Entanglement Transmission over Arbitrarily Varying Quantum Channels

Rudolf Ahlswede*, Igor Bjelaković†, Holger Boche† and Janis Nötzel†
*Working Group Information and Complexity, Universität Bielefeld, Germany
Email: ahlswede@mathematik.uni-bielefeld.de
†Heinrich Hertz-Lehrstuhl für Informationstheorie und theoretische Informationstechnik, Technische Universität Berlin, Germany
Email: {holger.boche, igor.bjelakovic, janis.noetzel}@mk.tu-berlin.de

***Abstract*—We derive a regularized formula for the common randomness assisted entanglement transmission capacity of finite arbitrarily varying quantum channels (AVQC's). For finite AVQC's with positive capacity for classical message transmission we show, by derandomization through classical forward communication, that the random capacity for entanglement transmission equals the deterministic capacity for entanglement transmission. This is a quantum version of the famous Ahlswede dichotomy. In the infinite case, we derive a similar result for certain classes of AVQC's. At last, we give two possible definitions of symmetrizability of an AVQC.**

I. Introduction

We consider the task of entanglement transmission over an arbitrarily varying channel. This can be viewed as a three-party game in the following sense.

The sender's goal is to transmit one half of a maximally entangled state to the receiver by some (large) number of uses of a quantum channel which is under the control of a third party, called the adversary. The adversary is free to choose the channel out of a set of memoryless, partly nonstationary channels (cf. the beginning of section III). Only this given set is previously known to both sender and receiver.

To make the situation even worse, the adversary knows the encoding-decoding procedure employed by sender and receiver, so that they have to choose this procedure such that it works well for all possible choices of channels that the adversary might come up with.

Earlier results in comparable situations have been obtained by Ahlswede [1],[2],[3] for classical arbitrarily varying channels and Ahlswede and Blinovsky [4] in the case of classical message transmission over an arbitrarily varying quantum channel.

In both cases we encounter a dichotomy: Either the capacity for classical message transmission over the arbitrarily varying (quantum) channel is zero or it equals its common-randomness assisted capacity. Also, for these models there exists the notion of *symmetrizability*. This is a necessary and sufficient single-letter condition for an arbitrarily varying (quantum) channel to have zero capacity for message transmission. Our work is based on ideas mainly taken from [1], [2] and our earlier results for compound quantum channels [6].

The paper is organized as follows: In Section II we fix the basic notation. Section III introduces our channel model, in Section IV we summarize those of our results that lead to the quantum Ahlswede dichotomy. An outline of the strategy of proof is given in Section V. Finally, in Section VI we address the question of symmetrizability.

Details of the proofs given in this paper as well as the converse part of the coding theorem can be picked up in the accompanying paper [7].

II. Notation and conventions

All Hilbert spaces are assumed to have finite dimension and are over the field $\mathbb{C}$. $\mathcal{S}(\mathcal{H})$ is the set of states, i.e. positive semi-definite operators with trace 1 acting on the Hilbert space $\mathcal{H}$. If $\mathcal{F} \subset \mathcal{H}$ is a subspace of $\mathcal{H}$ then we write $\pi_{\mathcal{F}}$ for the maximally mixed state on $\mathcal{F}$, i.e. $\pi_{\mathcal{F}} = \frac{p_{\mathcal{F}}}{\mathrm{tr}(p_{\mathcal{F}})}$ where $p_{\mathcal{F}}$ stands for the projection onto $\mathcal{F}$. For a finite set A, $\mathfrak{P}(A)$ denotes the set of probability distributions on A.

The set of completely positive trace preserving (CPTP) maps between the operator spaces $\mathcal{B}(\mathcal{H})$ and $\mathcal{B}(\mathcal{K})$ is denoted by $\mathcal{C}(\mathcal{H},\mathcal{K})$. $\mathcal{C}^{\downarrow}(\mathcal{H},\mathcal{K})$ stands for the set of completely positive trace decreasing maps between $\mathcal{B}(\mathcal{H})$ and $\mathcal{B}(\mathcal{K})$.

We use the base two logarithm which is denoted by log. The von Neumann entropy of a state $\rho \in \mathcal{S}(\mathcal{H})$ is given by

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

The coherent information for $\mathcal{N} \in \mathcal{C}(\mathcal{H},\mathcal{K})$ and $\rho \in \mathcal{S}(\mathcal{H})$ is defined by

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

where $\psi \in \mathcal{H} \otimes \mathcal{H}$ is an arbitrary purification of the state ρ. Following the usual conventions we let $S_e(\rho,\mathcal{N}) := S((id_{\mathcal{B}(\mathcal{H})} \otimes \mathcal{N})(|\psi\rangle\langle\psi|))$ denote the entropy exchange.

As a measure of entanglement preservation we use entanglement fidelity. For $\rho \in \mathcal{S}(\mathcal{H})$ and $\mathcal{N} \in \mathcal{C}^{\downarrow}(\mathcal{H},\mathcal{K})$ it 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. We use the diamond norm $||\cdot||_{\diamond}$ as a measure of closeness in the set of quantum channels, which is given by

$$||\mathcal{N}||_{\diamond} := \sup_{n\in\mathbb{N}} \max_{a\in\mathcal{B}(\mathbb{C}^n\otimes\mathcal{H}),||a||_1=1} ||(id_n \otimes \mathcal{N})(a)||_1, \quad (1)$$

where $id_n : \mathcal{B}(\mathbb{C}^n) \to \mathcal{B}(\mathbb{C}^n)$ is the identity channel, and $\mathcal{N} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ is any linear map, not necessarily completely positive. The merits of $||\cdot||_\diamond$ are due to the following facts (cf. [12]). First, $||\mathcal{N}||_\diamond = 1$ for all $\mathcal{N} \in \mathcal{C}(\mathcal{H},\mathcal{K})$. Thus, $\mathcal{C}(\mathcal{H},\mathcal{K}) \subset S_\diamond$, where $S_\diamond$ denotes the unit sphere of the normed space $(\mathcal{B}(\mathcal{B}(\mathcal{H}),\mathcal{B}(\mathcal{K})), ||\cdot||_\diamond)$. Moreover, $||\mathcal{N}_1 \otimes \mathcal{N}_2||_\diamond = ||\mathcal{N}_1||_\diamond ||\mathcal{N}_2||_\diamond$ for arbitrary linear maps $\mathcal{N}_1, \mathcal{N}_2 : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$. Finally, the supremum in (1) needs only be taken over n that range over $\{1, 2, \ldots, \dim \mathcal{H}\}$.
We further use the diamond norm to define the function $D_\diamond(\cdot,\cdot)$ on $\{(\mathfrak{I},\mathfrak{I}') : \mathfrak{I},\mathfrak{I}' \subset \mathcal{C}(\mathcal{H},\mathcal{K})\}$, which is for $\mathfrak{I},\mathfrak{I}' \subset \mathcal{C}(\mathcal{H},\mathcal{K})$ given by

$$D_\diamond(\mathfrak{I},\mathfrak{I}') := \max\{\sup_{\mathcal{N}\in\mathfrak{I}} \inf_{\mathcal{N}'\in\mathfrak{I}'} ||\mathcal{N}-\mathcal{N}'||_\diamond, \sup_{\mathcal{N}'\in\mathfrak{I}'} \inf_{\mathcal{N}\in\mathfrak{I}} ||\mathcal{N}-\mathcal{N}'||_\diamond\}.$$

For compact sets, this is basically the Hausdorff distance induced by the diamond norm.
For arbitrary $\mathfrak{I},\mathfrak{I}' \subset \mathcal{C}(\mathcal{H},\mathcal{K})$, $D_\diamond(\mathfrak{I},\mathfrak{I}') \leq \epsilon$ implies that for every $\mathcal{N} \in \mathfrak{I}$ ($\mathcal{N}' \in \mathfrak{I}'$) there exists $\mathcal{N}' \in \mathfrak{I}'$ ($\mathcal{N} \in \mathfrak{I}$) such that $||\mathcal{N}-\mathcal{N}'||_\diamond \leq 2\epsilon$. In this way $D_\diamond$ gives a measure of distance between sets of channels.
For an arbitrary set $\mathbf{S}$, $\mathbf{S}^l := \{(s_1,\ldots,s_l) : s_i \in \mathbf{S}\ \forall i \in \{1,\ldots,l\}\}$. We write s^l for the elements of $\mathbf{S}^l$.
For $\mathfrak{I} \subset \mathcal{C}(\mathcal{H},\mathcal{K})$ we denote its convex hull by $conv(\mathfrak{I})$, a notation which is adapted from [14].

III. Codes for entanglement and message transmission

An arbitrarily varying quantum channel (AVQC) generated by a set $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ of CPTP maps with input Hilbert space $\mathcal{H}$ and output Hilbert space $\mathcal{K}$ is the family of CPTP maps $\{\mathcal{N}_{s^l} : \mathcal{B}(\mathcal{H})^{\otimes l} \to \mathcal{B}(\mathcal{K})^{\otimes l}\}_{l\in\mathbb{N}, s^l\in\mathbf{S}^l}$, where

$$\mathcal{N}_{s^l} := \mathcal{N}_{s_1} \otimes \ldots \otimes \mathcal{N}_{s_l} \qquad (s^l \in \mathbf{S}^l).$$

In order to relieve ourselves of the burden of complicated notation we will simply write $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ for the AVQC.
Even in the case of a finite set $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$, showing the existence of reliable codes for the AVQC $\mathfrak{I}$ is a non-trivial task, since for each block length $l \in \mathbb{N}$ we have to deal with $|\mathfrak{I}|^l$ memoryless partly non-stationary quantum channels simultaneously.
Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be an AVQC.
An $(l,k_l)-$*random entanglement transmission code* for $\mathfrak{I}$ is a probability measure μ_l on $(\mathcal{C}(\mathcal{F}_l,\mathcal{H}) \times \mathcal{C}(\mathcal{K},\mathcal{F}_l'), \sigma_l)$, where $\dim \mathcal{F}_l = k_l$, $\mathcal{F}_l \subset \mathcal{F}_l'$ and the sigma-algebra σ_l is chosen such that $F_e(\pi_{\mathcal{F}_l}, (\cdot)\circ\mathcal{N}_{s^l}\circ(\cdot))$ is measurable w.r.t. σ_l for every $s^l \in \mathbf{S}^l$. Moreover, we assume that σ_l contains all singleton sets. An example of such a sigma-algebra σ_l is given by the product of sigma-algebras of Borel sets induced on $\mathcal{C}(\mathcal{F}_l,\mathcal{H})$ and $\mathcal{C}(\mathcal{K},\mathcal{F}_l')$ by the standard topologies of the ambient spaces.

Definition 1: A non-negative number R is said to be an achievable entanglement transmission rate for $\mathfrak{I}$ with random codes if there is a sequence of $(l,k_l)-$random entanglement transmission codes such that
1) $\liminf_{l\to\infty} \frac{1}{l}\log k_l \geq R$ and
2) $\lim_{l\to\infty} \inf_{s^l\in\mathbf{S}^l} \int F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l\circ\mathcal{N}_{s^l}\circ\mathcal{P}^l) d\mu_l(\mathcal{P}^l,\mathcal{R}^l) = 1$.
The random capacity $\mathcal{A}_{\mathrm{r}}(\mathfrak{I})$ for entanglement transmission over $\mathfrak{I}$ is defined by

$$\mathcal{A}_{\mathrm{r}}(\mathfrak{I}) := \sup\{R \ : \ R \text{ is an achievable entanglement transmission rate for } \mathfrak{I} \text{ with random codes}\}.$$

We are now in a position to introduce deterministic codes: An $(l,k_l)-$code for entanglement transmission over $\mathfrak{I}$ is an $(l,k_l)-$random code for $\mathfrak{I}$ with $\mu_l(\{(\mathcal{P}^l,\mathcal{R}^l)\}) = 1$ for some encoder-decoder pair $(\mathcal{P}^l,\mathcal{R}^l)$[1] and $\mu_l(A) = 0$ for any $A \in \sigma_l$ with $(\mathcal{P}^l,\mathcal{R}^l) \notin A$. We will refer to such measures as point measures in what follows.

Definition 2: A non-negative number R is a deterministically achievable rate for entanglement transmission over $\mathfrak{I}$ if it is achievable in the sense of Definition 1 for random codes with *point measures* μ_l.
The deterministic capacity $\mathcal{A}_{\mathrm{d}}(\mathfrak{I})$ for entanglement transmission over the AVQC $\mathfrak{I}$ is given by

$$\mathcal{A}_{\mathrm{d}}(\mathfrak{I}) := \sup\{R \ : \ R \text{ is a deterministically achievable rate for entanglement transmission over } \mathfrak{I}\}.$$

Finally, we shall need the notion of the classical deterministic capacity $C_{\mathrm{det}}(\mathfrak{I})$ of the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ with *average* error criterion. An (l,M_l)-(deterministic) code for message transmission is a family of pairs $\mathfrak{C}_l = (\rho_i, D_i)_{i=1}^{M_l}$ where $\rho_1,\ldots,\rho_{M_l} \in \mathcal{S}(\mathcal{H}^{\otimes l})$, and positive semi-definite operators $D_1,\ldots,D_{M_l} \in \mathcal{B}(\mathcal{K}^{\otimes l})$ satisfying $\sum_{i=1}^{M_l} D_i = \mathbf{1}_{\mathcal{K}^{\otimes l}}$. The underlying error criterion we shall use is the worst-case average probability of error of the code $\mathfrak{C}_l$ which is given by

$$\bar{P}_{e,l}(\mathfrak{I}) := \sup_{s^l\in\mathbf{S}^l} \bar{P}_e(\mathfrak{C}_l, s^l), \tag{2}$$

where for $s^l \in \mathbf{S}^l$ we set

$$P_e(\mathfrak{C}_l, s^l) := \frac{1}{M_l}\sum_{i=1}^{M_l} \left(1 - \mathrm{tr}(\mathcal{N}_{s^l}(\rho_i)D_i)\right).$$

The achievable rates and the classical deterministic capacity $C_{\mathrm{det}}(\mathfrak{I})$ of $\mathfrak{I}$, with respect to the error criterion given in (2), are then defined in the usual way (see e.g. [4]).

IV. Main results

The compound quantum channel generated by $conv(\mathfrak{I})$ (cf. [6] for the relevant definitions) shall play the crucial role in our derivation of the coding results stated below.
Our main result, a quantum version of Ahlswede's dichotomy for finite AVQCs, goes as follows:

Theorem 3: Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC.

1) The random capacity for entanglement transmission over $\mathfrak{I}$ is given by

$$\mathcal{A}_{\mathrm{r}}(\mathfrak{I}) = \lim_{l\to\infty} \frac{1}{l} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes l})} \inf_{\mathcal{N}\in conv(\mathfrak{I})} I_c(\rho, \mathcal{N}^{\otimes l}). \tag{3}$$

[1] This explains our requirement on σ_l to contain all singleton sets.

2) Either $C_{\text{det}}(\mathfrak{I}) = 0$ or else $\mathcal{A}_{\text{d}}(\mathfrak{I}) = \mathcal{A}_{\text{r}}(\mathfrak{I})$.

Remark. It is clear from convexity of entanglement fidelity in the input state that $\mathcal{A}_{\text{d}}(\mathfrak{I}) \leq C_{\text{det}}(\mathfrak{I})$, so that $C_{\text{det}}(\mathfrak{I}) = 0$ implies $\mathcal{A}_{\text{d}}(\mathfrak{I}) = 0$. Therefore, Theorem 3 determines $\mathcal{A}_{\text{d}}(\mathfrak{I})$, in principle, up to required regularization on the right-hand side of (3) and the question of when $C_{\text{det}}(\mathfrak{I}) = 0$ happens. We derive a non-single-letter necessary and sufficient condition for the latter in Section VI.

In the case that $\mathbf{S}$ is infinite, we have the following statement:

Theorem 4: Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be any AVQC and $\partial\mathcal{C}$ the topological boundary of $\mathcal{C}(\mathcal{H}, \mathcal{K})$. If $D_\diamondsuit(\tilde{\mathfrak{I}}, \partial\mathcal{C}) > 0$, then

$$\mathcal{A}_{\text{r}}(\mathfrak{I}) = \lim_{l\to\infty} \frac{1}{l} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes l})} \inf_{\mathcal{N}\in conv(\mathfrak{I})} I_c(\rho, \mathcal{N}^{\otimes l}).$$

Remark. The condition $D_\diamondsuit(\tilde{\mathfrak{I}}, \partial\mathcal{C}) > 0$ in Theorem 4 stems from our strategy of approximation of an infinite AVQC through a sequence of finite AVQC's. We hope to be able to drop this artificial constraint in the final version of the paper.

V. Outline of the proof

This section is split into three parts. First, we demonstrate the existence of asymptotically optimal sequences of random codes (in the sense of (3)). We use Ahlswede's robustification technique originally presented in [2] in the form presented in [3] and our results on compound quantum channels [6] in order to get a sequence of finitely supported probability measures μ_l on the set of encoding and decoding maps. Second, we show that the support of each μ_l can be taken as a set with cardinality l^2.

Third, we show that $C_d(\mathfrak{I}) > 0$ implies that we can derandomize our code without any asymptotic loss of capacity, so that $\mathcal{A}_d(\mathfrak{I}) = \mathcal{A}_r(\mathfrak{I})$ holds.

Fourth, we briefly sketch how approximation of $conv(\mathfrak{I})$ by convex polytopes leads to Theorem 4.

A. Finite AVQC

Let $l \in \mathbb{N}$ and let $\mathbf{P}_l$ denote the set of permutations acting on $\{1, \ldots, l\}$. Suppose we are given a finite set $\mathbf{S}$. Then each permutation $P \in \mathbf{P}_l$ induces an action on $\mathbf{S}^l$ by $P : \mathbf{S}^l \to \mathbf{S}^l$, $P(s^l)_i := s_{P(i)}$. By $T(l, \mathbf{S})$, we denote the set of types on $\mathbf{S}$ induced by the elements of $\mathbf{S}^l$, i.e. the set of empirical distributions on $\mathbf{S}$ generated by sequences in $\mathbf{S}^l$. Now Ahlswede's robustification can be stated as follows.

Theorem 5 (Robustification technique, cf. [3]): If a function $f : \mathbf{S}^l \to [0, 1]$ satisfies

$$\sum_{s^l\in\mathbf{S}^l} f(s^l)q(s_1)\cdot\ldots\cdot q(s_l) \geq 1 - \gamma \tag{4}$$

for all $q \in T(l, \mathbf{S})$ and some $\gamma \in [0, 1]$, then

$$\frac{1}{l!}\sum_{P\in\mathbf{P}_l} f(P(s^l)) \geq 1 - (l+1)^{|\mathbf{S}|}\cdot\gamma \qquad \forall s^l \in \mathbf{S}^l. \tag{5}$$

As another ingredient for the arguments to follow we need an achievability result for the compound channel $conv(\mathfrak{I})$. We set for $k \in \mathbb{N}$

$$conv(\mathfrak{I})^{\otimes k} := \{\mathcal{N}_q^{\otimes k}\}_{q\in\mathfrak{P}(\mathbf{S})}.$$

Lemma 6: Let $k \in \mathbb{N}$. Suppose that

$$\max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes k})} \inf_{\mathcal{N}\in conv(\mathfrak{I})^{\otimes k}} I_c(\rho, \mathcal{N}) > 0$$

holds. Then for each sufficiently small $\eta > 0$ there is a sequence of (l, k_l)-codes $(\mathcal{P}^l, \mathcal{R}^l)_{l\in\mathbb{N}}$ such that for all $l \geq l_0(\eta)$ the inequalities

$$F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}^{\otimes l} \circ \mathcal{P}^l) \geq 1 - 2^{-lc} \qquad \forall \mathcal{N} \in conv(\mathfrak{I}), \tag{6}$$

$$\frac{1}{l}\log\dim\mathcal{F}_l \geq \frac{1}{k} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes k})} \inf_{\mathcal{N}\in conv(\mathfrak{I})^{\otimes k}} I_c(\rho, \mathcal{N}) - \eta, \tag{7}$$

hold with a constant $c = c(k, \dim\mathcal{H}, \dim\mathcal{K}, conv(\mathfrak{I}), \eta) > 0$.

Proof: The proof follows from an application of the compound BSST Lemma and Lemma 9 in [6]. These two statements show the existence of well behaved codes for the channels $\mathcal{N}_q^{\otimes m\cdot k}$, where m depends on $conv(\mathfrak{I})$, k and η. For fixed k, all we have to do is convert these codes to codes for the channels $\mathcal{N}_q$. ∎

In the next step we will combine the robustification technique and Lemma 6 to prove the existence of good random codes for the AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$.

Recall that there is a canonical action of $\mathbf{P}_l$ on $\mathcal{B}(\mathcal{H})^{\otimes l}$ given by $P_{\mathcal{H}}(a_1 \otimes \ldots \otimes a_l) := a_{P^{-1}(1)} \otimes \ldots \otimes a_{P^{-1}(n)}$. It is easy to see that $P_{\mathcal{H}}(a) = U_P a U_P^*$, $(a \in \mathcal{B}(\mathcal{H})^{\otimes l})$ with the unitary operator $U_P : \mathcal{H}^{\otimes l} \to \mathcal{H}^{\otimes l}$ defined by $U_P(x_1 \otimes \ldots \otimes x_l) = x_{P^{-1}(1)} \otimes \ldots \otimes x_{P^{-1}(l)}$.

Theorem 7 (Conversion of compound codes): Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC. For each $k \in \mathbb{N}$ and any sufficiently small $\eta > 0$ there is a sequence of (l, k_l)-codes $(\mathcal{P}^l, \mathcal{R}^l)_{l\in\mathbb{N}}$, $\mathcal{P}^l \in \mathcal{C}(\mathcal{F}_l, \mathcal{H}^{\otimes l}), \mathcal{R}^l \in \mathcal{C}(\mathcal{K}^{\otimes l}, \mathcal{F}_l')$, for the compound channel built up from $conv(\mathfrak{I})$ satisfying

$$\frac{1}{l}\log\dim\mathcal{F}_l \geq \frac{1}{k} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes k})} \inf_{\mathcal{N}\in conv(\mathfrak{I})^{\otimes k}} I_c(\rho, \mathcal{N}) - \eta \tag{8}$$

and, for all sufficiently large $l \in \mathbb{N}$ and $s^l \in \mathbf{S}^l$,

$$\sum_{P\in\mathbf{P}_l} \frac{1}{l!} F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ P_{\mathcal{K}}^{-1} \circ \mathcal{N}_{s^l} \circ P_{\mathcal{H}} \circ \mathcal{P}^l) \geq 1 - (l+1)^{|\mathbf{S}|}\cdot 2^{-lc}, \tag{9}$$

with a positive number $c = c(k, \dim\mathcal{H}, \dim\mathcal{K}, conv(\mathfrak{I}), \eta)$.

Proof: We let $(\mathcal{R}^l, \mathcal{P}^l)$ be as in Theorem 6. Setting $f(s^l) := F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}_{s^l} \circ \mathcal{P}^l)$ and applying Theorem 5 proves the theorem. ∎

For $l \in \mathbb{N}$, define a discretely supported probability measure μ_l by

$$\mu_l := \frac{1}{l!}\sum_{P\in\mathbf{P}_l} \delta_{(P_{\mathcal{H}}\circ\mathcal{P}^l, \mathcal{R}^l\circ P_{\mathcal{K}}^{-1})},$$

where $\delta_{(P_{\mathcal{H}}\circ\mathcal{P}^l, \mathcal{R}^l\circ P_{\mathcal{K}}^{-1})}$ denotes the probability measure that puts measure 1 on the point $(P_{\mathcal{H}} \circ \mathcal{P}^l, \mathcal{R}^l \circ P_{\mathcal{K}}^{-1})$, we obtain for each $k \in \mathbb{N}$ a sequence of (l, k_l)-random codes achieving

$$\frac{1}{k} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes k})} \inf_{\mathcal{N}\in conv(\mathfrak{I})^{\otimes l}} I_c(\rho, \mathcal{N}).$$

This leads to the following corollary to Theorem 7.

Corollary 8: For any finite AVQC $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ we have

$$\mathcal{A}_{\text{r}}(\mathfrak{I}) \geq \lim_{l\to\infty} \frac{1}{l} \max_{\rho\in\mathcal{S}(\mathcal{H}^{\otimes l})} \inf_{\mathcal{N}\in conv(\mathfrak{I})} I_c(\rho, \mathcal{N}^{\otimes l}).$$

B. Derandomization

In this section we will prove the second claim made in Theorem 3 by following Ahlswede's elimination technique. The proof is based on the following lemma, which shows that not much of common randomness is needed to achieve $\mathcal{A}_{\mathrm{r}}(\mathfrak{I})$.

Lemma 9 (Random Code Reduction): Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ be a finite AVQC, $l \in \mathbb{N}$, and μ_l an (l, k_l)-random code for the AVQC $\mathfrak{I}$ with

$$\min_{s^l\in\mathbf{S}^l} \int F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}_{s^l} \circ \mathcal{P}^l) d\mu_l(\mathcal{P}^l, \mathcal{R}^l) \geq 1 - 2^{-la} \quad (10)$$

for some positive constant $a \in \mathbb{R}$.

Let $\varepsilon \in (0, 1)$. Then for all sufficiently large $l \in \mathbb{N}$ there exist l^2 codes $\{(\mathcal{P}_i^l, \mathcal{R}_i^l) : i = 1, \ldots, l^2\} \subset \mathcal{C}(\mathcal{F}_l, \mathcal{H}^{\otimes l}) \times \mathcal{C}(\mathcal{K}^{\otimes l}, \mathcal{F}_l')$ such that

$$\frac{1}{l^2}\sum_{i=1}^{l^2} F_e(\pi_{\mathcal{F}_l}, \mathcal{R}_i^l \circ \mathcal{N}_{s^l} \circ \mathcal{P}_i^l) > 1 - \varepsilon \qquad \forall s^n \in \mathbf{S}^n. \quad (11)$$

Proof: We define random variables (Λ_i, Ω_i), $i = 1, \ldots, l^2$ with values in $\mathcal{C}(\mathcal{F}_l, \mathcal{H}^{\otimes l}) \times \mathcal{C}(\mathcal{K}^{\otimes l}, \mathcal{F}_l')$ which are i.i.d. according to $\mu_l^{\otimes l^2}$. Using Markov's inequality and the inequality $2^{\gamma t} \leq (1-t)2^{\gamma\cdot 0} + t2^{\gamma} \leq 1 + t2^{\gamma},\ t \in [0, 1], \gamma > 0$ as well as the union bound we get $\mathbb{P}\left(\frac{1}{l^2}\sum_{i=1}^{l^2} F_e(\pi_{\mathcal{F}_l}, \Lambda_i \circ \mathcal{N}_{s^l} \circ \Omega_i) > 1 - \varepsilon\ \forall s^l \in \mathbf{S}^l\right) \geq 1 - |\mathbf{S}|^l \cdot 2^{-l^2\varepsilon}$. For large enough l the above probability is positive. This shows the existence of the required realization of $(\Lambda_i, \Omega_i)_{i=1}^{l^2}$. ∎

Proof: (Of the second claim in Theorem 3). As shown above, in order to achieve $\mathcal{A}_r(\mathfrak{I})$ we need only random codes with discrete support on subexponentially many points. Whenever $C_d(\mathfrak{I}) > 0$ and $\mathcal{A}_r(\mathfrak{I}) > 0$ the sender can transmit classical information at rate zero over the AVQC in order to derandomize the code without any asymptotic reduction in the capacity for entanglement transmission. ∎

C. Infinite AVQC's

Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ with $|\mathbf{S}| = \infty$. We consider the set $\tilde{\mathfrak{I}} := \overline{conv(\mathfrak{I})}^{||\cdot||_\diamond}$ - the closure of $conv(\mathfrak{I})$ w.r.t. $||\cdot||_\diamond$. Suppose that

$$D_\diamond(\tilde{\mathfrak{I}}, \partial\mathcal{C}) =: a > 0. \quad (12)$$

Our goal is to find an outer approximation of $\tilde{\mathfrak{I}}$ in Hausdorff metric (cf. Section II) by polytopes contained entirely in the set $\mathcal{C}(\mathcal{H}, \mathcal{K})$. To this end, we need the following result of convex analysis (cf. Theorem 3.1.6, p. 109, in [14]).

Theorem 10: Let A be a non-empty compact convex set in $\mathbb{R}^d$ and let $\varepsilon > 0$. Then there exist polytopes P, Q in $\mathbb{R}^d$ such that $P \subseteq A \subseteq Q$ and $D(A, P) \leq \varepsilon$, $D(A, Q) \leq \varepsilon$, where $D(\cdot, \cdot)$ denotes the Hausdorff distance induced by the euclidean norm on $\mathbb{R}^d$.

We note that the presence of $\mathbb{R}^d$ and the euclidean norm in Theorem 10 is not essential at all. The theorem holds as well for any finite dimensional normed space with corresponding Hausdorff distance induced by the given norm.

Proof: (Of Theorem 4.) We apply Theorem 10 to the space $H(\mathcal{H}, \mathcal{K}) := \mathcal{B}_h(\mathcal{B}(\mathcal{H}), \mathcal{B}(\mathcal{K}))$ of hermiticity preserving linear maps from $\mathcal{B}(\mathcal{H})$ into $\mathcal{B}(\mathcal{K})$ endowed with $||\cdot||_\diamond$ and obtain for each $\varepsilon > 0$ a polytope $\bar{Q}_\varepsilon$ with $\tilde{\mathfrak{I}} \subseteq \bar{Q}_\varepsilon$ and $D_\diamond(\tilde{\mathfrak{I}}, \bar{Q}_\varepsilon) \leq \varepsilon$.

Let E denote the affine hull of $\mathcal{C}(\mathcal{H}, \mathcal{K})$ in $H(\mathcal{H}, \mathcal{K})$ and set $Q_\varepsilon := E \cap \bar{Q}_\varepsilon$. Then Q_ε is a polytope and for all sufficiently small $\varepsilon > 0$ ($\varepsilon \leq \frac{a}{3}$, say, is small enough for this purpose) we have $\tilde{\mathfrak{I}} \subseteq Q_\varepsilon \subset \mathcal{C}(\mathcal{H}, \mathcal{K})$ by (12). More important, we also have

$$D_\diamond(\tilde{\mathfrak{I}}, Q_\varepsilon) \leq D_\diamond(\tilde{\mathfrak{I}}, \bar{Q}_\varepsilon) \leq \varepsilon. \quad (13)$$

Let $\mathfrak{I}_\varepsilon = \{\mathcal{N}_1, \ldots, \mathcal{N}_K\}$ be the extremal points of Q_ε. Then $\mathfrak{I}_\varepsilon$ has the following properties: 1) $conv(\mathfrak{I}) \subset \tilde{\mathfrak{I}} \subset Q_\varepsilon = conv(\mathfrak{I}_\varepsilon)$, 2) $D_\diamond(\tilde{\mathfrak{I}}, conv(\mathfrak{I}_\varepsilon)) \leq \varepsilon$ for all sufficiently small $\varepsilon > 0$ by (13).

We can now apply all results from Section V-A to the finite AVQC generated by $\mathfrak{I}_\varepsilon$ giving us to each sufficiently small $\eta > 0$ and $k \in \mathbb{N}$ a sequence of (l, k_l)-random codes $(\mathcal{P}^l, \mathcal{R}^l)_{l\in\mathbb{N}}$ with $\mathcal{P}^l \in \mathcal{C}(\mathcal{F}_l, \mathcal{H}^{\otimes l})$, $\mathcal{R}^l \in \mathcal{C}(\mathcal{K}^{\otimes l}, \mathcal{F}_l')$,

$$F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}_{t^l} \circ \mathcal{P}^l) \geq 1 - (l+1)^K \cdot 2^{-lc} \qquad \forall\, t^l \in \{1, \ldots, K\}^l, \quad (14)$$

and

$$\frac{1}{l}\log k_l \geq \frac{1}{k} \inf_{\mathcal{N}\in conv(\mathfrak{I}_\varepsilon)} I_c(\rho, \mathcal{N}^{\otimes k}) - \frac{\eta}{2}, \quad (15)$$

for any $\rho \in \mathcal{S}(\mathcal{H}^{\otimes k})$ and all sufficiently large $l \in \mathbb{N}$ with a positive constant $c = c(k, \dim\mathcal{H}, \dim\mathcal{K}, \mathfrak{I}_\varepsilon, \eta)$. Since $\mathfrak{I} \subseteq \tilde{\mathfrak{I}} \subseteq conv(\mathfrak{I}_\varepsilon)$ we can find to any finite collection $\mathcal{N}_1', \ldots, \mathcal{N}_l' \in \mathfrak{I}$ probability distributions $q_1, \ldots, q_l \in \mathfrak{P}(\{1, \ldots, K\})$ with $\mathcal{N}_i' = \sum_{j=1}^K q_i(j)\mathcal{N}_j \qquad (\mathcal{N}_j \in \mathfrak{I}_\varepsilon, j \in \{1, \ldots, K\})$. Thus, for any choice of $\mathcal{N}_1', \ldots, \mathcal{N}_l' \in \mathfrak{I}$

$$F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ (\otimes_{i=1}^l \mathcal{N}_i') \circ \mathcal{P}^l) \geq 1 - (l+1)^K \cdot 2^{-lc}, \quad (16)$$

by (14). On the other hand, Lemma 16 in [6] and $D_\diamond(conv(\mathfrak{I}), conv(\mathfrak{I}_\varepsilon)) \leq D_\diamond(\tilde{\mathfrak{I}}, conv(\mathfrak{I}_\varepsilon)) \leq \varepsilon$ shows that

$$\frac{1}{l}\log k_l \geq \frac{1}{k} \inf_{\mathcal{N}\in conv(\mathfrak{I})} I_c(\rho, \mathcal{N}^{\otimes k}) - \eta, \quad (17)$$

whenever ε is small enough. It should be noted that k and l in the above equation tend to infinity when η goes to zero. Since $\eta > 0$ was arbitrary, we are done. ∎

VI. Symmetrizability

In this section we introduce a notion of symmetrizability which is a sufficient and necessary condition for $C_{\mathrm{det}}(\mathfrak{I}) = 0$. Our approach is motivated by the corresponding concept for arbitrarily varying channels with classical input and quantum output (cq-AVC) given in [4]. In what follows we will restrict ourselves to the case $|\mathbf{S}| < \infty$.

Definition 11: Let $\mathbf{S}$ be a finite set and $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ an AVQC.

1) $\mathfrak{I}$ is called l-symmetrizable, $l \in \mathbb{N}$, if for each finite set $\{\rho_1, \ldots, \rho_K\} \subset \mathcal{S}(\mathcal{H}^{\otimes l})$, $K \in \mathbb{N}$, there is a

map $p : \{\rho_1, \ldots, \rho_K\} \to \mathfrak{P}(\mathbf{S}^l)$ such that for all $i, j \in \{1, \ldots, K\}$ the following holds:

$$\sum_{s^l \in \mathbf{S}^l} p(\rho_i)(s^l)\mathcal{N}_{s^l}(\rho_j) = \sum_{s^l \in \mathbf{S}^l} p(\rho_j)(s^l)\mathcal{N}_{s^l}(\rho_i). \quad (18)$$

2) We call $\mathfrak{I}$ symmetrizable if it is l-symmetrizable for all $l \in \mathbb{N}$.

Theorem 12: Let $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$, $|\mathbf{S}| < \infty$, be an AVQC. Then $\mathfrak{I}$ is symmetrizable if and only if $C_{\text{det}}(\mathfrak{I}) = 0$.

Proof: The proof follows closely the corresponding arguments given in [11], [10], and [4]. ∎

Corollary 13: If the AVQC $\mathfrak{I} = \{\mathcal{N}\}_{s\in\mathbf{S}}$ is symmetrizable then $\mathcal{A}_{\text{d}}(\mathfrak{I}) = 0$.

Proof: Note that $\mathcal{A}_{\text{d}}(\mathfrak{I}) \leq C_{\text{det}}(\mathfrak{I})$ and apply Theorem 12. ∎

What is missing now is the reverse direction in Corollary 13: That an AVQC with $\mathcal{A}_{\text{d}}(\mathfrak{I}) = 0$ is symmetrizable. It is not known yet whether this implication is true or not.

The final issue in this section is a sufficient condition for $\mathcal{A}_{\text{r}}(\mathfrak{I}) = 0$ which is based on the notion of qc-symmetrizability. Let $\mathcal{B}_+(\mathcal{H}) \subset \mathcal{B}(\mathcal{H})$ be the set of nonnegative operators. Set

$$\text{QC}(\mathcal{H}, \mathbf{S}) := \{\{T_s\}_{s\in\mathbf{S}} \subset \mathcal{B}_+(\mathcal{H}) : \sum_{s\in\mathbf{S}} T_s = \mathbf{1}_{\mathcal{H}}\}.$$

For a given finite set of quantum channels $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ and $T \in \text{QC}(\mathcal{H}, \mathbf{S})$ we define a CPTP map $\mathcal{M}_{T,\mathbf{S}} : \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ by

$$\mathcal{M}_{T,\mathbf{S}}(a \otimes b) := \sum_{s\in\mathbf{S}} \text{tr}(T_s a)\mathcal{N}_s(b). \quad (19)$$

Definition 14: An arbitrarily varying quantum channel, generated by a finite set $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$, is called qc-symmetrizable if there is $T \in \text{QC}(\mathcal{H}, \mathbf{S})$ such that for all $a, b \in \mathcal{B}(\mathcal{H})$

$$\mathcal{M}_{T,\mathbf{S}}(a \otimes b) = \mathcal{M}_{T,\mathbf{S}}(b \otimes a) \quad (20)$$

holds, where $\mathcal{M}_{T,\mathbf{S}} : \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{K})$ is the CPTP map defined in (19).

The best illustration of the definition of qc-symmetrizability is given in the proof of our next theorem:

Theorem 15: If an arbitrarily varying quantum channel generated by a finite set $\mathfrak{I} = \{\mathcal{N}_s\}_{s\in\mathbf{S}}$ is qc-symmetrizable, then for any sequence of (l, k_l)-random codes $(\mu_l)_{l\in\mathbb{N}}$ with $k_l = \dim \mathcal{F}_l \geq 2$ for all $l \in \mathbb{N}$ we have

$$\inf_{s^l\in\mathbf{S}^l} \int F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}_{s^l} \circ \mathcal{P}^l) d\mu_l(\mathcal{R}^l, \mathcal{P}^l) \leq \frac{1}{2},$$

for all $l \in \mathbb{N}$. Thus $\mathcal{A}_{\text{r}}(\mathfrak{I}) = 0$, and consequently

$$\mathcal{A}_{\text{d}}(\mathfrak{I}) = 0.$$

Remark: Our Definition 14 addresses the notion of qc-symmetrizability for block length $l = 1$. In our accompanying paper [7] we show that the corresponding definition for arbitrary l is equivalent.

Proof: Let $l \in \mathbb{N}$. We fix $\sigma \in \mathcal{S}(\mathcal{H})$ and define $E_1, E_2 \in \mathcal{C}(\mathcal{H}, \mathcal{K})$ by $E_1(a) := \mathcal{M}_{T,\mathbf{S}}(\sigma \otimes a)$,

$$E_2(a) := \mathcal{M}_{T,\mathbf{S}}(a \otimes \sigma) = \sum_{s\in\mathbf{S}} \text{tr}(E_s a)\mathcal{N}_s(\sigma). \quad (21)$$

Setting $E_{s^l} := E_{s_1} \otimes \ldots \otimes E_{s_l}$, we can show that

$$\int F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ E_1^{\otimes l} \circ \mathcal{P}^l) d\mu_l(\mathcal{R}^l, \mathcal{P}^l) \geq \inf_{s^l\in\mathbf{S}^l} \int F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}_{s^l} \circ \mathcal{P}^l) d\mu_l(\mathcal{R}^l, \mathcal{P}^l). \quad (22)$$

Now, by the assumed qc-symmetrizability, we get

$$id_{\mathcal{F}_l} \otimes (\mathcal{R}^l \circ E_1^{\otimes l}) = id_{\mathcal{F}_l} \otimes (\mathcal{R}^l \circ E_2^{\otimes l}), \text{ thus} \quad (23)$$

$$F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ E_1^{\otimes l} \circ \mathcal{P}^l) = F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ E_2^{\otimes l} \circ \mathcal{P}^l). \quad (24)$$

But E_2 is entanglement breaking, implying that $(id_{\mathcal{F}_l} \otimes \mathcal{R}^l \circ E_2^{\otimes l} \circ \mathcal{P}^l)(|\psi_l\rangle\langle\psi_l|)$ (for a purification ψ_l of $\pi_{\mathcal{F}_l}$) is separable. A standard result from entanglement theory implies that

$$\langle\psi_l, (id_{\mathcal{F}_l} \otimes \mathcal{R}^l \circ E_2^{\otimes l} \circ \mathcal{P}^l)(|\psi_l\rangle\langle\psi_l|)\psi_l\rangle \leq \frac{1}{k_l} \quad (25)$$

holds, since ψ_l is maximally entangled with Schmidt rank k_l. Combining (22), (24), (25) and our assumption $k_l \geq 2$ we get $\inf_{s^l\in\mathbf{S}^l} \int F_e(\pi_{\mathcal{F}_l}, \mathcal{R}^l \circ \mathcal{N}_{s^l} \circ \mathcal{P}^l) d\mu_l(\mathcal{R}^l, \mathcal{P}^l) \leq \frac{1}{2}$. ∎

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, "Coloring Hypergraphs: A New Approach to Multi-user Source Coding-II", *Journal of Combinatorics, Information & System Sciences* Vol. 5, No. 3, 220-268 (1980)

[3] R. Ahlswede, "Arbitrarily Varying Channels with States Sequence Known to the Sender", *IEEE Trans. Inf. Th.* Vol. 32, 621-629, (1986)

[4] R. Ahlswede, V. Blinovsky, "Classical Capacity of Classical-Quantum Arbitrarily Varying Channels", *IEEE Trans. Int. Th.* Vol. 53, No. 2, 526-533 (2007)

[5] I. Bjelaković, H. Boche, J. Nötzel, "Quantum capacity of a class of compound channels", *Phys. Rev. A* 78, 042331, (2008)

[6] I. Bjelaković, H. Boche, J. Nötzel, "Entanglement transmission and generation under channel uncertainty: Universal quantum channel coding", *Commun. Math. Phys.* 292, 55-97 (2009) - Available at: http://arxiv.org/abs/0811.4588

[7] R. Ahlswede, I. Bjelaković, H. Boche, J. Nötzel, "Entanglement Transmission under Adversarially Selected Quantum Noise", *unpublished* - Available at: http://www.mk.tu-berlin.de/Members/Noetzel/AP.pdf

[8] D. Blackwell, L. Breiman, A.J. Thomasian, "The capacities of certain channel classes under random coding", *Ann. Math. Stat.* 31, 558-567 (1960)

[9] I. Csiszar, J. Körner, *Information Theory; Coding Theorems for Discrete Memoryless Systems*, Akadémiai Kiadó, Budapest/Academic Press Inc., New York 1981

[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] T. Ericson, "Exponential Error Bounds for Random Codes in the Arbitrarily Varying Channel", *IEEE Trans. Inf. Th.* Vol. 31, No. 1, 42-48 (1985)

[12] A.Yu. Kitaev, A.H. Shen, M.N. Vyalyi, *Classical and Quantum Computation*, Graduate Studies in Mathematics 47, American Mathematical Society, Providence, Rhode Island 2002

[13] V. Paulsen, "Completely Bounded Maps and Operator Algebras", Cambridge Studies in Advanced Mathematics vol. 78, Cambridge University Press 2002

[14] R. Webster, "Convexity", Oxford University Press 1994