where $\bar{\psi}_A$ is the average input state.

Now again suppose that we have a zero-cost state ψ^0. We then obtain the following simpler expression for the private capacity per unit cost.

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

Theorem 13: If there is a state ψ^0 with zero cost, then the private capacity per unit cost of a degradable channel $\mathcal{N}_{A\to B}$ is given by

$$\boldsymbol{P}(\mathcal{N}) = \sup_{\psi} \boldsymbol{P}_{\psi^0}(\mathcal{N}, \psi), \tag{95}$$

where ψ is pure,

$$\boldsymbol{P}_{\psi^0}(\mathcal{N}, \psi) \equiv \begin{cases} \frac{N_{\mathcal{N}}(\psi, \psi^0)}{\langle \psi | G | \psi \rangle} & N_{\mathcal{N}}(\psi, \psi^0) > 0 \\ 0 & \textit{otherwise}, \end{cases} \tag{96}$$

$$N_{\mathcal{N}}(\psi, \psi^0) \equiv D(\mathcal{N}(\psi) \| \mathcal{N}(\psi^0)) - D(\mathcal{N}^c(\psi) \| \mathcal{N}^c(\psi^0)), \tag{97}$$

and $\mathcal{N}^c_{A\to E}$ denotes the complementary channel of $\mathcal{N}$ corresponding to an isometric channel $\mathcal{U}_{A\to BE}$ extending $\mathcal{N}$.

Proof: Suppose that the state φ^0 has zero cost. If $N_{\mathcal{N}}(\varphi^0, \psi^0) \neq 0$, we have a zero-cost binary alphabet over which we can form ensembles for which $I(X;B) - I(X;E) > 0$. Hence, by Theorem 12, we can attain infinite private capacity per unit cost. Thus, it suffices to assume $N_{\mathcal{N}}(\varphi^0, \psi^0) = 0$.

Now, once again by concavity and the existence of a zero-cost state,

$$\boldsymbol{P}(\mathcal{N}) = \lim_{\beta \searrow 0} \frac{P(\mathcal{N}, \beta)}{\beta}. \tag{98}$$

Let $\beta \in (0, \langle \psi | G | \psi \rangle)$, and let ψ be a pure state. We can assume that ψ has positive cost since it is trivial to attain zero rate. Consider the following classical-quantum state:

$$\rho^{\beta}_{XBE} = \left(1 - \frac{\beta}{\langle \psi | G | \psi \rangle}\right) |0\rangle\langle 0|_X \otimes \mathcal{U}_{A\to BE}(\psi^0_A) + \frac{\beta}{\langle \psi | G | \psi \rangle} |1\rangle\langle 1|_X \otimes \mathcal{U}_{A\to BE}(\psi_A). \tag{99}$$

By a similar argument as in the unassisted case applied to each relative entropy in $N_{\mathcal{N}}$, in the limit $\beta \searrow 0$, this ensemble achieves the desired quantity:

$$\boldsymbol{P}(\mathcal{N}) \geq \lim_{\beta \searrow 0} \frac{I(X;B)_{\rho^\beta} - I(X;E)_{\rho^\beta}}{\beta} \geq \frac{N_{\mathcal{N}}(\psi, \psi^0)}{\langle \psi | G | \psi \rangle}. \tag{100}$$

In arriving at the above result, we need to make use of the lower semi-continuity of the private information as a function of the input ensemble. This is proven for bounded cost ensembles in certain settings in Corollary 3 of [44] and in particular applies to our case here.

For the converse, we note that for any ensemble $\{p_X, \rho^x\}$,

$$\begin{aligned} I(X;B)_\rho - I(X;E)_\rho \\ &= \sum_x p_X(x) N_{\mathcal{N}}(\rho^x, \bar{\rho}) && (101) \\ &= \sum_x p_X(x) N_{\mathcal{N}}(\rho^x, \psi^0) - N_{\mathcal{N}}(\bar{\rho}, \psi^0) && (102) \\ &\leq \sum_x p_X(x) N_{\mathcal{N}}(\rho^x, \psi^0). && (103) \end{aligned}$$

The inequality follows since by degradability of $\mathcal{N}$ and monotonicity of relative entropy [45], $N_{\mathcal{N}}(\rho, \sigma) \geq 0$ for all states ρ and σ. If any of the $N_{\mathcal{N}}$ quantities are infinite, the bound is trivial.

We can then argue for all $\beta > 0$,

$$\begin{aligned} \frac{P(\mathcal{N}, \beta)}{\beta} &= \frac{1}{\beta} \sup_{\substack{\{p_X, \psi^x\} \\ \mathrm{tr}[G\bar{\psi}] \leq \beta}} I(X;B) - I(X;E) && (104) \\ &\leq \frac{1}{\beta} \sup_{\substack{\{p_X, \psi^x\} \\ \mathrm{tr}[G\bar{\psi}] \leq \beta}} \sum_x p_X(x) N_{\mathcal{N}}(\psi^x, \psi^0). && (105) \end{aligned}$$

Now, just as in the entanglement-assisted case, we can restrict the supremum to be taken over positive-cost states ψ^x:

$$\begin{aligned} \frac{P(\mathcal{N}, \beta)}{\beta} &\leq \frac{1}{\beta} \sup_{\substack{\{p_X, \psi^x\} \\ \frac{1}{\beta}\mathrm{tr}[G\bar{\psi}] \leq 1}} \sum_x p_X(x) N_{\mathcal{N}}(\psi^x, \psi^0) && (106) \\ &= \sup_{\substack{\{p_X, \psi^x\} \\ \frac{1}{\beta}\mathrm{tr}[G\bar{\psi}] \leq 1}} \sum_x p_X(x) \frac{N_{\mathcal{N}}(\psi^x, \psi^0)}{\langle \psi^x | G | \psi^x \rangle} \frac{\langle \psi^x | G | \psi^x \rangle}{\beta} && (107) \\ &\leq \sup_{\psi} \frac{N_{\mathcal{N}}(\psi, \psi^0)}{\langle \psi | G | \psi \rangle}. && (108) \end{aligned}$$

This concludes the proof. □

A. Pulse-Position-Modulation Scheme for Private Communication

We now give an alternative proof of the achievability part of Theorem 13 via a PPM scheme that achieves the private capacity per unit cost for a degradable channel $\mathcal{N}_{A\to B}$.

Codebook: As discussed above, without loss of generality, we can restrict the discussion to positive-cost pure states ψ such that $N_{\mathcal{N}}(\psi, \psi^0) > 0$. Let ψ be such a state. Then, fix $M, L, N \in \mathbb{N}$. We have ML codewords labeled by (m, l) where $m \in [1:M]$ and $l \in [1:L]$. For codeword (m, l), the corresponding input quantum state is

$$\begin{aligned} &\left[\left((\psi^0)^{\otimes N}\right)^{\otimes L}\right]^{\otimes m-1} \\ &\otimes \left[\left((\psi^0)^{\otimes N}\right)^{\otimes l-1} \otimes \psi^{\otimes N} \otimes \left((\psi^0)^{\otimes N}\right)^{\otimes L-l}\right] \\ &\otimes \left[\left((\psi^0)^{\otimes N}\right)^{\otimes L}\right]^{\otimes M-m}. \end{aligned} \tag{109}$$

This can be understood as a ψ-pulse amidst a baseline of ψ^0 states, which is itself a pulse amidst a $(\psi^0)^{\otimes L}$ baseline. Note that the cost of this codeword is $N\langle \psi | G | \psi \rangle$.

Encoding: The sender transmits the message m to the receiver and uses l to obscure the message on the eavesdropper's side. Given message $m \in [1:M]$, he uniformly chooses at random $l \in [1:L]$ and transmits N times the quantum state corresponding to (m, l).

Decoding: The receiver performs ML binary quantum hypothesis tests, using N copies for each test, in order to determine the pulse position. Again this can be done with vanishing error provided that, for some $\delta > 0$,

$$\frac{\log_2(ML)}{N} < D(\mathcal{N}(\psi) \| \mathcal{N}(\psi^0)) - \delta. \tag{110}$$

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

Privacy: Given the randomization over l, the state that the eavesdropper obtains is

$$\left[\left(\mathcal{N}^c(\psi^0)^{\otimes N}\right)^{\otimes L}\right]^{\otimes m-1} \otimes \xi_L \otimes \left[\left(\mathcal{N}^c(\psi^0)^{\otimes N}\right)^{\otimes L}\right]^{\otimes M-m}, \quad (111)$$

where

$$\xi_L \equiv \frac{1}{L}\sum_{l=1}^{L}\left(\mathcal{N}^c(\psi^0)^{\otimes N}\right)^{\otimes l-1} \otimes\mathcal{N}^c(\psi)^{\otimes N} \otimes \left(\mathcal{N}^c(\psi^0)^{\otimes N}\right)^{\otimes L-l}. \quad (112)$$

Now, by a corollary to the convex-split lemma [36], the state in eq. (111) is approximately $\mathcal{N}^c(\psi^0)^{\otimes NLM}$ if L is chosen large enough. More precisely, given $\delta', \varepsilon > 0$,

$$\begin{aligned}&\frac{1}{2}\left\|\mathcal{N}^c(\psi^0)^{\otimes NL(m-1)} \otimes \xi_L \otimes \mathcal{N}^c(\psi^0)^{\otimes NL(M-m)} - \mathcal{N}^c(\psi^0)^{\otimes NLM}\right\|_1 \\ &= \frac{1}{2}\left\|\xi_L - \left(\mathcal{N}^c(\psi^0)^{\otimes N}\right)^{\otimes L}\right\|_1 \\ &\leq 2\varepsilon + \delta' \end{aligned} \quad (113)$$

if

$$L > 2^{D^{\varepsilon}_{\max}(\mathcal{N}^c(\psi)^{\otimes N}\|\mathcal{N}^c(\psi^0)^{\otimes N})}\delta'^{-2}, \quad (114)$$

where $D^{\varepsilon}_{\max}$ denotes the smooth max-relative entropy [46][1]:

$$D^{\varepsilon}_{\max}(\rho\|\sigma) \equiv \inf_{\tilde{\rho}\in B^{\varepsilon}(\rho)} D_{\max}(\tilde{\rho}\|\sigma). \quad (115)$$

Here, $B^{\varepsilon}(\rho)$ denotes the ε-ball around ρ:

$$B^{\varepsilon}(\rho) \equiv \left\{\tilde{\rho} \geq 0 : \sqrt{1 - F^2(\tilde{\rho}, \rho)} \leq \varepsilon, \mathrm{tr}[\tilde{\rho}] = 1\right\}, \quad (116)$$

where F is the quantum fidelity [47], and

$$D_{\max}(\rho\|\sigma) \equiv \log \inf\{\lambda \geq 0 : \rho \leq \lambda\sigma\}. \quad (117)$$

Hence, using the quantum asymptotic equipartition property [48] for smooth max-relative entropy, for small enough ε, all $\delta'' > 0$, and sufficiently large N, eq. (114) is satisfied if

$$L > 2^{N\left(D(\mathcal{N}^c(\psi)\|\mathcal{N}^c(\psi^0))+\delta''\right)}\delta'^{-2}. \quad (118)$$

Taking the logarithm on both sides and dividing by N, we obtain

$$\frac{\log_2 L}{N} > D(\mathcal{N}^c(\psi)\|\mathcal{N}^c(\psi^0)) + \delta'' - \frac{2\log_2 \delta'}{N}. \quad (119)$$

For large enough N, the condition becomes

$$\frac{\log_2 L}{N} > D(\mathcal{N}^c(\psi)\|\mathcal{N}^c(\psi^0)) + \delta''' \quad (120)$$

for some $\delta''' > 0$.

We conclude that we can attain arbitrarily low decoding and privacy error if

$$\frac{\log_2(ML)}{N} < D(\mathcal{N}(\psi)\|\mathcal{N}(\psi^0)) - \delta \quad (121)$$

[1]The original definition differs slightly from the definition in [36], which is the one we use here.

and

$$\frac{\log_2 L}{N} > D(\mathcal{N}^c(\psi)\|\mathcal{N}^c(\psi^0)) + \delta'''. \quad (122)$$

Combining the two inequalities, we obtain

$$\frac{\log_2 M}{N\langle\psi|G|\psi\rangle} < \frac{N_{\mathcal{N}}(\psi, \psi^0)}{\langle\psi|G|\psi\rangle} - \frac{\delta + \delta'''}{\langle\psi|G|\psi\rangle}. \quad (123)$$

Hence, we can achieve a private rate per unit cost of $\frac{N_{\mathcal{N}}(\psi,\psi^0)}{\langle\psi|G|\psi\rangle}$.

Note that the above protocol does not use the fact that the channel is degradable. Hence, this gives an achievability result for non-degradable quantum channels as well. Furthermore, we can achieve this with a mixed state ρ instead of a pure state ψ, which might be necessary for non-degradable channels. We conclude for general quantum channels $\mathcal{N}$,

$$\boldsymbol{P}(\mathcal{N}) \geq \sup_{\rho\in\mathcal{S}(\mathcal{H}_A)} \boldsymbol{P}_{\psi^0}(\mathcal{N}, \rho). \quad (124)$$

VI. Quantum Communication

We now formulate the quantum capacity per unit cost. Quantum capacity was first studied in [39] and [49]–[53] when there is no cost constraint and recently in [41] when there is a cost constraint. Let $\mathcal{N}_{A\to B}$ be a quantum channel, and let $n, Q \in \mathbb{N}$, $\nu \in \mathbb{R}_{>0}$, and $\varepsilon \in [0, 1]$. An (n, Q, ν, ε) quantum code has blocklength n, dimension Q for the total input space, total cost at most ν, and quantum decoding error at most ε. In more detail, an (n, Q, ν, ε) code for quantum communication consists of an encoding channel $\mathcal{E}^n : \mathcal{S}(\mathcal{H}_S) \to \mathcal{S}(\mathcal{H}_A^{\otimes n})$ and a decoding channel $\mathcal{D}^n : \mathcal{S}(\mathcal{H}_B^{\otimes n}) \to \mathcal{S}(\mathcal{H}_S)$, where $\dim(\mathcal{H}_S) = Q$. The cost constraint imposes the following bound on all states resulting from the output of the encoding channel $\mathcal{E}^n$:

$$\mathrm{Tr}\left\{G_n\mathcal{E}^n(\rho_S)\right\} \leq \nu, \quad (125)$$

where $\rho_S \in \mathcal{S}(\mathcal{H}_S)$ and G_n is defined in eq. (1). Finally, we have the error bounded by ε, in the sense that for all pure states $\phi_{RS} \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_S)$, where $\mathcal{H}_R$ is isomorphic to $\mathcal{H}_S$, the following trace distance bound holds:

$$\frac{1}{2}\left\|\phi_{RS} - (\mathrm{id}_R \otimes[\mathcal{D}^n \circ \mathcal{N}^{\otimes n} \circ \mathcal{E}^n])(\phi_{RS})\right\|_1 \leq \varepsilon. \quad (126)$$

Definition 14: Given $\beta > 0$, R_q is an achievable quantum communication rate with average cost not exceeding β if for all $\varepsilon \in (0, 1)$ and $\delta > 0$, $\exists n_0$ such that for $n \geq n_0$, $\exists$ an $(n, Q, n\beta, \varepsilon)$ code for which

$$\frac{\log_2 Q}{n} > R_q - \delta. \quad (127)$$

The quantum capacity cost function $Q(\mathcal{N}, \beta)$ is equal to the supremum of all achievable quantum communication rates with average cost not exceeding β.

Building on [54], the expression for $Q(\mathcal{N}, \beta)$ when $\mathcal{N}$ is degradable was shown in [41] to be the following.

Theorem 15 [41]: The quantum capacity cost function for a degradable channel $\mathcal{N}_{A\to B}$ is given by

$$Q(\mathcal{N}, \beta) = \sup_{\substack{\varphi_{RA} \\ \mathrm{tr}[G\varphi_A]\leq\beta}} I(R\rangle B)_{\varphi}, \quad (128)$$

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

where $I(R\rangle B) \equiv S(B) - S(RB)$ is the coherent information [49] and

$$\varphi_{RB} \equiv (\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(\varphi_{RA}). \tag{129}$$

We then define the quantum capacity per unit cost.

Definition 16: $\boldsymbol{R}_q$ is an achievable quantum communication rate per unit cost if for any $\delta, \varepsilon > 0$, $\exists \nu_0 > 0$ such that for $\nu \geq \nu_0$ there is an (n, Q, ν, ε) code for which

$$\log_2 Q > \nu(\boldsymbol{R}_q - \delta). \tag{130}$$

The quantum capacity per unit cost is then defined to be the supremum of all achievable quantum communication rates per unit cost and is denoted as $\boldsymbol{Q}(\mathcal{N})$.

Using the achievability and converse proofs for $Q(\mathcal{N}, \beta)$, and reasoning similar to that in the proof of Theorem 4, we obtain the following expressions for $\boldsymbol{Q}(\mathcal{N})$.

Theorem 17: The quantum capacity per unit cost for a degradable channel $\mathcal{N}_{A\to B}$ is given by

$$\boldsymbol{Q}(\mathcal{N}) = \sup_{\beta>0} \frac{Q(\mathcal{N}, \beta)}{\beta} = \sup_{\varphi_{RA}} \frac{I(R\rangle B)_\varphi}{\mathrm{tr}[G\varphi_A]}. \tag{131}$$

However, note that since $Q(\mathcal{N}, \beta) = P(\mathcal{N}, \beta)$ [41], [55] for degradable channels, in this case the quantum capacity per unit cost is equal to the private capacity per unit cost. In particular, if a zero-cost state exists, then the quantum capacity per unit cost of a degradable channel is given by the expression in Theorem 13.

A. Pulse-Position-Modulation Scheme for Quantum Communication

We propose a PPM scheme for achieving the quantum capacity per unit cost for a degradable channel $\mathcal{N}_{A\to B}$. We do this by operating the PPM scheme for private communication in a coherent fashion analogous to that of [39]. Since the approach is so similar (yet tailored to a PPM coding scheme), we merely sketch the proof for simplicity and point to [39] for more details (see also [56] in this context). The task we consider is entanglement generation, in which the goal is to establish a maximally entangled state between the sender and receiver. To generalize this to arbitrary quantum states, we again point to [39]. Let $\mathcal{U}_{A\to BE}$ be an isometric channel extending $\mathcal{N}_{A\to B}$ and let $U_{A\to BE}$ denote the corresponding isometry. Let ψ^0 be a zero-cost pure state and ψ a positive-cost pure state for which $N_{\mathcal{N}}(\psi, \psi^0) > 0$.

We first consider the case in which ψ is orthogonal to ψ^0.

Codebook: As in the private PPM scheme, we fix $M, L, N \in \mathbb{N}$. For each ordered pair (m, l), where $m \in [1 : M]$ and $l \in [1 : L]$, consider the following pure quantum state:

$$\begin{aligned}\psi^{m,l} \equiv & \left[\left((\psi^0)^{\otimes N}\right)^{\otimes L}\right]^{\otimes m-1} \\ & \otimes \left[\left((\psi^0)^{\otimes N}\right)^{\otimes l-1} \otimes \psi^{\otimes N} \otimes \left((\psi^0)^{\otimes N}\right)^{\otimes L-l}\right] \\ & \otimes \left[\left((\psi^0)^{\otimes N}\right)^{\otimes L}\right]^{\otimes M-m}.\end{aligned} \tag{132}$$

Note that since ψ is orthogonal to ψ^0, $\psi^{m,l}$ are orthogonal for different m, l. Observe also that since $G\,|\psi^0\rangle = 0$,

$$G_K\,|\psi^{m,l}\rangle_{A^K} = \sum_{j=n(m,l)}^{n(m,l)+N-1} \left(I^{\otimes j-1} \otimes G \otimes I^{\otimes K-j}\right) |\psi^{m,l}\rangle_{A^K}\,, \tag{133}$$

where $K \equiv NML$ and $n(m,l) \equiv NL(m-1) + N(l-1) + 1$ is the position of the first ψ state in $\psi^{m,l}$.

Encoding: Let $|\Phi\rangle_{R\hat{A}}$ denote the maximally entangled state to be established with the receiver, where the dimension of $\hat{A}$, the system the sender is to transmit, is at most M. We can decompose the state with respect to some orthonormal bases $\{|m\rangle_R\}$ and $\{|m\rangle_{\hat{A}}\}$:

$$|\Phi\rangle_{R\hat{A}} = \frac{1}{\sqrt{M}} \sum_m |m\rangle_R\,|m\rangle_{\hat{A}}\,. \tag{134}$$

Depending on the value of m, the sender coherently prepares a uniform superposition of $|\psi^{m,l}\rangle$ over the l variable. That is, the mapping is given by

$$|m\rangle_{\hat{A}} \mapsto \frac{1}{\sqrt{L}} \sum_{l=1}^{L} |\psi^{m,l}\rangle_{A^K}\,. \tag{135}$$

Since $\psi^{m,l}$ are orthogonal for different m, l, the above mapping is an isometry. The overall state after the encoding is

$$|\Psi\rangle_{RA^K} = \frac{1}{\sqrt{ML}} \sum_{m,l} |m\rangle_R\,|\psi^{m,l}\rangle_{A^K}\,. \tag{136}$$

Note that the reduced state on A^K is

$$\Psi_{A^K} = \frac{1}{ML} \sum_{m,l,l'} |\psi^{m,l}\rangle\langle\psi^{m,l'}|_{A^K} \tag{137}$$

and therefore has cost $N\langle\psi|\,G\,|\psi\rangle$ by eq. (133).

Decoding: After K uses of the isometric extension, the overall state is

$$|\Psi\rangle_{RB^KE^K} = \frac{1}{\sqrt{ML}} \sum_{m,l} |m\rangle_R\,|\psi^{m,l}\rangle_{B^KE^K}\,, \tag{138}$$

where $|\psi^{m,l}\rangle_{B^KE^K} \equiv U_{A\to BE}^{\otimes K}\,|\psi^{m,l}\rangle_{A^K}$. Let $\{\Lambda^{m,l}_{B^K}\}_{m,l}$ denote the POVM used as a decoder in the private communication protocol. A coherent version of this measurement is given by the isometry $V_{B^K\to B^K\hat{B}_0\hat{B}_1} = \sum_{m,l} \sqrt{\Lambda^{m,l}_{B^K}} \otimes |m\rangle_{\hat{B}_0} \otimes |l\rangle_{\hat{B}_1}$, and after performing it, the resulting state is approximately equal to the following one:

$$|\Psi\rangle_{RB^KE^K\hat{B}_0\hat{B}_1} = \frac{1}{\sqrt{ML}} \sum_{m,l} |m\rangle_R\,|\psi^{m,l}\rangle_{B^KE^K}\,|m\rangle_{\hat{B}_0}|l\rangle_{\hat{B}_1}. \tag{139}$$

At this point, we know from the privacy condition for the private code, that for each m, the following approximation holds: $\frac{1}{L}\sum_l \psi^{m,l}_{E^K} \approx \mathcal{N}^c(\psi^0)^{\otimes K}$. Thus, given m, the eavesdropper's system is approximately independent of m. By Uhlmann's theorem [47], for each m, there exists an isometry $W^m_{B^K\hat{B}_1\to\hat{B}_2}$ such that

$$W^m_{B^K\hat{B}_1\to\hat{B}_2}\left[\frac{1}{\sqrt{L}} \sum_l |\psi^{m,l}\rangle_{B^KE^K}\,|l\rangle_{\hat{B}_1}\right] \approx |\varsigma\rangle_{E^K\hat{B}_2}, \tag{140}$$

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

where $|\varsigma\rangle_{E^K\hat{B}_2}$ is some state independent of m. So this means that the receiver can perform the controlled isometry $\sum_m |m\rangle\langle m|_{\hat{B}_0} \otimes W^m_{B^K\hat{B}_1\to\hat{B}_2}$, and the resulting state is approximately close to the following state:

$$\frac{1}{\sqrt{M}}\sum_m |m\rangle_R\,|m\rangle_{\hat{B}_0} \otimes |\varsigma\rangle_{E^K\hat{B}_2}. \tag{141}$$

By the properties of the PPM scheme for private communication, the quantum rate per unit cost of this scheme is equal to $N_{\mathcal{N}}(\psi,\psi^0)/\langle\psi|\,G\,|\psi\rangle$.

Now, if ψ is not orthogonal to ψ^0, we implement the above protocol but replacing $\psi^{\otimes N}$ with its normalized rejection from $(\psi^0)^{\otimes N}$. That is, we take the component of $|\psi\rangle^{\otimes N}$ orthogonal to $|\psi^0\rangle^{\otimes N}$ and normalize it. Calling this $\psi^{\perp}_{A^N}$, we have

$$|\psi^\perp\rangle = \frac{1}{\sqrt{1-\left|\langle\psi^0|\psi\rangle\right|^{2N}}}\left(|\psi\rangle^{\otimes N} - \langle\psi^0|\psi\rangle^N\,|\psi^0\rangle^{\otimes N}\right), \tag{142}$$

and so

$$\frac{1}{2}\left\|\psi^\perp_{A^N} - \left(\psi^{\otimes N}\right)_{A^N}\right\|_1 = \left|\langle\psi^0|\psi\rangle\right|^N \equiv \delta_N. \tag{143}$$

By monotonicity, the trace distance is at most δ_N after N uses of $\mathcal{N}$ or $\mathcal{N}^c$. Hence, since ψ is positive-cost and so $\left|\langle\psi^0|\psi\rangle\right| < 1$, by using $\psi^\perp$ we expect to obtain the desired rate in the limit of large N. Indeed, since $\psi^\perp$ is orthogonal to $(\psi^0)^{\otimes N}$, we can implement the above protocol and achieve a quantum rate per unit cost

$$\Big[D^\varepsilon_H\left(\mathcal{N}^{\otimes N}(\psi^\perp)\|\mathcal{N}(\psi^0)^{\otimes N}\right) - D^{\varepsilon'}_{\max}\left((\mathcal{N}^c)^{\otimes N}(\psi^\perp)\|\mathcal{N}^c(\psi^0)^{\otimes N}\right)\Big]/\left(\langle\psi^\perp|\,G_N\,|\psi^\perp\rangle\right) \tag{144}$$

for any $\varepsilon,\varepsilon' > 0$, where D^ε_H is the hypothesis testing relative entropy [57], [58]:

$$D^\varepsilon_H(\rho\|\sigma) \equiv -\log_2 \inf_{\substack{0\le\Lambda\le I\\ \mathrm{tr}[\Lambda\rho]\ge 1-\varepsilon}} \mathrm{tr}[\Lambda\sigma]. \tag{145}$$

Note that this is simply the negative logarithm of the quantity defined in eq. (6). For sufficiently large N, we have that $\delta_N < \varepsilon$. Then, by [59, Lemma 7],

$$\begin{aligned} D^\varepsilon_H&\left(\mathcal{N}^{\otimes N}(\psi^\perp)\|\mathcal{N}(\psi^0)^{\otimes N}\right)\\ &\ge D^{\varepsilon-\delta_N}_H(\mathcal{N}(\psi)^{\otimes N}\|\mathcal{N}(\psi^0)^{\otimes N}) &(146)\\ &\ge D^{\delta(\varepsilon)}_H(\mathcal{N}(\psi)^{\otimes N}\|\mathcal{N}(\psi^0)^{\otimes N}), &(147)\end{aligned}$$

where $\delta(\varepsilon) = \varepsilon - \delta_{N(\varepsilon)}$ and $N(\varepsilon)$ is the smallest integer such that $\delta_{N(\varepsilon)} < \varepsilon$. Furthermore, by the definition of smooth max-relative entropy in eq. (115) and the triangle inequality, for sufficiently large N such that $\delta_N < \varepsilon'$, we have

$$\begin{aligned} D^{\varepsilon'}_{\max}&((\mathcal{N}^c)^{\otimes N}(\psi^\perp)\|\mathcal{N}^c(\psi^0)^{\otimes N})\\ &\le D^{\varepsilon'-\delta_N}_{\max}(\mathcal{N}^c(\psi)^{\otimes N}\|\mathcal{N}^c(\psi^0)^{\otimes N}) &(148)\\ &\le D^{\delta(\varepsilon')}_{\max}(\mathcal{N}^c(\psi)^{\otimes N}\|\mathcal{N}^c(\psi^0)^{\otimes N}). &(149)\end{aligned}$$

Lastly,

$$\begin{aligned}\langle\psi^\perp|\,G_N\,|\psi^\perp\rangle &= \frac{1}{1-\left|\langle\psi^0|\psi\rangle\right|^{2N}}\langle\psi|^{\otimes N}\,G_N\,|\psi\rangle^{\otimes N} &(150)\\ &= \frac{N\langle\psi|\,G\,|\psi\rangle}{1-\left|\langle\psi^0|\psi\rangle\right|^{2N}}. &(151)\end{aligned}$$

We conclude that we can achieve

$$\left(1-\left|\langle\psi^0|\psi\rangle\right|^{2N}\right)\Big[D^{\delta(\varepsilon)}_H(\mathcal{N}(\psi)^{\otimes N}\|\mathcal{N}(\psi^0)^{\otimes N}) - D^{\delta(\varepsilon')}_{\max}(\mathcal{N}^c(\psi)^{\otimes N}\|\mathcal{N}^c(\psi^0)^{\otimes N})\Big]/\left(N\langle\psi|\,G\,|\psi\rangle\right). \tag{152}$$

By Quantum Stein's Lemma (eq. (7)) and the quantum asymptotic equipartition property for smooth max-relative entropy, in the limit of large N we can therefore achieve a quantum rate per unit cost of $\frac{N_{\mathcal{N}}(\psi,\psi^0)}{\langle\psi|G|\psi\rangle}$.

Note that just like in the private case, this scheme gives achievability for non-degradable channels as well.

VII. Capacities per Unit Cost of Quantum Gaussian Channels

By the methods developed and used in [16], [17], [25], and [41], we can generalize the above results to infinite dimensions, in particular for quantum Gaussian channels. We will use the formulas derived above to compute various capacities per unit cost for specific Gaussian channels, where the cost observable is the photon number operator $\hat{n} = \sum_{n=0}^\infty n|n\rangle\langle n|$, with $|n\rangle$ being a photon number state. Since the channels we consider already have known capacity cost functions, it is easiest for us to compute the capacity per unit cost via the following formula:

$$\boldsymbol{C}(\mathcal{N}) = \lim_{\bar{n}\to 0}\frac{C(\mathcal{N},\bar{n})}{\bar{n}}. \tag{153}$$

Note that we could also compute the capacities per unit cost using the optimized relative entropy formulas that we obtained in the previous sections.

The quantum Gaussian channels we consider are the following [28], [60], [61]. The thermal channel $\mathcal{E}^{n_{\text{th}}}_\eta$ with transmissivity $\eta \in (0,1)$ and thermal photon number $n_{\text{th}} \in \mathbb{R}_{>0}$ is a Gaussian channel which mixes the input signal with a thermal Gaussian state. This is summarized by the following Heisenberg evolution:

$$a_{\text{in}} \mapsto \sqrt{\eta}a_{\text{in}} + \sqrt{1-\eta}a_{\text{th}}, \tag{154}$$

where a_{in}, a_{th} are the annihilation operators for the input and thermal modes, respectively. We also consider the additive classical noise channel $\mathcal{N}_N$ with variance $N \in \mathbb{R}_{>0}$, which describes classical noise that displaces the signal in phase space according to a Gaussian distribution. The Heisenberg evolution is

$$a_{\text{in}} \mapsto a_{\text{in}} + \xi, \tag{155}$$

where ξ is a complex normal random variable with mean zero and variance N. Next, the amplifier channel $\mathcal{A}^{n_{\text{th}}}_\kappa$ with gain parameter $\kappa > 1$ and thermal photon number $n_{\text{th}} \in \mathbb{R}_{>0}$ describes the effect of a two-mode squeezing Hamiltonian that

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

acts on the input mode and a thermal mode. This effectively amplifies the input signal but at the cost of adding noise. The resulting Heisenberg evolution is given by

$$a_{\text{in}} \mapsto \sqrt{\kappa} a_{\text{in}} + \sqrt{\kappa - 1} a_{\text{th}}^{\dagger}. \tag{156}$$

Lastly, we also look at the weak conjugate of the amplifier channel, the contravariant amplifier $\tilde{\mathcal{A}}_{\kappa}^{n_{\text{th}}}$ with gain parameter $\kappa > 1$, and thermal photon number $n_{\text{th}} \in \mathbb{R}_{>0}$.

A. Classical Communication Over Gaussian Channels

We compute the unassisted classical capacities per unit cost for these four channels. For the thermal channel, the classical capacity cost function is given by [27], [28]

$$C(\mathcal{E}_{\eta}^{n_{\text{th}}}, \bar{n}) = g(\eta \bar{n} + (1-\eta) n_{\text{th}}) - g((1-\eta) n_{\text{th}}), \tag{157}$$

where

$$g(x) \equiv (x+1)\log_2(x+1) - x \log_2 x. \tag{158}$$

Hence, by applying eq. (153), we find the following:

$$\boldsymbol{C}(\mathcal{E}_{\eta}^{n_{\text{th}}}) = \eta \log_2\left(1 + \frac{1}{n_{\text{th}}(1-\eta)}\right). \tag{159}$$

Now, consider the additive-noise channel, which has the following classical capacity cost function [27], [28]

$$C(\mathcal{N}_N, \bar{n}) = g(\bar{n} + N) - g(N). \tag{160}$$

Hence,

$$\boldsymbol{C}(\mathcal{N}_N) = \log_2\left(1 + \frac{1}{N}\right). \tag{161}$$

Next, we consider the amplifier channel, which has a classical capacity cost function [27], [28]

$$C(\mathcal{A}_{\kappa}^{n_{\text{th}}}, \bar{n}) = g(\kappa \bar{n} + (\kappa - 1)(n_{\text{th}} + 1)) - g((\kappa - 1)(n_{\text{th}} + 1)). \tag{162}$$

We find

$$\boldsymbol{C}(\mathcal{A}_{\kappa}^{n_{\text{th}}}) = \kappa \log_2\left(1 + \frac{1}{(\kappa-1)(n_{\text{th}}+1)}\right). \tag{163}$$

Finally, for the contravariant amplifier channel, which has the capacity cost function [28]

$$C(\tilde{\mathcal{A}}_{\kappa}^{n_{\text{th}}}, \bar{n}) = g(\kappa n_{\text{th}} + (\kappa - 1)(\bar{n} + 1)) - g(\kappa(n_{\text{th}} + 1) - 1), \tag{164}$$

we have

$$\boldsymbol{C}(\tilde{\mathcal{A}}_{\kappa}^{n_{\text{th}}}) = (\kappa - 1)\log_2\left(1 + \frac{1}{\kappa(n_{\text{th}}+1) - 1}\right). \tag{165}$$

Note that given eq. (38) and the achievability result in Theorem 4, when a zero-cost state exists, we can achieve the capacity per unit cost with any code that achieves the cost-constrained capacity in the limit of zero cost. For example, for the pure-loss bosonic channel, single-photon-detection achieves the classical capacity in the limit $\bar{n} \to 0$ [62]. In general, we can achieve the capacity per unit cost with any code that achieves $C(\beta_{\max})$ where $\beta_{\max} = \arg\sup_{\beta>0} C(\beta)/\beta$.

B. Entanglement-Assisted Communication Over Gaussian Channels

We now compute the entanglement-assisted capacity per unit cost for the first three channels. For the thermal channel, the entanglement-assisted capacity cost function is given by [61], [63]

$$\begin{aligned} C_{\text{EA}}(\mathcal{E}_{\eta}^{n_{\text{th}}}, \bar{n}) &= g(\bar{n}) + g(\eta\bar{n} + (1-\eta)n_{\text{th}}) \\ &\quad - g\Big(\frac{1}{2}\Big(\sqrt{((1+\eta)\bar{n} + (1-\eta)n_{\text{th}} + 1)^2 - 4\eta\bar{n}(\bar{n}+1)} \\ &\qquad - (1-\eta)(\bar{n} - n_{\text{th}}) - 1\Big)\Big) \\ &\quad - g\Big(\frac{1}{2}\Big(\sqrt{((1+\eta)\bar{n} + (1-\eta)n_{\text{th}} + 1)^2 - 4\eta\bar{n}(\bar{n}+1)} \\ &\qquad + (1-\eta)(\bar{n} - n_{\text{th}}) - 1\Big)\Big). \end{aligned} \tag{166}$$

We compute the limit as per eq. (153) and find that the entanglement-assisted capacity per unit cost of the thermal channel diverges.[2] For the additive noise channel, the entanglement-assisted capacity cost function is [61], [63]

$$\begin{aligned} C_{\text{EA}}(\mathcal{N}_N, \bar{n}) &= g(\bar{n}) + g(\bar{n} + N) - g\left(\frac{1}{2}\left(\sqrt{(N+1)^2 + 4N\bar{n}} - N - 1\right)\right) \\ &\quad - g\left(\frac{1}{2}\left(\sqrt{(N+1)^2 + 4N\bar{n}} + N - 1\right)\right), \end{aligned} \tag{167}$$

which also gives an infinite capacity per unit cost. Lastly, for the amplifier channel,

$$\begin{aligned} C_{\text{EA}}(\mathcal{A}_{\kappa}^{n_{\text{th}}}, \bar{n}) &= g(\bar{n}) + g(\kappa\bar{n} + (\kappa-1)(n_{\text{th}}+1)) \\ &\quad - g\Big(\frac{1}{2}\Big(\sqrt{((\kappa+1)\bar{n} + (\kappa-1)(n_{\text{th}}+1) + 1)^2 - 4\kappa\bar{n}(\bar{n}+1)} \\ &\qquad - (\kappa-1)(\bar{n} + n_{\text{th}} + 1) - 1\Big)\Big) \\ &\quad - g\Big(\frac{1}{2}\Big(\sqrt{((\kappa+1)\bar{n} + (\kappa-1)(n_{\text{th}}+1) + 1)^2 - 4\kappa\bar{n}(\bar{n}+1)} \\ &\qquad + (\kappa-1)(\bar{n} + n_{\text{th}} + 1) - 1\Big)\Big). \end{aligned} \tag{168}$$

Computing the ratio again gives an infinite value as $\bar{n} \to 0$.

We show the divergence of $\boldsymbol{C}_{\text{EA}}$ by plotting the bits per photon against the number of photons for these three Gaussian channels in fig. 1. It is likely that the divergences for these Gaussian channels appear since we are allowing for an unbounded amount of entanglement assistance per unit cost. However, it is not true that this potentially infinite entanglement assistance always leads to divergences. Trivial examples include channels where $C_{\text{EA}}(\mathcal{N}, \beta) = 0$ for all β and when the cost observable is positive definite. We can also find examples using the fact that entanglement assistance sometimes does not help. Take for instance the state preparation qubit channel

$$\mathcal{N}_s : \rho \mapsto \langle 0| \rho |0\rangle \rho^0 + \langle 1| \rho |1\rangle \rho^1 \tag{169}$$

with cost observable $G = |1\rangle\langle 1|$, where $\rho^0, \rho^1 \in \mathcal{S}(\mathcal{H}_{A'})$ such that $0 < D(\rho^1 \| \rho^0) < \infty$. By Proposition 4 in [64],

[2]For many of these calculations, see the Mathematica file included in arXiv posting.

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

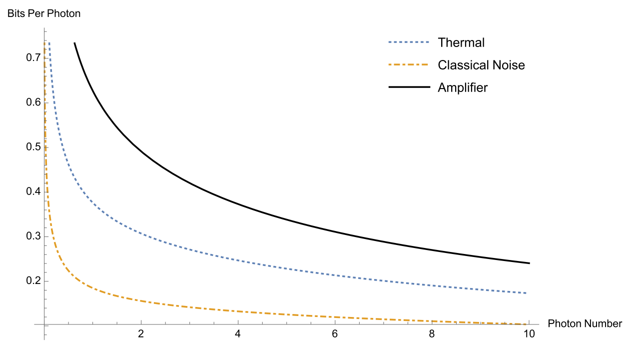


Fig. 1. The figure illustrates the divergence of $C_{\text{EA}}(\mathcal{N}, \bar{n})/\bar{n}$ as $\bar{n} \to 0$. For the thermal channel we set $n_{\text{th}} = 10$, $\eta = 0.7$, for the classical noise channel $N = 10$, and for the amplifier channel $n_{\text{th}} = 10$, $\kappa = 1.3$.

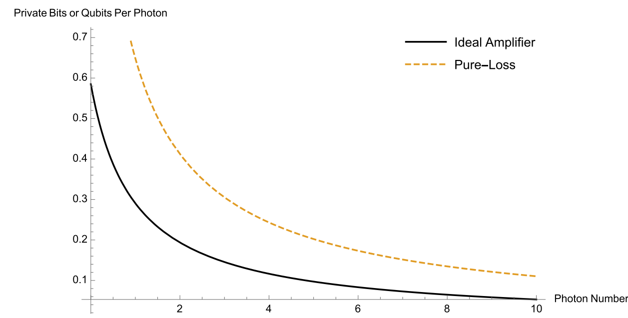


Fig. 2. Plot of $P(\mathcal{N}, \bar{n})/\bar{n} = Q(\mathcal{N}, \bar{n})/\bar{n}$ versus $\bar{n}$. For the ideal amplifier we set $\kappa = 3$ and for the pure-loss channel $\eta = 0.7$.

$C_{\text{EA}}(\mathcal{N}_s, \beta) = C(\mathcal{N}_s, \beta)$ for all β. Now, we have a zero-cost state $|0\rangle\langle 0|$, so we can use Theorem 5:

$$\begin{aligned}
\boldsymbol{C}(\mathcal{N}_s) &= \sup_{\psi \neq |0\rangle\langle 0|} \frac{D(\mathcal{N}_s(\psi) \| \mathcal{N}_s(|0\rangle\langle 0|))}{\langle \psi | G | \psi \rangle} && (170)\\
&= \sup_{\psi \neq |0\rangle\langle 0|} \frac{D\left(|c_0|^2 \rho^0 + |c_1|^2 \rho^1 \| \rho^0\right)}{|c_1|^2} && (171)\\
&\leq \sup_{\psi \neq |0\rangle\langle 0|} \frac{1}{|c_1|^2} \left(|c_0|^2 D(\rho^0 \| \rho^0) + |c_1|^2 D(\rho^1 \| \rho^0)\right) && (172)\\
&= D(\rho^1 \| \rho^0) && (173)\\
&< \infty, && (174)
\end{aligned}$$

where $|\psi\rangle \equiv c_0 |0\rangle + c_1 |1\rangle$ and we can divide by $|c_1|^2$ since $\psi \neq |0\rangle\langle 0|$. The inequality follows from the convexity of the relative entropy in the first argument. We conclude $\boldsymbol{C}_{\text{EA}}(\mathcal{N}_s) = \boldsymbol{C}(\mathcal{N}_s) < \infty$. However, since $D(\rho^1 \| \rho^0) > 0$, this channel clearly has a non-zero $C(\mathcal{N}_s, \beta)$ and so non-zero $C_{\text{EA}}(\mathcal{N}_s, \beta)$. It is an interesting open question to find an explicit nontrivial channel for which there is a gain from entanglement assistance but $\boldsymbol{C}_{\text{EA}}$ is finite.

C. Private and Quantum Communication Over Gaussian Channels

We next compute the private and quantum capacities per unit cost for degradable Gaussian channels. In particular, we consider ideal amplifiers $\mathcal{A}_\kappa^0$ and pure-loss channels $\mathcal{E}_\eta^0$ for $\eta \geq 1/2$. For the former, we have the capacity cost function [41]

$$P(\mathcal{A}_\kappa^0, \bar{n}) = Q(\mathcal{A}_\kappa^0, \bar{n}) = g(\kappa(\bar{n}+1) - 1) - g((\kappa - 1)(\bar{n} + 1)). \quad (175)$$

Hence,

$$\boldsymbol{P}(\mathcal{A}_\kappa^0) = \boldsymbol{Q}(\mathcal{A}_\kappa^0) = \log_2\left(\frac{\kappa}{\kappa - 1}\right), \quad (176)$$

which demonstrates that the quantum and private capacity per unit cost are equal to the unconstrained quantum and private capacity of the ideal amplifier channel [41], [65]. Finally, for the pure-loss channel, we have that [41]

$$P(\mathcal{E}_\eta^0, \bar{n}) = Q(\mathcal{E}_\eta^0, \bar{n}) = g(\eta\bar{n}) - g((1 - \eta)\bar{n}). \quad (177)$$

We divide by $\bar{n}$ and find the following divergent term for $\eta > 1/2$ as $\bar{n} \to 0$:

$$(2\eta - 1) \log_2(1/\bar{n}). \quad (178)$$

Hence, the pure-loss channel for $\eta > 1/2$ has an infinite private and quantum capacity per unit cost, while for $\eta \leq 1/2$ the capacities per unit cost are zero since the channel is antidegradable in this regime. In fig. 2 we plot the private bits or qubits per photon against the number of photons for these two channels.

Another interesting communication setting that we can consider is that of private and quantum communication assisted by a side classical communication channel, their corresponding cost-constrained capacities denoted by $P_2(\mathcal{N}, \beta)$ and $Q_2(\mathcal{N}, \beta)$, for which a general theory has been developed recently in [66]. Just as for the other communication settings considered in this paper, we could trivially take an achievability result for the cost-constrained capacity to obtain one for the capacity per unit cost. For something less trivial, we can consider the example of the pure-loss bosonic channel, for which it is known [67] that $\lim_{\bar{n} \to \infty} P_2(\mathcal{E}_\eta^0, \bar{n})$, $Q_2(\mathcal{E}_\eta^0, \bar{n})$ is finite. This is a pessimistic result which can be interpreted to imply that the rate of quantum key distribution over a fiber-optic cable is finite even if one uses arbitrarily high input energy. However, the situation is different for capacity per unit cost.

Previously we calculated that the unassisted private and quantum capacities per unit cost of this channel are infinite, and since these trivially lower bound the two-way assisted capacities, we conclude that $\boldsymbol{P}_2(\mathcal{E}_\eta^0), \boldsymbol{Q}_2(\mathcal{E}_\eta^0)$ are infinite.

The situation for these capacities per unit cost for the quantum-limited amplifier channel $\mathcal{A}_\kappa^0$ of gain $\kappa > 1$ is more interesting. In this case, we can use the following upper bound from [68] (see also [66, Remark 3])

$$\begin{aligned}
P_2(\mathcal{A}_\kappa^0, \bar{n}) &\leq E_{\text{sq}}(\mathcal{A}_\kappa^0, \bar{n})\\
&\leq g((1+\kappa)\bar{n}/2 + (\kappa - 1)/2) - g((\kappa - 1)(\bar{n}+1)/2).
\end{aligned} \quad (179)$$

where $E_{\text{sq}}(\mathcal{A}_\kappa^0, \bar{n})$ denotes the energy-constrained squashed entanglement of the channel [66]. This was used to show that the private capacity in the limit of infinite photon number is finite. For this channel this is true for the private capacity per

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

unit cost as well:

$$\boldsymbol{P}_2(\mathcal{A}_\kappa^0) = \lim_{\bar{n}\to 0} \frac{P_2(\mathcal{A}_\kappa^0, \bar{n})}{\bar{n}} \tag{180}$$
$$\leq \lim_{\bar{n}\to 0} \frac{g((1+\kappa)\bar{n}/2 + (\kappa-1)/2) - g((\kappa-1)(\bar{n}+1)/2)}{\bar{n}} \tag{181}$$
$$= \log_2\left(\frac{\kappa+1}{\kappa-1}\right). \tag{182}$$

Note that without any improved upper bounds on $P_2(\mathcal{A}_\kappa^0, \bar{n})$, there thus remains a gap between the lower bound from eq. (176) and the upper bound given above. Also, since private capacity bounds quantum capacity from above, the same conclusions follow for the quantum capacity.

VIII. Blocklength-Constrained Capacity per Unit Cost

In section VII, we find many infinite capacities per unit cost. Although we are able to ascribe these infinities to unphysical assumptions such as unbounded entanglement assistance, we can alternatively ascribe almost any infinite capacity per unit cost to the *absence of a time constraint*. The key is to notice that although Theorem 3 is very similar to Theorem 1, there is a significant asymmetry: while the latter has a constraint on the cost divided by blocklength, the former does not have an analogous constraint. Indeed, infinite capacities is not a new phenomenon: it was encountered in the study of continuous variable channels, which was part of the motivation of studying cost constraints in the first place. Hence, *just as cost constraints tamed infinite capacities for continuous variable channels, we likewise expect that blocklength constraints would tame infinite capacities per unit cost*.

Indeed, we can show that the former implies the latter. We first define the blocklength-constrained capacity per unit cost. For concreteness, we state everything in the unassisted classical communication setting.

Definition 18: A non-negative number $\boldsymbol{R}$ *is an achievable rate per unit cost with blocklength constraint* $\alpha \in \mathbb{R}_{>0}$ *if for every* $\varepsilon \in (0,1), \delta > 0$, $\exists \nu_0 > 0$ *such that if* $\nu \geq \nu_0$, $\exists$ *an* (n, M, ν, ε) *code such that* $\log_2 M > \nu(\boldsymbol{R} - \delta)$ *and* $n \leq \nu\alpha$. *The capacity per unit cost with blocklength constraint* α *is the supremum of all achievable rates per unit cost with constraint* α*, denoted as* $\boldsymbol{C}(\mathcal{N}, \alpha)$.

Conveniently, we can show that $\boldsymbol{C}(\mathcal{N}, \alpha)$ has a characterization similar to that of $\boldsymbol{C}(\mathcal{N})$. The proof of this theorem uses results from the proof of Theorem 4 and that of the corollary in [14].

Theorem 19: For blocklength constraint $\alpha > 0$*, the blocklength-constrained capacity per unit cost of a quantum channel* $\mathcal{N}$ *is given by*

$$\boldsymbol{C}(\mathcal{N}, \alpha) = \sup_{\beta \geq \frac{1}{\alpha}} \frac{C(\mathcal{N}, \beta)}{\beta}. \tag{183}$$

Proof: We first show achievability. Let $\beta > 0$. By definition, we can achieve a rate $C(\mathcal{N}, \beta)$ with cost β.

Let $\varepsilon \in (0,1), \delta > 0$. Then, using the direct part in the proof of Theorem 4, $\exists \nu_0$ such that for $\nu \geq \nu_0$ we can find an (n, M, ν, ε) code where

$$\frac{\log_2 M}{\nu} > \frac{C(\mathcal{N}, \beta)}{\beta} - \delta \tag{184}$$

and

$$n \leq \frac{\nu}{\beta}. \tag{185}$$

Hence, for $\beta \geq 1/\alpha$, we achieve a rate per unit cost $C(\mathcal{N}, \beta)/\beta$ with blocklength constraint $\frac{1}{\beta} \leq \alpha$.

We now show the converse. We claim that if we can achieve a rate per unit cost $\boldsymbol{R}$ with blocklength constraint α, then we can achieve a rate $\boldsymbol{R}/\alpha$ at cost $1/\alpha$.

To see this, let $\varepsilon \in (0,1), \delta > 0$. Then, by Theorem 18, there exists ν_0 such that for all $\nu \geq \nu_0$, there is an (n, M, ν, ε) code where $n \leq \nu\alpha$ and

$$\frac{\log_2 M}{\nu} > \boldsymbol{R} - \alpha\delta. \tag{186}$$

Thus, this is an (n, M, ν, ε) code that satisfies

$$\frac{\log_2 M}{n} \geq \frac{\log_2 M}{\nu\alpha} > \frac{\boldsymbol{R}}{\alpha} - \delta. \tag{187}$$

Let $n_0 \equiv \nu_0\alpha$ and $n \geq n_0$. Then, let $\nu = n/\alpha$. This implies $\nu \geq n_0/\alpha = \nu_0$, so the above code with this ν achieves a rate per channel use $\boldsymbol{R}/\alpha$ and also has an average cost $1/\alpha$. This establishes the claim.

We now proceed by contradiction. Suppose we can achieve a rate per unit cost $\boldsymbol{R} > \sup_{\beta \geq \frac{1}{\alpha}} \frac{C(\mathcal{N},\beta)}{\beta}$ with constraint α. Then, by the claim we can achieve the following rate with cost $1/\alpha$:

$$\frac{\boldsymbol{R}}{\alpha} > \sup_{\beta \geq \frac{1}{\alpha}} \frac{C(\mathcal{N}, \beta)}{\beta\alpha} \geq C(\mathcal{N}, 1/\alpha). \tag{188}$$

Since this contradicts the definition of the capacity cost function, the converse follows. □

In particular, when there is a zero-cost state, by concavity $C(\mathcal{N}, \beta)/\beta$ is monotone non-increasing on $(0, +\infty)$ and so

$$\boldsymbol{C}(\mathcal{N}, \alpha) = \alpha C(\mathcal{N}, 1/\alpha). \tag{189}$$

This therefore removes the infinities, assuming that the capacity cost function does not diverge at finite cost. Also, note that eq. (189) gives an operational interpretation of the ratio of the cost-constrained capacity to the cost: When there is a zero-cost state, for any $\beta > 0$, $C(\mathcal{N}, \beta)/\beta$ is the capacity per unit cost with blocklength constraint $1/\beta$. Furthermore, by inverting eq. (189), we obtain an operational interpretation of the ratio of the blocklength-constrained capacity per unit cost to the blocklength constraint.

Interestingly, even in the general case where there might not be a zero-cost state, we can express the cost-constrained capacity in terms of the blocklength-constrained capacity per unit cost. Indeed, by the same proof of Theorem 19 except simply switching the achievability and the converse, we can show that

$$C(\mathcal{N}, \beta) = \sup_{\alpha \geq \frac{1}{\beta}} \frac{\boldsymbol{C}(\mathcal{N}, \alpha)}{\alpha}. \tag{190}$$

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

This expression and Theorem 19 therefore establish a duality between the two quantities, which we can refer to as the *blocklength-cost duality*. We can find many instances of this duality by exchanging "blocklength" with "cost" and vice versa.

A. The Infinite Capacity per Unit Photon of the Pure-Loss Bosonic Channel

In the limit $n_{\text{th}} \to 0$, the thermal channel reduces to the pure-loss bosonic channel $\mathcal{L}_\eta$ [26], which has classical capacity

$$C(\mathcal{L}_\eta, \bar{n}) = g(\eta\bar{n}). \qquad (191)$$

With a simple calculation we find that $\boldsymbol{C}(\mathcal{L}_\eta)$ is infinite, an observation made in [12] and earlier in the context of infinite bandwidth [69]–[71].[3] This is a uniquely quantum phenomenon as there is no direct analogue of the pure-loss channel in classical information theory, and this therefore raised the debate of whether quantum mechanics somehow unlocks the ability to achieve arbitrarily high rates of communication. Our answer to this is negative, and as mentioned above, we propose a solution to this and other infinite capacities per unit cost by introducing a blocklength constraint. In particular, just as not having a photon number constraint led to diverging capacities of bosonic channels, not having a blocklength constraint can lead to diverging capacities per unit cost. The unphysical assumption in the former is that infinite input power is available, while that of the latter is that infinite *time* is available.

This observation motivates considering a composite cost observable given by the sum of time and energy:

$$G \equiv I + \hat{n}. \qquad (192)$$

This way, we can remove both unphysical assumptions at once by effectively constraining both time *and* energy. And we indeed find that with respect to this cost observable, the capacity per unit cost is finite. To see this, let $\mathcal{L}_\eta$ be for instance the pure-loss bosonic channel. Then,

$$\begin{aligned} \boldsymbol{C}(\mathcal{L}_\eta) &= \sup_{\beta>0} \frac{C(\mathcal{L}_\eta, \beta)}{\beta} \\ &= \sup_{\beta>1} \frac{C_{G=\hat{n}}(\mathcal{L}_\eta, \beta-1)}{\beta} \\ &= \sup_{\beta>1} \frac{g(\eta(\beta-1))}{\beta}, \end{aligned} \qquad (193)$$

where we take the supremum over $\beta > 1$ since otherwise the numerator is zero, and

$$C_{G=I+\hat{n}}(\mathcal{L}_\eta, \beta) = C_{G=\hat{n}}(\mathcal{L}_\eta, \beta-1) \qquad (194)$$

since any protocol with average cost β with respect to cost $I + \hat{n}$ is also a protocol with average cost $\beta - 1$ with respect to $\hat{n}$. Now,

$$\lim_{\beta\to 1} \frac{g(\eta(\beta-1))}{\beta} = 0, \qquad (195)$$

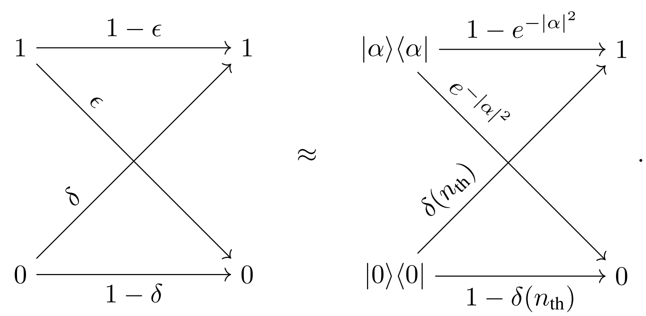
$$\lim_{\beta\to\infty} \frac{g(\eta(\beta-1))}{\beta} = \lim_{\beta\to\infty} \frac{\eta \log\left(1 + \frac{1}{\eta(\beta-1)}\right)}{1} = 0. \qquad (196)$$

Furthermore, eq. (193) is continuous for $\beta \in (1, \infty)$. Hence, it is bounded and thus $\boldsymbol{C}(\mathcal{L}_\eta)$ with respect to the cost observable $I + \hat{n}$ is finite as claimed. Thus, if we have constraints on both time and energy, the capacity is finite. This is superficially reminiscent of the time-energy uncertainty principle in quantum mechanics: just as the individual precisions of time and energy can be unbounded but their product cannot, the capacities with respect to time and energy can be unbounded but the capacity with respect to their sum cannot.

Another way to make sense of the infinite capacity per unit cost of the pure-loss channel is to look at $\boldsymbol{C}(\mathcal{E}_\eta^{n_{\text{th}}})$ for small n_{th}:

$$\boldsymbol{C}(\mathcal{E}_\eta^{n_{\text{th}}}) = -\eta \log_2(n_{\text{th}}(1-\eta)) + \mathcal{O}(n_{\text{th}}). \qquad (197)$$

This is finite for any $n_{\text{th}} > 0$, but diverges as $-\log_2(n_{\text{th}})$ as $n_{\text{th}} \to 0$. Since n_{th} physically corresponds to temperature, this suggests that the infinity comes about since zero temperature is unphysical. It also implies that the capacity per unit cost can be increased arbitrarily by going to lower temperatures. We find that a toy model of a classical binary channel reproduces this qualitative difference between the zero and non-zero temperature cases and the logarithmic scaling of the capacity per unit cost in the noise parameter of the channel:



(198)

On the left in (198) is the binary channel $\mathcal{B}_{\epsilon,\delta}$ with crossover probabilities ϵ and δ, and with input '0' having cost 0, input '1' having cost 1. On the right in (198) is a binary channel induced by a PPM scheme for the thermal channel: the sender sends either the vacuum state $|0\rangle\langle 0|$ at cost 0 or the coherent state $|\alpha\rangle\langle\alpha|$ at cost $|\alpha|^2$, and the detector is a photon counter that measures either a click ('1') or no click ('0'), with crossover probabilities shown on the diagram. A short computation shows that the capacity per unit cost for the binary channel $\mathcal{B}_{\epsilon,\delta}$ is:

$$\boldsymbol{C}(\mathcal{B}_{\epsilon,\delta}) = -(1-\epsilon)\log_2(\delta) - \epsilon \log_2(1-\delta) - h(\epsilon), \qquad (199)$$

where $h(x) \equiv -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. Thus the capacity per unit cost of the classical binary channel $\mathcal{B}_{\epsilon,\delta}$ diverges as $-\log_2(\delta)$ as $\delta \to 0$, analogous to the behavior of (197) as $n_{\text{th}} \to 0$.

[3]For a connection between infinite bandwidth capacity and capacity per unit cost, see [14].

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

IX. Discussion

In this paper we generalized the notion of capacity per unit cost to quantum channels for the tasks of classical communication, entanglement-assisted classical communication, private communication, and quantum communication. There are some simple extensions of our results that hold but for which we do not provide details. First, for private capacity per unit cost, we could also consider, as in [40], the more general case of a quantum wiretap channel $\mathcal{N}_{A\to BE}$ where $\mathcal{N}$ is not necessarily an isometry. The results we found in Section V apply directly to the more general case of a degraded quantum wiretap channel.

Another is to consider non-additive quantum channels, for which we will find regularized expressions of the formulas given in Theorem 4, Theorem 5, Theorem 12, and Theorem 17. For example, for the regularized classical capacity per unit cost we obtain

$$\boldsymbol{C}(\mathcal{N}) = \lim_{n\to\infty} \sup_{\beta>0} \frac{C(\mathcal{N}^{\otimes n}, n\beta)}{n\beta}. \tag{200}$$

This expression motivates an open question we raise: can additivity depend on cost constraint? For example, can the cost-constrained Holevo information $\chi(\mathcal{N}, \beta)$ be additive for some values of β but not others? This is trivially true if we pick some non-additive channel and compare $\beta = 0$ with $\beta = \infty$, but it would be fascinating to find examples where there is some non-trivial dependence.

We think there are a number of interesting directions for future work. One direction is to consider non-degradable quantum channels with a zero-cost state. As discussed earlier, a lower bound for the private capacity per unit cost in this case is given by our private PPM scheme and for classical channels in [42], but the converse remains open. It would also be interesting to give an expression for the quantum capacity per unit cost in terms of an optimized relative entropy. Another possible direction is to prove a strong converse for the capacity per unit cost. However, as was shown in [72], the strong converse holds for Gaussian channels with an approximate peak cost constraint but not an average cost constraint. Hence, for Gaussian channels we cannot directly prove a strong converse for the classical capacity per unit cost in the same way as in Theorem 4. Lastly, we can consider the regime of finite blocklength or finite-sized measurement blocks and see how much information can be sent per cost in this context.

In general, we can find a myriad of new directions by extensive use of the blocklength-cost duality. For instance, instead of one-shot capacities we could consider one-photon capacities, or more generally, "unit-cost" capacities. Instead of finite blocklength analyses of information processing tasks, we could perform finite cost analyses. The reverse substitution is also interesting. As we saw above, rather than cost-constrained capacities, we can consider blocklength-constrained capacities per unit cost. For probabilistic protocols or settings with feedback, we could imagine having an expected blocklength constraint instead of an expected cost constraint. Indeed, blocklength-cost duality allows us to take almost any question in information theory and ask its dual question by simply exchanging "blocklength" and "cost."

Acknowledgements

The authors are grateful to Emmanuel Abbe, Saikat Guha, Patrick Hayden, Alexander Holevo, Hideo Mabuchi, Sergio Verdu, and Tsachy Weissman for helpful conversations about this work.

References

[1] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.
[2] J. Pierce, E. Posner, and E. Rodemich, "The capacity of the photon counting channel," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 1, pp. 61–77, Jan. 1981.
[3] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.
[4] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, Sep. 2017.
[5] F. M. Reza, *An Introduction to Information Theory*. Chelmsford, MA, USA: Courier Corporation, 1961.
[6] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.
[7] J. Pierce, "Optical channels: Practical limits with photon counting," *IEEE Trans. Commun.*, vol. COMM-26, no. 12, pp. 1819–1821, Dec. 1978.
[8] M. J. E. Golay, "Note on the theoretical efficiency of information reception with PPM," *Proc. Inst. Radio Eng.*, vol. 37, no. 9, p. 1031, 1949.
[9] R. G. Gallager, "Energy limited channels: Coding, multiaccess, and spread spectrum," Tech. Rep., 1987. [Online]. Available: https://dspace.mit.edu/handle/1721.1/3023
[10] S. Guha, J. L. Habif, and M. Takeoka, "Approaching Helstrom limits to optical pulse-position demodulation using single photon detection and optical feedback," *J. Mod. Opt.*, vol. 58, nos. 3–4, pp. 257–265, 2011, doi: 10.1080/09500340.2010.533204.
[11] S. Guha, "Structured optical receivers to attain superadditive capacity and the Holevo limit," *Phys. Rev. Lett.*, vol. 106, no. 24, p. 240502, 2011.
[12] S. Guha, Z. Dutton, and J. H. Shapiro, "On quantum limit of optical communications: Concatenated codes and joint-detection receivers," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul./Aug. 2011, pp. 274–278.
[13] S. Dolinar, K. M. Birnbaum, B. I. Erkmen, and B. Moision, "On approaching the ultimate limits of photon-efficient and bandwidth-efficient optical communication," in *Proc. Int. Conf. Space Opt. Syst. Appl. (ICSOS)*, May 2011, pp. 269–278.
[14] S. Verdú, "On channel capacity per unit cost," *IEEE Trans. Inf. Theory*, vol. 36, no. 5, pp. 1019–1030, Sep. 1990.
[15] I. Csiszár, F. Hiai, and D. Petz, "Limit relation for quantum entropy and channel capacity per unit cost," *J. Math. Phys.*, vol. 48, no. 9, p. 092102, 2007.
[16] A. S. Holevo, "Entanglement-assisted capacities of constrained quantum channels," in *Proc. 1st Int. Symp. Quantum Informat.*, 2003, pp. 62–69.
[17] A. S. Holevo, "Entanglement-assisted capacities of constrained quantum channels," *Theory Probab. Appl.*, vol. 48, no. 2, pp. 243–255, 2004, doi: 10.1137/S0040585X97980415.
[18] P. W. Shor, "Additivity of the classical capacity of entanglement-breaking quantum channels," *J. Math. Phys.*, vol. 43, no. 9, pp. 4334–4340, 2002.
[19] M. E. Shirokov, "The Holevo capacity of infinite dimensional channels and the additivity problem," *Commun. Math. Phys.*, vol. 262, no. 1, pp. 137–159, Feb. 2006, doi: 10.1007/s00220-005-1457-8.
[20] A. S. Holevo, "Entanglement-breaking channels in infinite dimensions," *Problems Inf. Transmiss.*, vol. 44, no. 3, pp. 171–184, 2008.
[21] H. Umegaki, "Conditional expectation in an operator algebra, IV (entropy and information)," *Kodai Math. Seminar Rep.*, vol. 14, no. 2, pp. 59–85, 1962.
[22] M. Jarzyna. (Apr. 2017). "Classical capacity per unit cost for quantum channels." [Online]. Available: https://arxiv.org/abs/1704.06696v1
[23] W. F. Stinespring, "Positive functions on C^*-algebras," *Proc. Amer. Math.*, vol. 6, no. 2, pp. 211–216, 1955.
[24] V. Paulsen, *Completely Bounded Maps and Operator Algebras*, vol. 78. Cambridge, U.K.: Cambridge Univ. Press, 2002.

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.

[25] A. S. Holevo, *Quantum Systems, Channels, Information*, vol. 16. Berlin, Germany: Walter de Gruyter, 2012.
[26] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, “Classical capacity of the lossy bosonic channel: The exact solution,” *Phys. Rev. Lett.*, vol. 92, no. 2, p. 027902, 2004.
[27] V. Giovannetti, A. S. Holevo, and R. García-Patrón, “A solution of Gaussian optimizer conjecture for quantum channels,” *Commun. Math. Phys.*, vol. 334, no. 3, pp. 1553–1571, 2015.
[28] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo, “Ultimate classical communication rates of quantum optical channels,” *Nature Photon.*, vol. 8, pp. 796–800, Sep. 2014.
[29] F. Hiai and D. Petz, “The proper formula for relative entropy and its asymptotics in quantum probability,” *Commun. Math. Phys.*, vol. 143, no. 1, pp. 99–114, 1991.
[30] T. Ogawa and H. Nagaoka, “Strong converse and Stein’s lemma in quantum hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2428–2433, Nov. 2000.
[31] B. Schumacher and M. D. Westmoreland, “Sending classical information via noisy quantum channels,” *Phys. Rev. A, Gen. Phys.*, vol. 56, p. 131, Jul. 1997.
[32] A. S. Holevo, “The capacity of the quantum channel with general signal states,” *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan. 1998.
[33] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2017.
[34] A. Winter, “Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints,” *Commun. Math. Phys.*, vol. 347, no. 1, pp. 291–313, 2016.
[35] H. P. Yuen and M. Ozawa, “Ultimate information carrying limit of quantum systems,” *Phys. Rev. Lett.*, vol. 70, no. 4, pp. 363–366, 1993.
[36] A. Anshu, R. Jain, and N. A. Warsi. (Feb. 2017). “One shot entanglement assisted classical and quantum communication over noisy quantum channels: A hypothesis testing and convex split approach.” [Online]. Available: https://arxiv.org/abs/1702.01940
[37] A. Winter, “Coding theorem and strong converse for quantum channels,” *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2481–2485, Nov. 1999.
[38] A. Winter, “Coding theorems of quantum information theory,” Ph.D. dissertation, Dept. Math., Bielefeld Univ., Bielefeld, Germany, Jul. 1999.
[39] I. Devetak, “The private classical capacity and quantum capacity of a quantum channel,” *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.
[40] N. Cai, A. Winter, and R. W. Yeung, “Quantum privacy and quantum wiretap channels,” *Problems Inf. Transmiss.*, vol. 40, no. 4, pp. 318–336, 2004.
[41] M. M. Wilde and H. Qi. (Sep. 2016). “Energy-constrained private and quantum capacities of quantum channels.” [Online]. Available: https://arxiv.org/abs/1609.01997
[42] M. El-Halabi, T. Liu, and C. N. Georghiades, “Secrecy capacity per unit cost,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1909–1920, Sep. 2013.
[43] R. König, R. Renner, A. Bariska, and U. Maurer, “Small accessible quantum information does not imply security,” *Phys. Rev. Lett.*, vol. 98, no. 14, p. 140502, 2007.
[44] M. E. Shirokov and A. S. Holevo, “On lower semicontinuity of the entropic disturbance and its applications in quantum information theory,” *Izvestiya, Math.*, vol. 81, no. 5, pp. 1044–1060, 2017.
[45] G. Lindblad, “Completely positive maps and entropy inequalities,” *Commun. Math. Phys.*, vol. 40, no. 2, pp. 147–151, 1975.
[46] N. Datta, “Min- and max-relative entropies and a new entanglement monotone,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2816–2826, Jun. 2009.
[47] A. Uhlmann, “The ‘transition probability’ in the state space of a *-algebra,” *Reports Math. Phys.*, vol. 9, no. 2, pp. 273–279, 1976.
[48] M. Tomamichel, *Quantum Information Processing With Finite Resources: Mathematical Foundations* (SpringerBriefs in Mathematical Physics), vol. 5. Berlin, Germany: Springer, 2016.
[49] B. Schumacher and M. A. Nielsen, “Quantum data processing and error correction,” *Phys. Rev. A, Gen. Phys.*, vol. 54, no. 4, pp. 2629–2635, 1996.
[50] S. Lloyd, “Capacity of the noisy quantum channel,” *Phys. Rev. A, Gen. Phys.*, vol. 55, no. 3, pp. 1613–1622, 1997.
[51] H. Barnum, E. Knill, and M. A. Nielsen, “On quantum fidelities and channel capacities,” *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1317–1329, Jul. 2000.
[52] H. Barnum, M. A. Nielsen, and B. Schumacher, “Information transmission through a noisy quantum channel,” *Phys. Rev. A, Gen. Phys.*, vol. 57, no. 6, pp. 4153–4175, 1998.
[53] P. W. Shor, “The quantum channel capacity and coherent information,” in *Proc. MSRI Workshop Quantum Comput.*, 2002.
[54] I. Devetak and P. W. Shor, “The capacity of a quantum channel for simultaneous transmission of classical and quantum information,” *Commun. Math. Phys.*, vol. 256, no. 2, pp. 287–303, 2005.
[55] G. Smith, “Private classical capacity with a symmetric side channel and its application to quantum cryptography,” *Phys. Rev. A, Gen. Phys.*, vol. 78, p. 022306, Aug. 2008.
[56] I. Devetak and A. Winter, “Relating quantum privacy and quantum coherence: An operational approach,” *Phys. Rev. Lett.*, vol. 93, no. 8, p. 080501, 2004.
[57] L. Wang and R. Renner, “One-shot classical-quantum capacity and hypothesis testing,” *Phys. Rev. Lett.*, vol. 108, p. 200501, May 2012.
[58] F. Buscemi and N. Datta, “The quantum capacity of channels with arbitrarily correlated noise,” *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1447–1460, Mar. 2010.
[59] N. Datta, M. Tomamichel, and M. M. Wilde, “On the second-order asymptotics for entanglement-assisted communication,” *Quantum Inf. Process.*, vol. 15, no. 6, pp. 2569–2591, Jun. 2016.
[60] A. S. Holevo, “Sending quantum information with Gaussian states,” in *Quantum Communication, Computing, and Measurement*. Berlin, Germany: Springer, 2002, pp. 75–82.
[61] A. S. Holevo and R. F. Werner, “Evaluating capacities of bosonic Gaussian channels,” *Phys. Rev. A, Gen. Phys.*, vol. 63, p. 032312, Feb. 2001.
[62] M. Takeoka and S. Guha, “Capacity of optical communication in loss and noise with general quantum Gaussian receivers,” *Phys. Rev. A, Gen. Phys.*, vol. 89, no. 4, p. 042309, 2014.
[63] A. S. Holevo and V. Giovannetti, “Quantum channels and their entropic characteristics,” *Rep. Progr. Phys.*, vol. 75, no. 4, p. 046001, 2012.
[64] M. E. Shirokov, “Conditions for coincidence of the classical capacity and entanglement-assisted capacity of a quantum channel,” *Problems Inf. Transmiss.*, vol. 48, no. 2, pp. 85–101, 2012.
[65] M. M. Wolf, D. Pérez-García, and G. Giedke, “Quantum capacities of bosonic channels,” *Phys. Rev. Lett.*, vol. 98, no. 13, p. 130501, 2007.
[66] N. Davis, M. E. Shirokov, and M. M. Wilde, “Energy-constrained two-way assisted private and quantum capacities of quantum channels,” *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 6, p. 062310, Jun. 2018.
[67] M. Takeoka, S. Guha, and M. M. Wilde, “Fundamental rate-loss tradeoff for optical quantum key distribution,” *Nature Commun.*, vol. 5, p. 5235, Oct. 2014.
[68] K. Goodenough, D. Elkouss, and S. Wehner, “Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels,” *New J. Phys.*, vol. 18, p. 063005, Jun. 2016.
[69] D. S. Lebedev and L. B. Levitin, “Information transmission by electromagnetic field,” *Inf. Control*, vol. 9, no. 1, pp. 1–22, 1966.
[70] C. M. Caves and P. D. Drummond, “Quantum limits on bosonic communication rates,” *Rev. Mod. Phys.*, vol. 66, no. 2, p. 481, 1994.
[71] H. P. Yuen, R. S. Kennedy, and M. Lax, “Optimum testing of multiple hypotheses in quantum detection theory,” *IEEE Trans. Inf. Theory*, vol. IT-21, no. 2, pp. 125–134, Mar. 1975.
[72] B. R. Bardhan, R. García-Patrón, M. M. Wilde, and A. Winter, “Strong converse for the classical capacity of optical quantum communication channels,” *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1842–1850, Apr. 2015.

Dawei Ding is a PhD candidate in the Department of Applied Physics at Stanford University and is affiliated with the Stanford Institute for Theoretical Physics. He is a recipient of the National Defense Science and Engineering Graduate Fellowship and is a Stanford Graduate Fellow. He studies quantum Shannon theory, quantum chaos, and quantum computing. He is also involved in the It from Qubit Simons collaboration, a dialogue between quantum information and fundamental physics.

Dmitri S. Pavlichin is a postdoctoral scholar in the Applied Physics department at Stanford University in Stanford, California. He received his Ph.D. in Physics from Stanford University in 2014 and his A.B. *(summa cum laude)* in Physics from Harvard University in 2007. His research interests are in information theory and statistics, data compression, and bioinformatics.

Mark M. Wilde (M’99–SM’13) is an Assistant Professor in the Department of Physics and Astronomy and the Center for Computation and Technology at Louisiana State University in Baton Rouge, Louisiana. He is the recipient of a National Science Foundation Career Development Award and the APS-IUSSTF Professorship Award in Physics. His current research interests are in quantum Shannon theory, quantum optical communication, quantum computational complexity theory, and quantum error correction.

Authorized licensed use limited to: Louisiana State University. Downloaded on February 11,2022 at 16:48:17 UTC from IEEE Xplore. Restrictions apply.