Positivity, Discontinuity, Finite Resources, Nonzero Error for Arbitrarily Varying Quantum Channels

H. Boche, J. Nötzel
Lehrstuhl für Theoretische Informationstechnik, Technische Universität München
Email: {boche, janis.noetzel}@tum.de

***Abstract*—We give an explicit example that answers the question whether the transmission of messages over arbitrarily varying quantum channels can benefit from distribution of randomness between the legitimate sender and receiver in the affirmative.**
The specific class of channels introduced in that example is then extended to show that the deterministic capacity does have discontinuity points, while that behaviour is, at the same time, not generic: We show that it is in fact continuous around its positivity points. This is in stark contrast to the randomness-assisted capacity, which is continuous in the channel.
We then quantify the interplay between the distribution of finite amounts of randomness between the legitimate sender and receiver, the (nonzero) decoding error with respect to the average error criterion that can be achieved over a finite number of channel uses and the number of messages that can be sent. These results also apply to entanglement- and strong subspace transmission.

I. Introduction

We will first explain the model of an arbitrarily varying channel and provide examples for communication scenarios whose essential features are captured by the model. We then explain the effect of shared randomness for these systems and state a corresponding result. In close connection, we discuss the relevance of continuity of capacities, state results and give examples. Finally, we quantify the interplay between finite errors, block length and amount of common randomness needed to achieve that error.

Imagine a sender wants to transmit for example messages to a remote receiver. They each have access to a quantum system which is modeled on a finite dimensional Hilbert space and are connected by a quantum channel. Dependent on the message he wants to transmit the sender prepares some quantum state, which is then transmitted to the receiver over the channel. In-and output of the channel will most of the time not be identical. The question then is, whether the receiver can infer which message the sender intended to send just by performing measurements on the output states.
We assume that multiple channel uses are available and that the channel does not have a memory - but instead assume the existence of a jammer, which tries to prevent the two legal parties from communicating properly. Such a situation can arise e.g. in secret key distribution or transmission scenarios over quantum channels as developed by Devetak in [11], but when the evil third party is either not interested in or unable to do eavesdropping on the legal communication, but has some influence on the channel between the legal parties. The power of the jammer is, in the model chosen here, precisely quantified by his ability to influence the channel:
He is able to choose, for each of the multiple channel uses, one out of a fixed set $\mathfrak{I}$ of channels. This set is known to all three parties. The goal of sender and receiver is now to find encoding-and decoding procedures such that they can reliably transmit their data, no matter which choice the jammer makes. It can even be assumed that the jammer knows *in advance* how the encoding-decoding procedure of sender and receiver works. This assumption will always be satisfied in commercial communication systems, where standardized protocols are being used. The model that we just introduced is called an arbitrarily varying quantum channel, and will be abbreviated AVQC henceforth. A precise mathematical formulation is postponed to the definitions section. Please note that, throughout the entire manuscript, we restrict attention to finite AVQCs, e.g. those for which $|\mathfrak{I}| < \infty$ holds. The main reason for this is that it greatly simplifies proofs and puts a clean focus on the most relevant features of the systems under consideration. Nevertheless, it should be noted that all the approximation techniques to deal with the general cases are published in [4] and ready to use.
Of course, the very same model can be formulated by using as the basic channels either classical, classical-quantum or quantum-classical channels, and the underlying systems that the three parties act upon could be described by any kind of physical theory. Another possible change in the model would be to enable the jammer to use quantum inputs to the system. In this work, we will stick to the model we described first.
The situation described by the model can, in these days, be found in denial-of-service attacks. It is important to note that the quality of an arbitrarily varying classical channel can not only be described by entropical quantities, as is the case for stationary memoryless channels. It has rather been found that its capability to transmit any messages at all is completely characterized by so-called *symmetrizability conditions*.
Let us get into a bit more detail here. It has been proven, first in [1] for classical arbitrarily varying channels, then in [2] for classical-quantum arbitrarily varying channels that these systems exhibit a dichotomic behaviour: the message-transmission capacity under average error criterion, $\overline{C}_{\mathrm{d}}$, is either zero or equals an easily computable number, called the random capacity $\overline{C}_{\mathrm{r}}$. The latter quantity is the amount of messages that can be sent with transmission error approaching

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

zero, when the number of channel uses goes to infinity and sender and receiver share a sufficiently large amount of shared randomness (polynomially much common randomness, in the number of channel uses, is sufficient). It turned out later [10], [13] that those arbitrarily varying channels $\mathfrak{W}$ for which $\overline{C}_{\mathrm{d}}(\mathfrak{W}) = 0$ holds are exactly characterized by so-called "symmetrizability" conditions.

The dichotomic behaviour has been proven to hold true for both entanglement and message transmission over AVQCs in [4]. Another result of the work [4] was that encoding-decoding schemes for entanglement transmission are also good for strong subspace transmission and vice versa. The later work [8] showed that this is also true for message transmission under average- and maximal error criterion. These results enable us to restrict our discussion to the average error criterion and entanglement transmission henceforth.

Despite these achievements, it remained an open question until now whether shared randomness really helps the transmission of messages over AVQCs, and the same question remained open for entanglement-and strong subspace transmission.

More precisely, it has been conjectured in [4] that shared randomness does not increase the entanglement transmission capacity of AVQCs and in [8] that there exist examples of AVQCs $\mathfrak{I}$ for which $\overline{C}_{\mathrm{r}}(\mathfrak{I}) > 0$ but $\overline{C}_{\mathrm{d}}(\mathfrak{I}) = 0$ holds.

It is the first result of this work to give exactly such an example.

With hindsight on applications of the model, we then study the continuity properties of $\overline{C}_{\mathrm{d}}$ for AVQCs. It is desirable from a practical point of view to have a continuous dependence of the capacity of the system on its parameters, since small uncertainties due to measurement errors can never be totally eliminated. We find that $\overline{C}_{\mathrm{d}}$ is continuous around every AVQC $\mathfrak{I}$ for which $\overline{C}_{\mathrm{d}}(\mathfrak{I}) > 0$ holds. Put into simple words: If a system which is modeled as an AVQC is 'useful' in the sense that $\overline{C}_{\mathrm{d}}(\mathfrak{I}) > 0$, then this remains true even if small errors are present in the evaluation of the system parameters.

An obvious question that comes with the above two results is, whether there really exist discontinuities for the function $\mathfrak{I} \mapsto \overline{C}_{\mathrm{d}}(\mathfrak{I})$. The continuity of the message- and entanglement transmission capacity of a stationary memoryless quantum channel has been an open problem for quite a while, it was posed by M. Keyl and listed in the open problem page [16] of R. Werner's group since 2003. After partial results, it was completely solved by Leung and Smith in [15] in 2009, and answered in the affirmative: Both message- and entanglement transmission capacity are continuous for stationary memoryless quantum channels.

Quite on the contrary, we prove in this work that the message transmission capacity of AVQCs *without* assistance by shared randomness is not continuous. We do so by explicit construction of an example. This is the first example of a discontinuous behaviour of a quantum capacity other than the zero-error capacities [12].

Our previous results clearly demonstrate the importance of shared randomness for AVQCs. In [4], Ahlswede, Bjelaković and the authors showed that already a small amount of common randomness is sufficient to ensure that transmission of messages is possible at rates arbitrarily close to $\overline{C}_{\mathrm{r}}$. The same holds true for transmission of entanglement. Building on that and the work [3] of Ahlswede and Cai, the authors were able to to show in [8] that already the use of arbitrarily small amounts of correlation yield the same result.

This demonstrates that shared randomness has two important effects for AVQCs: First, it boosts the capacity to the maximally possible value, and second it stabilizes the system with respect to small changes (the capacity function with assistance by either unlimited shared randomness, positive correlation or small amounts of common randomness is always continuous).

This gives a strong motivation to start a closer investigation of the exact interplay between the system parameters, the error of message transmission at a specific block length and the amount of randomness used for stabilization of the system. The results of that investigation are summarized in Theorem 4. We give bounds on the number of shared secret bits (common randomness) K needed to achieve some pre-given maximal error λ within L channel uses. Assuming that the AVQC under consideration has $|\mathbf{S}|$ constituents, the scaling law is roughly $K \leq \frac{\log|\mathbf{S}|}{E\cdot\lambda}$, where E is the reliability function of the *compound channel* $\mathrm{conv}(\mathfrak{I})$ and L is more implicitly given through E, roughly scaling as $L(1-\frac{1}{L}\log L) \approx -E\log(E/\lambda)$. In case that the AVQC $\mathfrak{I}$ is symmetrizable, we note that the results of [4] imply $\frac{1}{2\lambda} \leq K$, and for non-symmetrizable AVQCs we know that $K = 0$ is sufficient by the quantum-Ahlswede dichotomy of [4].

Another important observation is that the number K of random bits needed to guarantee a certain quality of transmission is essentially independent of the number l of channel uses, if only $l \geq L$ holds, and is indefinite for $l < L$. The technique of proof we utilize here applies for entanglement transmission as well.

It is clear that a similar result could be obtained by using only correlation to first establish enough common randomness, then use it with the above stated bounds. The exact trade-off between λ, L and the 'amount' of correlation remains unclear and we leave that question open for future work.

II. Notation

All Hilbert spaces are assumed to have finite dimension and are over the field $\mathbb{C}$. The set of linear operators from $\mathcal{H}$ to $\mathcal{H}$ is denoted $\mathcal{B}(\mathcal{H})$. $\mathcal{S}(\mathcal{H})$ is the set of states, i.e. positive semi-definite operators with trace (the trace function on $\mathcal{B}(\mathcal{H})$ is written tr) 1 acting on the Hilbert space $\mathcal{H}$. The maximally mixed state with only one eigenvalue $\dim(\mathcal{H})$ in $\mathcal{S}(\mathcal{H})$ is written $\pi_{\mathcal{H}}$ or, if no confusion can arise, simply π. A vector $x \in \mathcal{H}$ of unit length will be referred to as a state vector, the corresponding state is denoted $|x\rangle\langle x|$. For a finite set $\mathbf{X}$, $\mathfrak{P}(\mathbf{X})$ is the set of probability distributions on $\mathbf{X}$, and $|\mathbf{X}|$ its cardinality. For any $l \in \mathbb{N}$, we define $\mathbf{X}^l := \{(x_1,\ldots,x_l) : x_i \in \mathbf{X}\ \forall i \in \{1,\ldots,l\}\}$, and write x^l for the elements of $\mathbf{X}^l$. For any natural number N, we define $[N]$ to be the shorthand for the set $\{1,...,N\}$.

The set of completely positive trace preserving (CPTP) maps (quantum channels) between $\mathcal{B}(\mathcal{H})$ and $\mathcal{B}(\mathcal{K})$ is denoted $\mathcal{C}(\mathcal{H},\mathcal{K})$.
Closely related is the set of classical-quantum channels (abbreviaton: 'cq-channels') with finite input alphabet $\mathbf{Z}$ and quantum output in $\mathcal{S}(\mathcal{K})$. This set is denoted $CQ(\mathbf{Z},\mathcal{K})$.
Using the usual operator ordering symbols $\leq$ and $\geq$ on $\mathcal{B}(\mathcal{H})$, the set of measurements with $N \in \mathbb{N}$ different outcomes is written
$\mathcal{M}_N^{\mathcal{H}} := \{\mathbf{D} = (D_i)_{i=1}^N : \sum_{i=1}^N D_i \leq \mathbb{1},\ D_i \geq 0\ \forall i \in [N]\}$.
Throughout the paper, we assume w.l.o.g. that $\sum_{i=1}^N D_i = \mathbb{1}$.
The von Neumann entropy of a state $\rho \in \mathcal{S}(\mathcal{H})$ is given by

$$S(\rho) := -\mathrm{tr}(\rho \log \rho),$$

where $\log(\cdot)$ denotes the base two logarithm which is used throughout the paper. The Holevo information is for a given channel $W \in CQ(\mathbf{X},\mathcal{H})$ and input probability distribution $p \in \mathfrak{P}(\mathbf{X})$ defined by

$$\chi(p,W) := S(\overline{W}) - \textstyle\sum_{x\in\mathbf{X}} p(x) S(W(x)),$$

where $\overline{W}$ is defined by $\overline{W} := \sum_{x\in\mathbf{X}} p(x) W(x)$. $H(p)$ is the usual Shannon entropy of $p \in \mathfrak{P}(\mathbf{X})$. The binary Shannon entropy of $p \in \mathfrak{P}(\{0,1\})$ is abbreviated by either $h(p(1))$ or $h(p(2))$.
For $\rho \in \mathcal{S}(\mathcal{H})$ and $\mathcal{N} \in \mathcal{C}(\mathcal{H},\mathcal{H})$ the entanglement fidelity (which was defined in [17]) is given by

$$F_e(\rho,\mathcal{N}) := \langle \psi, (id_{\mathcal{B}(\mathcal{H})} \otimes \mathcal{N})(|\psi\rangle\langle\psi|)\psi\rangle,$$

with $\psi \in \mathcal{H}\otimes\mathcal{H}$ being an arbitrary purification of the state ρ.
For a finite set $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}} \subset \mathcal{C}(\mathcal{H},\mathcal{K})$, the convex hull $\mathrm{conv}(\mathcal{W})$ is given by

$$\mathrm{conv}(\mathfrak{I}) = \left\{\textstyle\sum_{s\in\mathbf{S}} q(s) W_s : q \in \mathfrak{P}(\mathbf{S})\right\}.$$

The distance between sets $\mathfrak{I},\mathfrak{I}' \subset \mathcal{C}(\mathcal{H},\mathcal{K})$ is measured by $D_\diamond(\mathfrak{I},\mathfrak{I}')$ - the Hausdorff distance which is induced by the diamond norm $\|\cdot\|_\diamond$. Further details can be found in [9].

III. Definitions

For the rest of this subsection, let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}} \subset \mathcal{C}(\mathcal{H},\mathcal{K})$ denote a finite set of channels and $\mathcal{H},\mathcal{K}$ some arbitrary but fixed finite dimensional Hilbert spaces over $\mathbb{C}$. Henceforth, we follow the convention from [4], using the term 'the AVQC $\mathfrak{I}$' as a linguistic shorthand for the mathematical object $(\{\mathcal{N}_{s^l}\}_{s^l\in\mathbf{S}^l})_{l\in\mathbb{N}}$.
Due to the close correspondence between arbitrarily varying and certain compound channels, we will sometimes also encounter the case that $\mathfrak{I}$ stands for the compound channel $(\{\mathcal{N}_q^{\otimes l}\}_{\mathcal{N}_q\in\mathrm{conv}(\mathfrak{I})})_{l\in\mathbb{N}}$. In those cases, this will be explicitly mentioned. We will now define the entanglement transmission capacities of an AVQC. Corresponding coding theorems can be found in [4].

Definition 1. *An $(l,k_l)-$*random entanglement transmission code *for $\mathfrak{I}$ is a probability measure μ_l on $(\mathcal{C}(\mathcal{F}_l,\mathcal{H}^{\otimes l}) \times \mathcal{C}(\mathcal{K}^{\otimes l},\mathcal{F}_l),\sigma_l)$, where $\mathcal{F}_l$ is a Hilbert spaces with $\dim\mathcal{F}_l = k_l$ and σ_l a suitable σ-algebra. The error of the code is given by $\varepsilon_l := 1 - \int d\mu_l(\mathcal{R}^l,\mathcal{P}^l) F_e(\pi_{\mathcal{F}_l}, \mathcal{R}_l\circ\mathcal{N}_{s^l}\circ\mathcal{P}_l)$.*

Definition 2. *$R \geq 0$ is said to be an achievable entanglement transmission rate for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ with random codes and error $\lambda \in [0,1]$ if there is a sequence of $(l,k_l)-$random entanglement transmission codes such that both $\liminf_{l\to\infty}\frac{1}{l}\log k_l \geq R$ and $\limsup_{l\to\infty}\varepsilon_l = 1$.*
The corresponding capacity is defined by

$$\mathcal{A}_{\mathrm{r}}(\mathfrak{I},\lambda) := \sup\left\{ R : \begin{array}{l} R \text{ is ach. entanglement} \\ \text{transmission rate for } \mathfrak{I} \\ \text{w. random codes and error } \lambda \end{array} \right\}.$$

Remark 1. *This definition differs from the classical one used e.g. in [5]. Precisely speaking, if one would define capacities with finite errors in the spirit of [5] using the symbol $\tilde{\mathcal{A}}_{\mathrm{r}}$ for those, then one would set*

$$\tilde{\mathcal{A}}_{\mathrm{r}} := \lim_{n\to\infty}\frac{1}{n}\log\max\{k_l : \exists\ (l,k_l) - \text{code s.t. } \lambda_l \leq \lambda\}.$$

Since $\lambda \to \tilde{\mathcal{A}}_{\mathrm{r}}(\mathfrak{I},\lambda)$ is monotone increasing on $[0,1]$, the limits $\lim_{\varepsilon\to 0}\tilde{\mathcal{A}}_{\mathrm{r}}(\mathfrak{I},\lambda+\varepsilon)$ exist for every $\lambda \in [0,1)$. Thus, $\mathcal{A}_{\mathrm{r}}(\mathfrak{I},\lambda) = \lim_{\varepsilon\to 0}\tilde{\mathcal{A}}_{\mathrm{r}}(\mathfrak{I},\lambda+\varepsilon)$ holds for all $\lambda \in [0,1)$. This implies that $\mathcal{A}_{\mathrm{r}}$ is simply the right-regularized version of $\tilde{\mathcal{A}}_{\mathrm{r}}$. While $\tilde{A}_{\mathrm{r}}$ might be a practically more relevant definition, it is clear that the two definitions can lead to a different value in capacity only at discontinuity points of $\tilde{A}_{\mathrm{r}}$. Since both functions are monotone increasing on the interval $[0,1]$, the number of such points is countable by [18], Theorem 4.30. Notably, at $\lambda = 0$, one gets $\mathcal{A}_{\mathrm{r}}(\mathfrak{I},0) = \mathcal{A}_{\mathrm{r}}(\mathfrak{I})$ for 'the' random capacity $\mathcal{A}_{\mathrm{r}}$ of an AVQC according to Definition 2 in [4], while $\tilde{\mathcal{A}}_{\mathrm{r}}(\mathfrak{I},0)$ gives the randomness-assisted zero-error capacity of an AVQC.
This latter point makes our definition fit seamlessly with the previous work [4], [8] on AVQCs. At the same time, we do not encounter a dramatically different behaviour in most cases. The same reasoning applies to all the other capacities defined in this paper.

Having defined random codes and random code capacity for entanglement transmission we now introduce their deterministic counterparts:

Definition 3. *A non-negative number R is a deterministically achievable entanglement transmission rate for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ with error $\lambda \in [0,1]$ if it is achievable in the sense of Definition 2 but with* point measures *μ_l: For each μ_l there exist $(\mathcal{P}^l,\mathcal{R}^l)$ such that $\mathfrak{I}$ with $\mu_l(\{(\mathcal{P}^l,\mathcal{R}^l)\}) = 1$.*
The deterministic entanglement transmission capacity $\mathcal{A}_{\mathrm{d}}(\mathfrak{I},\lambda)$ is defined accordingly, in the spirit of Definition 2.

We need an additional capacity:

Definition 4 (Strong Subspace Transmission)**.** *The strong subspace transmission capacities $\mathcal{A}_{\mathrm{s,r}}$ and $\mathcal{A}_{\mathrm{s,d}}$ with assistance by shared randomness and without are defined analogously to the entanglement transmission capacities, but with each $F_e(\pi_{\mathcal{F}_l},\mathcal{R}^l\circ\mathcal{N}_{s^l}\circ\mathcal{P}^l)$ replaced by*

$$\min_{x\in\mathcal{F}_l:\langle x,x\rangle=1}\langle x,\mathcal{R}^l\circ\mathcal{N}_{s^l}\circ\mathcal{P}^l(|x\rangle\langle x|)x\rangle.$$

From the results in [8], we know that average- and maximal error criterion lead to the same capacity for AVQCs. Strictly speaking, this is a consequence of two facts: First, it does not really make sense to restrict the encoding functions to pure

signal states in the quantum case. Second, the two criteria are equivalent in the classical case as well, if one allows randomized encodings (see [1], Theorems 2 and 3).

Definition 5 (Codes for message transmission)**.** *Let $l \in \mathbb{N}$. A random code for message transmission over $\mathfrak{I}$ is given by a probability measure γ_l on the set $(CQ(M_l, \mathcal{H}^{\otimes l}) \times \mathcal{M}_{M_l}, \Sigma_l)$, where Σ_l is a suitable $\sigma-$algebra. A deterministic code is given by a random code γ_l, where γ_l is a point measure. The error of the code is defined by*

$$1 - \varepsilon_l := \min_{s^l \in \mathbf{S}^l} \int \frac{1}{M_l} \sum_{i=1}^{M_l} \mathrm{tr}\{D_i \mathcal{N}_{s^l}(\mathcal{P}(i))\} d\gamma_l(\mathcal{P}, \mathbf{D}).$$

Definition 6 (Achievability)**.** *A nonnegative number R is called achievable with random codes with error λ under the average error criterion if there exists a sequence $(\gamma_l)_{l\in\mathbb{N}}$ of random codes satisfying both $\limsup_{l\to\infty} \varepsilon_l \leq \lambda$ and $\liminf_{l\to\infty} \frac{1}{l} \log M_l \geq R$.*
If the sequence $(\gamma_l)_{l\in\mathbb{N}}$ can be chosen to consist of point measures only, then R is called achievable with deterministic codes under the average error criterion.

Definition 7 (Message transmission capacities of an AVQC)**.** *The corresponding capacities of $\mathfrak{I}$ are defined as*

$$\overline{C}_{\mathrm{d}}(\mathfrak{I}, \lambda) := \sup \left\{ R : \begin{array}{l} R \text{ is ach. with det. codes under} \\ \text{average error crit. with error } \lambda \end{array} \right\},$$

$$\overline{C}_{\mathrm{r}}(\mathfrak{I}, \lambda) := \sup \left\{ R : \begin{array}{l} R \text{ is ach. with det. codes under} \\ \text{average error crit. with error } \lambda \end{array} \right\}.$$

As mentioned already, every AVQC $\mathfrak{I}$ is intimately connected to the compound quantum channel $\mathrm{conv}(\mathfrak{I})$: the capacities of the AVQC $\mathfrak{I}$ are often given by the respective formulas for the corresponding compound quantum channels $\mathrm{conv}(\mathfrak{I})$. This connection especially shows up in the proof and formulation of our Theorem 4, where we encounter the reliability functions of compound quantum channels. In order to define these, we first define codes, achievability and corresponding capacities for compound quantum channels:

Definition 8 (Codes, achievability, capacity: compound case)**.** *Let $l \in \mathbb{N}$. A* code $\mathfrak{C}_l$ *for message transmission over the compound channel $\mathfrak{I}$ is given by a natural number M_l, an encoding $\mathcal{P} : [M_l] \to \mathcal{S}(\mathcal{H}^{\otimes l})$ and a decoding $\mathbf{D} \in \mathcal{M}_{M_l}$. The error ε_l associated to the code is given by*

$$\varepsilon_l := 1 - \min_{s\in\mathbf{S}} \frac{1}{M_l} \sum_{i=1}^{M_l} \mathrm{tr}\{D_i \mathcal{N}_s^{\otimes l}\}.$$

A nonnegative number R is called achievable *for the compound channel $\mathfrak{I}$ with error $\lambda \in [0, 1]$ if there exists a sequence $(\mathfrak{C}_l)_{l\in\mathbb{N}}$ of codes for $\mathfrak{I}$ satisfying both $\limsup_{l\to\infty} \varepsilon_l \leq \lambda$ and $\limsup_{l\to\infty} \frac{1}{l} \log M_l \geq R$.*
The deterministic capacity $\overline{C}^{\mathrm{c}}_{\mathrm{d}}(\mathfrak{I}, \lambda)$ *of the compound channel $\mathfrak{I}$ with error λ is given by the* supremum over all achivable rates for the compound channel $\mathfrak{I}$ under the average error criterion, with error λ.

These definitions enable us to define the following:

Definition 9 (Reliability Function)**.** *The reliability function $E : \mathcal{C}(\mathcal{H}, \mathcal{K}) \times \mathbb{R}_+ \to \mathbb{R}_+$ is, for a compound channel $\mathfrak{I}$ and rate $R \geq 0$, defined as:*
The supremum over all $E \geq 0$ such that there are $\varepsilon > 0$ and $N \in \mathbb{N}$ such that for all $n \geq N$ there is a code for message transmission over $\mathfrak{I}$ satisfying both $\frac{1}{l} \log(M_l) \geq R - \varepsilon$ and $\varepsilon_l \leq 2^{-l(E-\varepsilon)}$, under the average error criterion.

Remark 2. *$E(\mathfrak{I}, R)$ can have nonzero, finite values. This can be seen from [6], for example. We could make an analogous definition for any of the other transmission scenarios and reliability criteria. In case of entanglement transmission, our techniques are even of sufficient generality to yield comparably strong results, see the accompanying paper [9].*

Another important definition is that of *symmetrizability*:

Definition 10 (Cf. definition 39 in [4])**.** *Let $\mathfrak{I}$ denote an AVQC.*

1) *$\mathfrak{I}$ is called l-symmetrizable, $l \in \mathbb{N}$, if for each finite set $\{\rho_i\}_{i=1}^K \subset \mathcal{S}(\mathcal{H}^{\otimes l})$, there is a map $p : \{\rho_i\}_{i=1}^K \to \mathfrak{P}(\mathbf{S}^l)$ such that for all $i, j \in \{1, \ldots, K\}$ it holds $\sum_{s^l\in\mathbf{S}^l} p(\rho_i)(s^l)\mathcal{N}_{s^l}(\rho_j) = \sum_{s^l\in\mathbf{S}^l} p(\rho_j)(s^l)\mathcal{N}_{s^l}(\rho_i)$.*
2) *We call $\mathfrak{I}$ symmetrizable if it is l-symmetrizable for all $l \in \mathbb{N}$.*

It was one of the results in [4] (see theorem 40 there) that a finite AVQC $\mathfrak{I}$ is symmetrizable if and only if $\overline{C}_d(\mathfrak{I}, 0) = 0$.

IV. Main Results

We now list our main results. Throughout, $\mathfrak{I}$ is a fixed finite but otherwise completely arbitrary AVQC. If a capacity is written without specifying the error λ it is assumed that $\lambda = 0$ holds.

Theorem 1. *If $\mathfrak{I}$ has the form $\mathcal{N}_s(\rho) := \sum_{x\in\mathbf{X}} \mathrm{tr}\{\rho M_x\}\rho_{s,x}$, $s \in \mathbf{S}$, for some finite $\mathbf{S}$ and POVM $\{M_i\}_{i=1}^M$ and probability distributions $\{p_x\}_{x\in\mathbf{X}} \subset \mathfrak{P}(\mathbf{S})$ such that*

$$\sum_{s\in\mathbf{S}} p_{x'}(s)\rho_{s,x} = \sum_{s\in\mathbf{S}} p_x(s)\rho_{s,x'} \qquad \forall x, x' \in \mathbf{X}, \tag{1}$$

then it is symmetrizable and whence $\overline{C}_{\mathrm{d}}(\mathfrak{I}) = 0$. Moreover, there exist examples of such AVQCs where even $\overline{C}_{\mathrm{r}}(\mathfrak{I}) > 0$.

Remark 3. *Let us make a note on the intuition behind it. The channel $\mathfrak{I}$ is the concatenation of a stationary memoryless qc-channel (measurement) $\mathfrak{W}_1$ and an arbitrarily varying cq-channel $\mathfrak{W}_2$ given by the states $\{\rho_{s,x}\}_{s,x}$. This combination ensures that the channel itself is entanglement-breaking, whence its capacity has a one-shot formula and, even more important, it is l-symmetrizable for all $l \in \mathbb{N}$ if and only if it is 1-symmetrizable.*
Using entangled inputs as signal states for $\mathfrak{I}$ results in mixtures of product states after the application of $\mathfrak{W}_1$, so $\mathfrak{W}_2$ sees a randomized code. But since we allow mixed inputs, this is equivalent to using just a randomized code with separable inputs for $\mathfrak{W}_2$. But on the subset of separable states signal states, $1-$symmetrizability is equivalent to l-symmetrizability for all $l \in \mathbb{N}$, so no such code can transmit even a single bit

with asymptotically vanishing error. Therefore, the deterministic capacity of $\mathfrak{W}$ has to be equal to zero.

Remark 4. *It is clear that the conjectured statement "for all finite AVQCs, it holds that $\mathcal{A}_{\rm d}(\mathfrak{I}) = \mathcal{A}_{\rm r}(\mathfrak{I})$" is equivalent to saying that symmetrizability of a finite AVQC $\mathfrak{I}$ implies that $\mathcal{A}_{\rm r}(\mathfrak{I}) = 0$. It is also clear that either one of the above would imply that $\mathcal{A}_{\rm d}$ is continuous, since $\mathcal{A}_{\rm r}$ is.*

Theorem 2. *The capacity function $\overline{C}_{\rm det}(\cdot) : \mathcal{C}(\mathcal{H}, \mathcal{K}) \to \mathbb{R}_+$ is not continuous.*
More precisely, let $\mathbb{C}^2 = \operatorname{span}(\{e_1, e_2\}) \subset \mathbb{C}^3 = \operatorname{span}(\{e_i\}_{i=1}^3)$. Let the channels $\mathcal{D}_\eta \in \mathcal{C}(\mathbb{C}^2, \mathbb{C}^3)$ be defined through $\mathcal{D}_\eta(X) := (1-\eta)X + \eta \cdot \mathrm{tr}\{X\} \cdot \pi \ \forall X \in \mathcal{B}(\mathbb{C}^2)$. There exists a set $\{\mathcal{N}_s\}_{s\in\mathbf{S}} \subset \mathcal{C}(\mathbb{C}^2, \mathbb{C}^3)$ having the structure defined in theorem 1 such that for any $\lambda, \eta \in [0,1)$ the sequence $\mathfrak{I}_\lambda^\eta = \{\hat{\mathcal{N}}_{s,\eta,\lambda}\}_{s\in\mathbf{S}}$ of AVQCs defined by $\hat{\mathcal{N}}_{s,\eta,\lambda} := (1-\lambda)\mathcal{D}_\eta + \lambda\mathcal{N}_s$ satisfies

$$\lim_{\lambda\to 1} \overline{C}_{\rm r}(\mathfrak{I}_\lambda^\eta) \geq 0.5, \quad \overline{C}_{\rm d}(\mathfrak{I}_\lambda^\eta) = \overline{C}_{\rm r}(\mathfrak{I}), \quad C_{\rm d}(\mathfrak{I}_1) = 0$$

and $\lim_{\lambda\to 1} D_\diamondsuit(\mathfrak{I}_\lambda^\eta, \mathfrak{I}) = 0$ for all $\eta \in [0,1]$.

Remark 5. *This is the first example of discontinuous behaviour of a quantum capacity other than the zero-error capacities. It is not clear to the authors yet, whether similar results could be proven for purely classical systems.*
The example also highlights the stabilizing effect that is achieved by distribution of shared randomness in a communication system.

Theorem 3 (Positivity of $\overline{C}_{\rm d}$ is stable)**.** *If $\mathfrak{I}$ satisfies $\overline{C}_{\rm d}(\mathfrak{I}) > 0$, then there exists $\delta_0 > 0$ such that for all finite AVQCs $\mathfrak{I}'$ satisfying $D_\diamondsuit(\mathfrak{I}, \mathfrak{I}') \leq \delta_0$ it holds $C_{\rm d}(\mathfrak{I}') > 0$.*

Corollary 1. *For a sequence $(\mathfrak{I}_l)_{l\in\mathbb{N}}$ of finite AVQCs it holds: If $C_{\rm d}(\mathfrak{I}) > 0$ and $\lim_{l\to\infty} D_\diamondsuit(\mathfrak{I}, \mathfrak{I}_l) = 0$ then*

$$\lim_{l\to\infty} C_{\rm d}(\mathfrak{I}_l) = C_{\rm d}(\mathfrak{I}) \ \text{ and } \ \mathcal{A}_{\rm d}(\mathfrak{I}) = \mathcal{A}_{\rm r}(\mathfrak{I}) = \lim_{l\to\infty} \mathcal{A}_{\rm d}(\mathfrak{I}_l).$$

Theorem 4 (Random Code Reduction: finite error, finite randomness)**.** *Let $C_{\rm r}(\mathfrak{I}) > 0$ and $\lambda, \varepsilon > 0$, $0 < R < \overline{C}_{\rm r}(\mathfrak{I})$. There exist $L = L(\mathfrak{I}, \lambda, R, \varepsilon) \in \mathbb{N}$, $K = K(\mathfrak{I}, \lambda, R, \varepsilon) \in \mathbb{N}$ and $M_l \in \mathbb{N}$ satisfying $\frac{1}{l}\log M_l \geq R - \varepsilon$ such that for all $l \geq L$ there are K deterministic codes for $\mathfrak{I}$ such that:*

$$\min_{s^l\in\mathbf{S}^l} \frac{1}{K}\sum_{j=1}^{K} \frac{1}{M_l}\sum_{i=1}^{M_l} \mathrm{tr}(\mathcal{N}_{s^l}(\rho_{i,j})D_{i,j}^l) \geq 1 - \lambda.$$

Setting $E \equiv E(\mathfrak{I}, \mathrm{conv}(\mathfrak{I}))$, L and K are given by

$$L = \min\{L : L(1 - \frac{2|\mathbf{S}|\log(L)}{L(E-\varepsilon)}) \geq \frac{2}{E-\varepsilon}\log(\frac{4}{\lambda(E-\varepsilon)})\},$$
$$K = \frac{1}{\lambda}\cdot\frac{8\cdot\log|\mathbf{S}|}{E-\varepsilon}.$$

Remark 6. *It is clear that above statement is especially interesting for the message transmission capacity of an AVQC, and there only in the case when the deterministic capacity vanishes but the randomness assisted one does not.*
As a very rough approximation, one may use the scaling law $L(\mathfrak{I}, \lambda, R) \approx \frac{2}{E(\mathrm{conv}(\mathfrak{I}))-\varepsilon}\log(\frac{1}{\lambda}\cdot\frac{4}{E(\mathrm{conv}(\mathfrak{I}))-\varepsilon})$. It is clear that both L and K from above theorem are sub-optimal, even with the techniques used in this paper. However, their scaling with λ does not depend on the choice of constants in our proof. For fixed $\mathfrak{I}$ and rate R, this means that the block-length needed to achieve a certain error λ roughly scales as $\log(1/\lambda)$, and the randomness as $1/\lambda$.

Theorem 5. *Let $\mathfrak{I}$ be a finite AVQC and $\lambda \in [0,1]$. Then both*

$$\mathcal{A}_{\rm d}(\mathfrak{I}, \lambda) = \mathcal{A}_{\rm s,d}(\mathfrak{I}, \lambda) \qquad \text{and} \qquad \mathcal{A}_{\rm r}(\mathfrak{I}, \lambda) = \mathcal{A}_{\rm s,r}(\mathfrak{I}, \lambda).$$

Remark 7. *We expect this picture to change once finite block-lengths are considered. We leave this for future work.*

ACKNOWLEDGMENT

This work was supported by the DFG via grant BO 1734/20-1 (H.B.) and by the BMBF via grant 01BQ1050 (H.B., J.N.).

REFERENCES

[1] R. Ahlswede, "Elimination of Correlation in Random Codes for Arbitrarily Varying Channels", *Z. Wahrscheinlichkeitstheorie verw. Gebiete* 44, 159-175 (1978)
[2] R. Ahlswede, V. Blinovsky, "Classical capacity of classical-quantum arbitrarily varying channels", IEEE Trans. Inf. Theory, Vol. 53, No. 2, 526-533.
[3] R. Ahlswede, N. Cai, "Correlated sources help the transmission over AVC", *IEEE Trans. Inf. Th.*, Vol. 43, No. 4, 1254-1255 (1997)
[4] R. Ahlswede, I. Bjelakovic, H. Boche, J. Nötzel "Quantum capacity under adversarial noise: arbitrarily varying quantum channels", *Comm. Math. Phys.*, Vol. 317, Iss. 1, 103-156 (2013)
[5] R. Ahlswede, J. Wolfowitz, "The structure of capacity functions for compound channels", *Proc. of the Internat. Symposium on Probability and Information Theory at McMaster University, Canada*, 12-54, (1968)
[6] I. Bjelaković, H. Boche, "Classical Capacities of Averaged and Compound Quantum Channels", *IEEE Trans. Inf. Th.* Vol. 55, No. 7, 3360 - 3374 (2009)
[7] I. Bjelaković, H. Boche, J. Nötzel, "Entanglement transmission and generation under channel uncertainty: Universal quantum channel coding", *Commun. Math. Phys.* 292, 55-97 (2009)
[8] H. Boche, J. Nötzel, "Arbitrarily small amounts of correlation for arbitrarily varying quantum channels", *J. Math. Phys.* Vol. 54, 112202 (2013)
[9] H. Boche, J. Nötzel, "Positivity, Discontinuity, Finite Resources and Nonzero Error for Arbitrarily Varying Quantum Channels", *arXiv:1401.5360* (2014)
[10] I. Csiszar, P. Narayan, "The Capacity of the Arbitrarily Varying Channel Revisited: Positivity, Constraints", *IEEE Trans. Inf. Th.* Vol. 34, No. 2, 181-193 (1989)
[11] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel", *IEEE Trans. Inf. Th.* 51, No.1, 44-55 (2005)
[12] R. Duan, S. Severini, A. Winter, "Zero-error communication via quantum channels, non-commutative graphs and a quantum Lovász θ function", *IEEE Trans. Inf. Theory*, 59(2):1164-1174, (2013)
[13] T. Ericson, "Exponential Error Bounds for Random Codes in the Arbitrarily Varying Channel", *IEEE Trans. Inf. Th.* Vol. 31, No. 1, 42-48 (1985)
[14] J. Kiefer, J. Wolfowitz, "Channels with arbitrarily varying channel probability functions", *Information and Control* Vol. 5, 44-54 (1962)
[15] D. Leung, G. Smith, "Continuity of quantum channel capacities", *Commun. Math. Phys.* Vol. 292, 201-215, (2009)
[16] Quantum information problem page of the ITP Hannover, http://qig.itp.uni-hannover.de/qiproblems/11
[17] B. Schumacher, "Sending entanglement through noisy quantum channels" *Phys. Rev. A* 54, 2614 (1996)
[18] W. Rudin, *"Principles of Mathematical Analysis"*, 3rd. edition, Mc Graw-Hill, Inc. 1976