Simultaneous transmission of classical and quantum information under channel uncertainty and jamming attacks

Holger Boche, Gisbert Janßen, Sajad Saeedinaeeni
Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany
Email: {boche, gisbert.janssen, sajad.saeedinaeeni}@tum.de

Abstract—We derive universal codes for simultaneous transmission of classical messages and entanglement through quantum channels, possibly under attack of a malignant third party. These codes are robust to different kinds of channel uncertainty. We show these codes to be optimal by giving a multi-letter characterization of regions corresponding to capacity of compound quantum channels for simultaneously transmitting and generating entanglement with classical messages. Also, we give dichotomy statements in which we characterize the capacity of arbitrarily varying quantum channels for simultaneous transmission of classical messages and entanglement.

A full version of this paper is accessible at: https://arxiv.org/abs/1810.10406

I. Introduction

In real world communication using quantum or classical systems, the parameter determining the channel in use may belong to an uncertainty set, rendering the protocols that assume the channel to be perfectly known practically obsolete. Here, we consider three models that include channel uncertainty without attempting to reduce it via techniques such as channel identification or tomography. We refer to these models as the compound, arbitrarily varying and fully quantum arbitrarily varying channel models. Each of these models are considered here for transmission of entanglement and classical messages simultaneously between a sender and receiver. The first two models are precisely defined in Section III and the last one in Section IV.

Simultaneous transmission of classical and quantum messages, the subject of this work, has been of interest [11]. This includes scenarios where the communication parties would like to enhance their classical message transmission by sharing quantum information primarily at their disposal or vice versa([3], [13], [14]). The body of research in this area is clearly interesting, when regions beyond those achieved by simple time-sharing between established classical message and quantum information transmission codes are reached. Examples of channels where coding beyond time-sharing is indispensable does not depend on constructing pathologies. They are readily found even within the standard arsenal of qubit quantum channels, e.g. the dephasing qubit channels [11].

The codes used here for the compound model, are different from those used for the communication over a single known channel in [11]. To derive codes robust against channel uncertainty, we refine the entanglement transmission codes for compound quantum channels from [4], [5] instead of elaborating on the usual approach building up on codes from [10] that seem not suitable when considering the compound channel.

Next, we convert the codes derived for the compound channel, using Ahlswede's robustification and elimination techniques (see [1]) to derive suitable codes for arbitrarily varying quantum channels. This is possible given that the error functions associated with codes corresponding to the compound model decay to zero exponentially. We derive a dichotomy statement (see [1]), for the simultaneous classical message and entanglement transmission through AVQCs under the average error criterion. This dichotomy is observed when considering two scenarios where the communicating parties do and do not have access to unlimited common randomness, yielding the common-randomness and deterministic capacity regions of the channel model respectively.

We give a necessary and sufficient condition for the deterministic capacity region to be be the point (0,0). This condition is known as symmetrizability of the channel (see [2] and [6]). Finally, we show that the codes derived here, can be used for fully quantum AVCs where the jammer is not restricted to product states, but can use general quantum states to parametrize the channel used many times.

In the first section following this introduction, we introduce the notation used in this work.
Precise definitions of the channel models, codes used in different scenarios along with capacity regions and finally the main results in forms of Theorem 4, Theorem 11 and Theorem 12 are given in Section III. For the precise proofs and preliminary coding results, the reader is referred to the full version of this work.

II. Notations and conventions
All Hilbert spaces are assumed to have finite dimensions and are over the field \( \mathbb{C} \). All alphabets are also assumed to have finite dimensions. We denote the set of states by \( \mathcal{S}(H) := \{ \rho \in \mathcal{L}(H) : \rho \geq 0, \text{tr} (\rho) = 1 \} \). Pure states are given by projections onto one-dimensional subspaces. To each subspace \( F \subset H \), we can associate unique projection \( q_{F} \) whose range is the subspace \( F \) and we write \( \pi_{F} \) for the maximally mixed state on \( F \), i.e. \( \pi_{F} := \frac{q_{F}}{\text{tr}(q_{F})} \).

The set of completely positive trace preserving (CPTP) maps between the operator spaces \( \mathcal{L}(H_{A}) \) and \( \mathcal{L}(H_{B}) \) is denoted by \( \mathcal{C}(H_{A}, H_{B}) \). Thus the set of completely positive trace non-increasing maps between \( \mathcal{L}(H_{A}) \) and \( \mathcal{L}(H_{B}) \) stands for the set of completely positive trace non-increasing maps between \( \mathcal{L}(H_{A}) \) and \( \mathcal{L}(H_{B}) \). We use the base two logarithm which is denoted by \( \log \). The von Neumann entropy of a state \( \rho \in \mathcal{S}(H) \) is given by \( S(\rho) := -\text{tr}(\rho \log \rho) \).

The coherent information is defined in terms of the bipartite state \( \sigma \in \mathcal{S}(H_{A} \otimes H_{B}) \) with \( \sigma := \text{id}_{H_{A}} \otimes \mathcal{N}(|\psi\rangle\langle\psi|) \) as

\[
I(A;B,\sigma) := S(\sigma^{A}) - S(\sigma)
\]

where \( \sigma^{B} \) is the marginal state given by \( \sigma^{B} := \text{tr}_{A}(\sigma) \).

As a measure of closeness between two states \( \rho, \sigma \in \mathcal{S}(H) \), we may use the fidelity \( F(\rho, \sigma) := \| \sqrt{\rho} \sqrt{\sigma} \|_{1}^{2} \). The fidelity is symmetric in the input and for a pure state \( \rho = |\psi\rangle \langle \psi| \), we have \( F(|\psi\rangle \langle \psi|, \sigma) = (\langle \phi, \sigma \phi \rangle) \). A closely related quantity is the entanglement fidelity, which for \( \rho \in \mathcal{S}(H_{A}) \) and \( N \in \mathcal{C}(H_{A}, H_{B}) \), is given by

\[
F_{e}(\rho, N) := \langle \psi, (\text{id}_{H_{A}} \otimes N)| |\psi\rangle \langle \psi| \rangle \psi
\]

with \( \psi \in \mathcal{H}_{A} \otimes H_{A} \) an arbitrary purification of the state \( \rho \).

Another quantity that will be significant in the present work is the quantum mutual information (see e.g. [19]). For a state \( \rho \in \mathcal{S}(H_{A} \otimes H_{B}) \), the quantum mutual information is defined as

\[
I(A;B,\rho) := S(\rho^{A}) + S(\rho^{B}) - S(\rho)
\]

where \( \rho^{A} \) and \( \rho^{B} \) are marginal states of \( \rho \).

We use \( \text{cl}(A) \) to denote the closure of set \( A \) and finally, we use \( \mathcal{S}_{n} \) to denote the group of permutations on \( n \) elements such that \( \alpha(\mathcal{S}) = (s_{\alpha(1)}, \ldots, s_{\alpha(n)}) \) for each \( \alpha \in \mathcal{S}_{n} \) and \( s^{n} = (s_{1}, \ldots, s_{n}) \in \mathcal{S}^{n} \).

III. Basic definitions and main results
We consider two channel models of compound and arbitrarily varying quantum channels. They are both generated by an uncertainty set of CPTP maps. For the purposes of the present work, when considering the arbitrarily varying channel model, we assume finiteness of the generating uncertainty set. This assumption is absent in the case of the compound channel model.

A. The compound quantum channel
Let \( J = \{ N_{n} \} \subseteq \mathcal{C}(H_{A}, H_{B}) \) be a set of CPTP maps. The compound quantum channel generated by \( J \) is given by family \( \{ N_{n}^{\otimes n} : N \in J \} \). In other words, using \( n \) instances of the compound channel is equivalent to using \( n \) instances of one of the channels from the uncertainty set. The users of this channel may or may not have access to the Channel State Information (CSI). We will often use the set \( S \) to index members of \( J \). A compound channel is used \( \mathrm{n} \times \mathrm{n} \) times by the sender Alice, to convey classical messages from a set \( \{ M_{1}, \ldots, M_{n} \} \) to a receiver Bob. At the same time, the parties would like to communicate quantum information. Here, we consider two scenarios in which quantum information can be communicated between the parties.

Classically Enhanced Entanglement Transmission (CET): While transmitting classical messages using \( \mathrm{n} \times \mathrm{n} \) instances of the compound channel, the sender wishes to transmit the maximally entangled state in her control to the receiver. The subspace \( F_{\infty A} \) with \( F_{\infty A} \subset H_{B}^{\otimes n} \) and \( M_{2} := \dim(F_{\infty A}) \), quantifies the amount of quantum information transmitted. More precisely:

**Definition 1.** An \((n,M_{1,n},M_{2,n})\) CET code for \( J \subseteq \mathcal{C}(H_{A},H_{B}) \), is a family \( \mathcal{C}_{\text{CET}} := (P_{m}, R_{m})_{m \in \{ M_{1,n} \}} \) with

- \( P_{m} \in \mathcal{C}(F_{\infty A}, H_{B}^{\otimes n}) \),
- \( R_{m} \in \mathcal{C}(H_{B}^{\otimes n} \otimes F_{\infty A}, F_{\infty A}) \), with \( F_{\infty A} \subset F_{\infty A} \) and
- \( \sum_{m \in \{ M_{1,n} \}} R_{m} \in \mathcal{C}(H_{B}^{\otimes n} \otimes F_{\infty A}) \)

For every \( m \in M_{1,n} \) and \( s \in S \), we define the following performance function for this communication scenario when \( n \) \( \times \) \( n \) instances of the channel have been used,

\[
P(\mathcal{C}_{\text{CET}}, N_{n}^{\otimes n}, m) := F(|m\rangle \langle m| \otimes \Phi_{AB}^{+},
\text{id}_{F_{\infty A}} \otimes R \circ N_{n}^{\otimes n} \circ P_{m}(\Phi_{AA}^{+})),
\]

where \( \Phi_{XY}^{+} \) is a maximally entangled state on \( F_{\infty A} \otimes F_{\infty A} \) and \( R := \sum_{m \in \{ M_{1,n} \}} |m\rangle \langle m| \otimes R_{m} \).

Classically Enhanced Entanglement Generation (CEG): In this scenario, while transmitting classical messages, Alice wishes to establish a pure state
shared between her and Bob. As the maximally entangled pure state shared between the parties is an instance of such a pure state, it can be proven that the previous task achieved in CET, achieves the task laid out by this one, but the opposite is not necessarily true. More precisely:

**Definition 2.** An \((n,M_1,l,M_2,n)\) CEG code for \(J \subset \mathcal{C}(\mathcal{H}_A,\mathcal{H}_B)\) is a family \(C_{\text{CEG}} := \{\Psi_m, R_m\}_{m=1}^{M_1}\), where \(\Psi_m\) is a pure state on \(\mathcal{H}_A^n \otimes \mathcal{H}_B^n\) and

1. \(R_m \in \mathcal{C}(\mathcal{H}_B^n, \mathcal{F}_B)\) with \(\mathcal{F}_B \subset \mathcal{F}_B\) and
2. \(\sum_{m \in [M_1,l]} R_m \in \mathcal{C}(\mathcal{H}_B^n, \mathcal{F}_B)\).

The relevant performance functions for this task, for every \(m \in [M_1,l]\) and \(s \in S\), are

\[
P(C_{\text{CEG}}, N^s, m) := F(m) \langle m \rangle \otimes \Phi^{AB}, \text{id}_{\mathcal{F}_A,l}, \text{id}_{\mathcal{F}_B} \otimes R \otimes N^s \otimes \Psi_m, \tag{1}\]

with \(\Phi^{AB}\) maximally entangled on \(\mathcal{F}_A \otimes \mathcal{F}_B\).

Averaging over the message set \([M_1,l]\), will give us the corresponding average performance functions denoted by \(\overline{P}(X, N^s)\) for each \(s \in S\), for \(X \in \{\text{CET}, \text{CEG}\}\). For each scenario, we define the achievable rates.

**Definition 3.** Let \(X \in \{\text{CET, CEG}\}\). A pair \((R_1, R_2)\) of non-negative numbers is called an achievable \(X\) rate for the compound channel \(J\), if for each \(\epsilon, \delta > 0\) exists a number \(n_0 = n_0(\epsilon, \delta)\) such that for each \(n > n_0\) we find an \((n,M_1,l,M_2,n)\) X code \(C_X\) such that

1. \(\frac{1}{n} \log M_1 \geq R_1 - \epsilon\) for \(i \in \{1,2\}\),
2. \(\inf_{s \in S} \min_{m \in [M_1,l]} P(C_X, N^s, m) \geq 1 - \epsilon\)

are simultaneously fulfilled. We also define \(X\) “average-error-rates” by averaging the performance functions in the last condition over \(m \in [M_1,l]\). We define the \(X\) capacity region of \(J\) by

\[
C_X(J) := \{ (R_1, R_2) \in \mathbb{R}_+^2 : (R_1, R_2) \text{ is achievable } X \text{ rate for } J \}. \tag{2}\]

Also, the capacity region corresponding to average error criterion is denoted by \(\overline{C}_X(J)\).

Moreover, let \(X\) be an alphabet, \(M \in \mathcal{C}(\mathcal{H}_A,\mathcal{H}_B)\) \(\forall s \in S\), \(p \in \mathcal{P}(X)\) and \(\Psi_s\) be a pure state for all \(x \in X\). Given the state

\[
\omega(M, p, \Psi) := \sum_{x \in X} p(x) |x\rangle \otimes \text{id}_{\mathcal{H}_A} \otimes M(\Psi_x), \tag{3}\]

we introduce the following set,

\[
\hat{C}(N^s, p, \Psi) := \{ (R_1, R_2) \in \mathbb{R}_+^2 : R_1 \leq I(X; B, \omega(N^s, p, \Psi)) \wedge R_2 \leq I(ABX, \omega(N^s, p, \Psi)) \}
\]

with \(\Psi\) denoting \(\langle \Psi_x : x \in X \rangle\) collectively. We will also use \(\frac{1}{2} \mathbb{A} := \{ |x_1, x_2\rangle : (x_1, x_2) \in A \}\). The following statement is the first main result of this paper.

**Theorem 4.** Let \(J := \{N_i\}_{i \in S} \subset \mathcal{C}(\mathcal{H}_A,\mathcal{H}_B)\) be any compound quantum channel. Then

\[
C_{\text{CET}}(J) = \overline{C}_{\text{CET}}(J) = C_{\text{CEG}}(J) = \overline{C}_{\text{CEG}}(J) = \text{cl} \left( \bigcup_{i=1}^{\infty} \bigcup_{p \in \mathcal{P}(X)} \hat{C}(N^s, p, \Psi) \right)
\]

holds.

**Proof.** For the complete proof please see the full version of this article. Therein, after proving the converse, namely that \(\overline{C}_{\text{CEG}}(J)\) is a subset of the set on the rightmost set in the above equalities, we prove that the rightmost set is a subset of \(C_{\text{CET}}(J)\). This coding theorem involves generalizing the entanglement transmission codes form \([4]\) to be combined with classical message transmission codes from \([17]\). Together with the operational inclusions

\[
C_{\text{CET}}(J) \subset C_{\text{CEG}}(J)
\]

and

\[
C_X(J) \subset \overline{C}_X(J)
\]

for \(X \in \{\text{CET, CEG}\}\), we conclude the equalities in the statement of the theorem.

\[\square\]

**B. The arbitrarily varying quantum channel**

The arbitrarily varying quantum channel generated by a set \(J := \{N_i\}_{i \in S}\) of CPTP maps with input Hilbert space \(\mathcal{H}_A\) and output Hilbert space \(\mathcal{H}_B\) is given by family of CPTP maps \(\{N_i^s : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B), s \in S, i \in [1],\} \) where \(N_i^s := N_i ⊗ N_i^s, s \in S\).

We use \(J\) to denote the AVQC generated by \(J\). To avoid further technicalities, we always assume \(|S| < \infty\) for the AVQC generating sets appearing in this paper. Most of the results in this paper may be generalized to the case of general sets by clever use of approximation techniques from convex analysis together with continuity properties of the entropic quantities which appear in the capacity characterizations (see \([2]\)).

**Definition 5.** An \((l,M_1,l,M_2,l)\) random CET code for \(J\) is a probability measure \(\mu_i\) on \((\mathcal{C}(\mathcal{F}_A,l,\mathcal{H}_A^\otimes l, M_1,l), \Omega_i)\), where

1. \(\Omega_i := \{ (R_1^{(1)}, \ldots, R_i^{(M_1,i)}), \sum_{m \in [M_1,l]} R^{(m)} \in \mathcal{C}(\mathcal{H}_B^\otimes l, \mathcal{F}_B)\}\),
2. \(\dim(\mathcal{F}_A) = M_2, \mathcal{F}_A \subset \mathcal{H}_A^\otimes l, (x \in [A, B])\).
3. The sigma-algebra \(\Omega_i\) is chosen such that the function

\[
g_{l_2}(\mathcal{P}^{(m)}, R^{(m)}) := F(m) \langle m \rangle \otimes \Phi^{AB}, \text{id}_{\mathcal{F}_A} \otimes R \otimes N^{(m)}(\Phi^{AB}) \tag{4}\]

is measurable with respect to \(\mu_i\), for all \(m \in [M_1,l], s \in S\). In \((4)\), \(\Phi^{XY}\) is a maximally entangled state on \(\mathcal{F}_X \otimes \mathcal{F}_Y\) and \(R := \sum_{m \in [M_1,l]} |m\rangle \langle m| \otimes \mathcal{R}^{(m)}\).
We further require that $\sigma_l$ contains all the singleton sets. The case where $\mu_l$ is deterministic, namely is equal to unity on a singleton set and zero otherwise, gives us a deterministic $(I, M_{l,1}, M_{l,2})$ CET codes for $J$. Abusing the terminology, we also refer to the singleton set as deterministic codes.

Definition 6. A non-negative pair of real numbers $(R_1, R_2)$ is called an achievable CET rate pair for $J := \{N_s\}_{s \in S}$ with random codes and average error criterion, if there exists a random CET code $\mu_l$ for $J$ with members of singleton sets notified by $(P(m), R(m))_{m \in [M_{l,1}]}$ such that

1) $\liminf_{l \to \infty} \frac{1}{l} \log M_{l,2} \geq R_1 \ (i \in \{1, 2\}),$
2) $\liminf_{l \to \infty} \inf_{\mu_l} \sum_{N_s} \mu_l(N_s) d_{\mu_l}(P(m), R(m))_{m = 1} \to 1.$

The random CET capacity region with average error criterion of $J$ is defined by

$$\overline{A}_{\mu_l} := \left\{(R_1, R_2): (R_1, R_2) \text{ is achievable CET rate pair for } J \text{ with random codes and average error criterion}\right\}.$$

Definition 7. A non-negative pair of real numbers $(R_1, R_2)$ is called an achievable deterministic CET rate for $J$ with average error criterion, if there exists a deterministic $(I, M_{l,1}, M_{l,2})$ CET code $(P(m), R(m))_{m \in [M_{l,1}]}$ for $J$ with

1) $\liminf_{l \to \infty} \frac{1}{l} \log M_{l,2} \geq R_1 \ (i \in \{1, 2\}),$
2) $\liminf_{l \to \infty} \inf_{\mu_l} \sum_{N_s} \mu_l(N_s) d_{\mu_l}(P(m), R(m))_{m = 1} \to 1.$

Also, the capacity region corresponding to average error criterion is denoted by $\overline{A}_{\mu_l}$. The deterministic CET codes defined here, are entanglement transmission codes for each $m \in [M_{l,1}]$. More precisely we have the following definition.

Definition 8. An $(n, M)$, $n, M \in \mathbb{N}$, entanglement transmission code for AVQC $J \subset C(H_A, H_B)$ is a pair $(P, R)$ with $P \in C(F_{A,n}, H_A^\otimes n)$, $R \in C(H_B^\otimes n, F_{B,n})$ with $F_{A,n} \subset F_{B,n} \subset H_A^\otimes n$ and $\dim(F_{A,n}) = M$. The corresponding performance function for this task is $F(\Phi^{AB}, id_{\otimes n} \otimes R \circ N_s \circ P(\Phi^{AA}))$, $s^n \in S^n$.

Essential to the statement of our results is the concept of symmetrizability defined in the following.

Definition 9. Let $J := \{N_s\}_{s \in S} \subset C(H_A, H_B)$ with $|S| < \infty$ be an AVQC.

1) $J$ is called 1-symmetrizable for $l \in \mathbb{N}$, if for each finite set $\{\rho_1, \ldots, \rho_K\} \subset S(H_A^\otimes n)$ with $K \in \mathbb{N}$, there is a map $p : [\rho_1, \ldots, \rho_K] \to P(S^l)$ such that for all $i, j \in \{1, \ldots, K\}$

$$\sum_{s' \in S^l} p(\rho_i)(s'N_s(p_j) = \sum_{s' \in S^l} p(\rho_j)(s'N_s(p_i)).$$

2) We call $J$ symmetrizable if it is 1-symmetrizable for all $l \in \mathbb{N}$.

Remark 10. The above definition for symmetrizability was first established in [2], generalizing the concept of symmetrization for classical AVQCs from [12]. This definition for symmetrizability was meaningfully simplified in [6], to require checking of the condition (5) for two input states only ($K = 2$).

The following is the second main result of this paper.

Theorem 11. Let $J := \{N_s\}_{s \in S} \subset C(H_A, H_B)$ with $|S| < \infty$ be an AVQC. The following hold.

1) $\overline{A}_{\mu_l}(J) \neq \{(0, 0)\}$ implies $\overline{A}_{\mu_l}(J) = \overline{A}_{\mu_l}(J) = \overline{A}_{\mu_l}(J) = \overline{A}_{\mu_l}(J),$

$$\text{where } \overline{A}_{\mu_l}(J) \text{ is the CET capacity of compound channel } M \text{ with average error criterion defined in the previous section and}$$
$$\text{conv}(J) := \{N_s : N_s = \sum_{s \in S} q(s)N_s, q \in P(S)\}.$$
Theorem 12. Let the capacity regions (see the full version for proof) of CPTP maps\(^1\) introduced a derandomization technique to characterize the random classical message transmission mentioned techniques were used to also characterize random codes for the AVQC from good codes postselection technique from [9] to derive correlated random codes for the AVQC for the compound channel generated by \(I := \{ N_{\sigma} := N(\sigma): \sigma \in S(H_I) \} \). In recent work [7], the above mentioned techniques were used to also characterize the random classical message transmission capacity of the AVQC. Going beyond, the authors of [7] introduced a derandomization technique to derive a dichotomy for the entanglement and classical message transmission capacities of the AVQC. Given these ideas and the results of the present paper, we derive the following characterization of the capacity regions (see the full version for proof).

Theorem 12. Let \( N \in \mathcal{C}(H_A @ H_F, H_B) \), and \( I := \{ N_{\sigma} := N(\sigma): \sigma \in S(H_I) \} \). It holds \( \mathcal{A}_{\sigma, \text{CET}}(N) = \mathcal{T}_{\text{CET}}(I) \), (dichotomy for \( \mathcal{A}_{\sigma, \text{CET}}(N) \) equals \( \{0,0\} \) or \( \mathcal{A}_{\sigma, \text{CET}}(N) \).

V. Conclusion

We have developed universal codes for simultaneous transmission of classical information and entanglement under possible jamming attacks by a third malignant party. Today, in classical systems, secure communication is obtained by applying cryptographic methods upon available reliable communication schemes. Security of the resulting protocol, that can hence be separated into two protocols (one responsible for reliability and the other for security), relies on assumptions such as non-feasibility of certain tasks or the limited computational capabilities of illegal receivers. For the next generation of classical communication systems, it is expected that different applications (e.g. secure message transmission, broadcasting of common messages and message transmission), are all implemented by physical coding or "physical layer service integration" schemes (see [18]). For quantum systems that offer a larger variety of services, [11], [13], [14] were the first papers in this line of research. The present paper develops solutions for different models of channel uncertainty that are unavoidable when implementing such integrated services in real-world communication. Following up on the results of [8], an interesting direction for future work is towards finding the solution to the arbitrarily varying model for multiple access and broadcast channels as a key step in development of quantum networks.

Acknowledgment

This work was supported by the BMBF via grant 16KIS0118K.

References

[1] R. Ahlswede. Elimination of correlation in random codes for arbitrarily varying channels. Zf. Wahrscheinlichkeitstheorie und verwandte Gebiete 44, 139-176 (1978).
[2] R. Ahlswede, I. Bjelakovic, H. Boche, J. Ñotzâl. Quantum capacity under adversarial noise: arbitrarily varying quantum channels. Communications in Mathematical Physics 317, 103-156 (2013).
[3] C. H. Bennett, P. W. Shor, J. A. Smolin, A.V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. Physical Review Letters 83, 3081-3084 (1999).
[4] I. Bjelakovic, H. Boche, J. Ñotzâl. Entanglement transmission and generation under channel uncertainty: Universal Quantum Channel Coding. Communications in Mathematical Physics 292, 55-97 (2009).
[5] I. Bjelakovic, H. Boche, J. Ñotzâl. Quantum capacity of a class of compound channels. Physical Review A 78(4), 042331 (2008).
[6] H. Boche, J. Ñotzâl. Positivity, discontinuity, finite resources, and nonzero error for arbitrarily varying quantum channels. Journal of Mathematical Physics 55, 122201 (2014).
[7] H. Boche, C. Deppe, J. Ñotzâl, A. Winter. Fully Quantum Arbitrarily Varying Channels: Random Coding Capacity and Capacity Dichotomy. Proceedings of IEEE ISIT ’18 xxx–xxx (2018).
[8] H. Boche, G. Janßen, S. Saeedinaeeni. Universal random codes: Capacity regions of the compound quantum multiple-access channel with one classical and one quantum sender. arXiv:1801.03692 (2018).
[9] M. Christandl, R. König, R. Renner. Post-selection technique for quantum channels with applications to quantum cryptography. Physical Review Letters 102, 020504 (2009).
[10] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. IEEE Transactions on Information Theory 51(1), 44-55 (2005).
[11] I. Devetak, P.W. Shor. The capacity of quantum channels for simultaneous transmission of classical and quantum information. Communications in Mathematical Physics 256(2), 287-303 (2005).
[12] T. Ericson. Exponential error bounds for random codes in arbitrarily varying channel. IEEE Transaction on Information Theory 31(1), 42-48 (1985).
[13] M.H. Hsieh and M. Wilde. Entanglement-assisted communication of classical and quantum information. IEEE Transactions on Information Theory 56 (9), 4682-4704 (2010).
[14] M.H. Hsieh and M. Wilde. Trading classical communication, quantum communication and entanglement in quantum Shannon theory. IEEE Transactions on Information Theory 56(9), 4705-4730 (2010).
[15] S. Karumanchi, S. Mancini, A. Winter, D. Yang. Quantum Channel Capacities With Passive Environment Assistance IEEE Transactions on Information Theory 62, 1733–1747 (2016).
[16] R. Klesse. Approximate quantum error correction, random codes and quantum channel capacity. Physical Review A 75, 062315 (2007).
[17] M. Mosony. Coding theorems for compound problems via quantum Rényi divergences. IEEE Transactions on Information Theory 61, 2997-3012 (2015).
[18] R.F. Schaefer, H. Boche. Physical Layer Service Integration in Wireless Networks. IEEE Signal Processing Magazine 31(3), 147-156 (2014).
[19] M. Wilde. Quantum Information Theory. 2nd Ed., Cambridge University Press (2017).