Non-additivity of Channel Capacities in the Quantum Shannon Theory

Dariusz Lasecki

July 4, 2019

Chapter 1

Introduction

1.1 Motivation

Determining the capacity of a quantum channel to transmit classical or quantum information is a fundamental problem in the Quantum Information Theory. It gives us information, in terms of the optimal asymptotic rate of transmission, on how many bit or qubits can be sent through a channel per a single use of it with assumed fidelity (usually close to perfect with a vanishing error). Despite its importance and much effort of scientists, this problem is not yet well-understood even for simple channels. It turns out that the nature of quantum channels is much richer and more complicated that one may expect. One manifestation of this is the curious phenomenon of the non-additivity of capacities of quantum channels which does not exist in the classical information theory. In this work we will summarize two important results in this area which is non-additivity of private and quantum capacities.

1.2 Definitions

Definition 1 (Quantum channel)**.** *A quantum channel is a linear map $\mathcal{N}$ which is trace preserving, completely positive and represents a quantum evolution. A quantum channel can be characterized in terms of its Stinespring representation*

$$\mathcal{N}(\rho) = \mathrm{Tr}_E(V\rho V^\dagger),$$

where V is an isometry : $A \to BE$, mapping input A to output B and environment E. Often, a complementary quantum channel $\tilde{\mathcal{N}}$ is defined as

$$\tilde{\mathcal{N}}(\rho) = \mathrm{Tr}_B(V\rho V^\dagger).$$

To quantify a channel's ability to transmit information, we are interested in determining its capacity which is a notion from the classical information theory. However, the nature of quantum channels gives rise to several types of capacities. The basic types of quantum channel capacities are classical, private and quantum. The classical capacity quantifies the amount of classical information which can be transmitted using qubits and is captured by the HSW theorem [9].

Definition 2 (Classical capacity)**.** *A classical capacity $\mathcal{C}(\mathcal{N})$ of a channel $\mathcal{N}$ is defined as*

$$\chi(\mathcal{N}) \leq \mathcal{C}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\chi(\mathcal{N}^{\otimes n}),$$

where χ is a Holevo information defined with respect to an ensemble $\{p_i, \rho_i\}$

$$\chi(\mathcal{N}) = \max_{\{p_i,\rho_i\}} \chi_{\{p_i,\rho_i\}}(\mathcal{N}),$$

where

$$\chi_{\{p_i,\rho_i\}}(\mathcal{N}) = H(\mathcal{N}(\sum_i p_i\rho_i)) - \sum_i p_i H(\mathcal{N}(\rho_i)).$$

The private capacity tells us about classical information which can be sent securely via a quantum channel which was considered by Devetak in [8]. A private capacity $\mathcal{P}(\mathcal{N})$ of a channel $\mathcal{N}$ is defined as

Definition 3 (Private capacity)**.**

$$\mathcal{P}^{(1)}(\mathcal{N}) \leq \mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} P^{(1)}(\mathcal{N}^{\otimes n}),$$

where $\mathcal{P}^{(1)}(\mathcal{N})$ is defined with respect to an ensemble $\{p_i, \rho_i\}$ as

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\{p_i,\rho_i\}} (\chi_{\{p_i,\rho_i\}}(\mathcal{N}) - \chi_{\{p_i,\rho_i\}}(\tilde{\mathcal{N}})).$$

Quantum capacity is the measure of the number of qubits which can be reliably transferred from one party to the other and the formula is the subject of the LSD theorem [8, 10, 11].

Definition 4 (Quantum capacity)**.** *A quantum capacity $\mathcal{Q}(\mathcal{N})$ of a channel $\mathcal{N}$ is defined as*

$$\mathcal{Q}^{(1)}(\mathcal{N}) \leq \mathcal{Q}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}),$$

where $\mathcal{Q}^{(1)}(\mathcal{N})$ is defined with respect to a state ρ as

$$\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho}(H(\mathcal{N}(\rho)) - H(\tilde{\mathcal{N}}(\rho))).$$

It is useful to note that

$$C(\mathcal{N}) \leq \mathcal{P}(\mathcal{N}) \leq \mathcal{Q}(\mathcal{N}).$$

Although the quantum capacity is one of the most important concepts in the Quantum Shannon Theory, it turns out to be very difficult to determine due to its definition involving the limit in infinity. Thus, people often consider an assisted quantum capacity instead which was introduced by Smith, Smolin and Winter in [5]. This quantity is usually easier to be dealt with and can provide useful bounds on the quantum capacity.

Definition 5 (Assisted quantum capacity)**.** *An assisted quantum capacity $\mathcal{Q}_{\mathcal{A}}(\mathcal{N})$ of a channel $\mathcal{N}$ assisted by a channel $\mathcal{A}$ is defined as*

$$\mathcal{Q}_{\mathcal{A}}(\mathcal{N}) = \mathcal{Q}(\mathcal{N} \otimes \mathcal{A}) = \mathcal{Q}^{(1)}(\mathcal{N} \otimes \mathcal{A}).$$

Other quantities useful when reasoning about quantum channels are mutual information and coherent information defined below.

Definition 6 (Mutual information)**.** *A mutual information between quantum systems A and B is defined as*

$$I(A : B) = H(A) + H(Y) - H(AB).$$

Definition 7 (Coherent information)**.** *A coherent information between quantum systems B and E which are output and environment of the same quantum channel $\mathcal{N}$ with an input A is defined as*

$$I_c(\mathcal{N}, \rho^A) = H(B) - H(E).$$

Chapter 2

Non-additivity of Quantum Capacity

2.1 Summary of the results

We will show that using a private Horodecki channel $\mathcal{N}_H$ (with positive private and no quantum capacity) together with a symmetric channel $\mathcal{A}$ (with no private and no quantum capacity) gives $\mathcal{Q}(\mathcal{N}_H \otimes \mathcal{A}) > 0$ which is a superactivation of quantum capacity with infinite dimensional channels (input and output are unbounded). Then, we will show that using a private Horodecki channel $\mathcal{N}_H$ together with a 50%-erasure channel $\mathcal{A}_e$ (which is a finite dimensional symmetric channel) gives $\mathcal{Q}^{(1)}(\mathcal{N}_H \otimes \mathcal{A}_e) > 0$. These results were derived by Smith and Yard in [1].

2.2 Superactivation with infinite dimensional channels

The phenomenon of superactivation of quantum channels can be exposed by showing an example of two channels which individually have zero quantum capacity but allow for quantum transmission when used jointly. To do this, we may make use of two known classes of zero-capacity channels, namely symmetric channels and entanglement-binding channels (also known as Horodecki channels [3, 4]).

Definition 8 (Bound-entanglement state)**.** *A state is a bound-entanglement state if it cannot be transformed into a pure singlet state by using local operations and classical communication, i.e. a pure singlet cannot be distilled from a bound-entanglement state.*

Definition 9 (Horodecki channel)**.** *A channel $\mathcal{N}$ is Horodecki (entanglement-binding) if and only if $(\mathbb{1} \otimes \mathcal{N})\Phi$ is a bound-entanglement state, where Φ is the maximally entangled state.*

Definition 10 (Symmetric channel)**.** *Let us define $W_d \subset \mathcal{X} \otimes \mathcal{Y}$ to be the $\frac{d(d+1)}{2}$-dimensional subspace between complex Euclidean spaces $\mathcal{X}, \mathcal{Y} \in \mathbb{C}^d$. Let V_d be the isometry which maps from $\mathbb{C}^{\frac{d(d+1)}{2}}$ to W_d. The d-dimensional symmetric channel $\mathcal{A}_d$ from $\mathbb{C}^{\frac{d(d+1)}{2}}$ to $\mathcal{X}$ is defined as*

$$\mathcal{A}_d(X) = \mathrm{Tr}_{\mathcal{Y}}\, V_d X V_d^{\dagger}.$$

Channels from these classes do not allow for the communication of quantum data and the reason for this is different for each of these classes. Symmetric channels map symmetrically between their output and environment, thus by the no-cloning argument they cannot have quantum capacity. Horodecki channels have no quantum capacity because they cannot establish states useful for entanglement distillation between the parties which results in no possibility for quantum teleportation. The situation is not improved if we combine channels from the same class together. It turns out, however, that combining symmetric and Horodecki channels can lead to a superactivation.

We will consider a private Horodecki channel which is a Horodecki channel with a positive private capacity ([6, 7]) and a symmetric channel. The starting point is the following theorem relating private and assisted quantum capacities of any channel $\mathcal{N}$

Theorem 1. *Let $\mathcal{N}$ be a channel, then*

$$\frac{1}{2}\mathcal{P}(\mathcal{N}) \leq \mathcal{Q}_{\mathcal{A}}(\mathcal{N}).$$

Proof. Recall that

$$\mathcal{Q}_{\mathcal{A}}(\mathcal{N}) = \mathcal{Q}^{(1)}_{\mathcal{A}}(\mathcal{N}) = \frac{1}{2}\max_{\rho^{XAC}}(I(X:B|C) - I(X:E|C)),$$

where the channel $\mathcal{N}$ acts on the part A of the state ρ^{XAC} and maps it to parts B and E (environment). The definition of $\mathcal{Q}^{(1)}_{\mathcal{A}}(\mathcal{N})$ is similar to the definition of the private capacity

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{X,\rho^A_X}(I(X:B) - I(X:E)),$$

where ρ^A_X is a quantum state dependent on a random variable X. Since in $\mathcal{P}^{(1)}(\mathcal{N})$ we optimize over a smaller (more constrained) set of states, it follows that $\mathcal{Q}^{(1)}_{\mathcal{A}}(\mathcal{N}) \geq \frac{1}{2}\mathcal{P}^{(1)}(\mathcal{N})$ and therefore $\mathcal{Q}_{\mathcal{A}}(\mathcal{N}) \geq \frac{1}{2}\mathcal{P}(\mathcal{N})$. □

Using the theorem above, we conclude that for a private Horodecki channel $\mathcal{N}_H$ (which has $\mathcal{P}^{(1)}(\mathcal{N}_H) > 0$) assisted by a symmetric channel $\mathcal{A}$ the following holds

$$\mathcal{Q}_{\mathcal{A}}(\mathcal{N}_H) = \mathcal{Q}(\mathcal{N}_H \otimes \mathcal{A}) > 0.$$

2.3 Superactivation with finite dimensional channels

The superactivation result from the previous section was proved for channels with infinite input and output dimensions (due to regularization of quantum capacity). Although it is a strong theoretical result, it would be of great operational importance to show the same for a finite dimensional case. It can be shown that the similar phenomenon appears considering a finite case. It is based on the fact proved by Devetak in [8] that a bound

$$I(X:B) - I(X:E) \leq \mathcal{P}^{(1)}(\mathcal{N})$$

evaluated on the state

$$\rho^{XBE} = \sum_x p_x \left|x\right\rangle \left\langle x\right|^X \otimes \rho^{BE}_x$$

can be saturated using a finite ensemble as long as an input ρ^A_x to a channel (which results in a state ρ^{BE}_x after transmission) has a finite dimension. We will show the finite variant of the superactivation of a quantum capacity using a private Horodecki channel $\mathcal{N}_H$ ($\mathcal{P}^{(1)}(\mathcal{N}_{\mathcal{H}}) > 0$) assisted by a finite dimensional 50%-erasure channel $\mathcal{A}_e$ which is a member of a symmetric channels class.

Definition 11 (50%-erasure channel)**.** *The channel* Ξ *is the* 50%*-erasure channel if*

$$\Xi(X) = \frac{1}{2}X + \frac{1}{2}\operatorname{Tr}(X)\epsilon_{err}$$

where ϵ_{err} *is a symbol indicating an error.*

We will now present a theorem which holds for any channel $\mathcal{N}$ assisted by a 50%-erasure channel and then use it to show a superactivation for Horodecki channels. The theorem relates a coherent information I_c of an assisted transmission to a mutual information between an input and its outputs. We recall that the non-regularized quantum capacity is defined as $\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A}(H(B) - H(E)) = \max_{\rho^A}(I_c(\mathcal{N}, \rho^A))$ which will let us reason about the quantum capacity in this finite case.

Theorem 2. *Suppose we have an ensemble* $\{p_x, \rho_x^A\}$*, a channel* $\mathcal{N}$ *which maps* $A \to BE$ *and a* 50%*-erasure channel* $\mathcal{A}_e$ *which maps* $C \to DF$ *and which dimension of the input* C *equals the sum of the ranks of the states* ρ_x^A*. Then there exists a state* ρ^{AC} *such that*

$$I_c(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = \frac{1}{2}(I(X:B) - I(X:E)).$$

Proof. Let us consider a quantum state ρ^{AC} to be sent through channels $\mathcal{N}$ and $\mathcal{A}_e$. We consider the purification of the state ρ^{AC} which is

$$|\rho^{XAC}\rangle = \sum_x \sqrt{p_x}\, |x\rangle^X |\rho_x\rangle^{AC},$$

where $|\rho_x\rangle^{AC}$ are purifications of ρ_x^A and ρ_x^C have disjoint supports. From the definition of the coherent information we have

$$I_c(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = H(BD) - H(EF).$$

Considering the action of the 50%-erasure channel, we know that it either transmits C successfully with a probability $\frac{1}{2}$ and declares it as its output D or, with a probability $\frac{1}{2}$, transmits it to its environment F. Thus, we can rewrite

$$I_c(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = \frac{1}{2}(H(B) - H(EC)) + \frac{1}{2}(H(BC) - H(E)).$$

Using the assumption that we deal with purified states and the fact that for any pure states their bipartition has the same entropy, we have

$$I_c(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = \frac{1}{2}(H(B) - H(XB)) + \frac{1}{2}(H(XE) - H(E)),$$

what can be expressed in terms of the mutual information

$$I_c(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = \frac{1}{2}(I(X:B) - I(X:E)).$$

□

Let us consider a Horodecki channel $\mathcal{N}_H$ for which it holds that $\mathcal{P}^{(1)}(\mathcal{N}_H) > 0$ (all currently known private Horodecki channels have this property). From the definition of $\mathcal{P}^{(1)}$ we know that there exists an ensemble $\{p_x, \rho_x^A\}$ such that $I(X:B) - I(X:E) = \mathcal{P}^{(1)}(\mathcal{N}_H)$. For such an ensemble it follows that

$$I(X:B) - I(X:E) > 0,$$

where B and E are output systems of $\mathcal{N}_H$.
Together with this observation, we can apply the Theorem (2) to a Horodecki channel $\mathcal{N}_H$, which implies that there exists a state ρ^{AC} such that

$$I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho^{AC}) = \frac{1}{2}(I(X:B) - I(X:E)) > 0.$$

Thus, we conclude that

$$\mathcal{Q}^{(1)}(\mathcal{N}_H \otimes \mathcal{A}_e) = \max_{\rho^{AC}}(I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho^{AC})) > 0.$$

Chapter 3

Non-additivity of Private Capacity

3.1 Summary of the results

We will show how to construct a special type of a channel denoted by $\tau^k_{\mathcal{N}}$ which is based on any channel $\mathcal{N}$. We will show that using $\tau^k_{\mathcal{N}}$ together with a 50%-erasure channel $\mathcal{A}$ which has no private and no quantum capacity, we have $\mathcal{Q}(\tau^k_{\mathcal{N}} \otimes \mathcal{A}) > \mathcal{Q}(\tau^k_{\mathcal{N}})$ and $\mathcal{P}(\tau^k_{\mathcal{N}} \otimes \mathcal{A}) > \mathcal{P}(\tau^k_{\mathcal{N}})$. This result is an example of the non-additivity of both quantum and private capacity. This result was derived by Li, Winter, Zou and Guo in [2].

3.2 The special type of a channel

To demonstrate the non- additivity of the private capacity, we will use a special type of a channel $\tau^k_{\mathcal{N}}$ depicted in Fig. 3.1. Its construction is based on the idea of giving Bob access not only to an output system B of a certain channel $\mathcal{N}$ but also to a system which is usually referred to as an environment E. However, if we recall the Stinespring representation of a quantum channel

$$\mathcal{N}(\rho) = \mathrm{Tr}_E\, V\rho V^{\dagger},$$

where V is an isometry, we see that Bob having both $\mathcal{N}(\rho)$ and environment E can always perfectly recover the state ρ by reverting the isometry V. To make the situation the same as normally from the Bob's point of view, we introduce a channel $\tau^k_{\mathcal{N}}$ which incorporates the channel of our interest $\mathcal{N}$ and additionally randomizes its output E to a maximally mixed state via the random application of one of the discrete Weyl operators $W_j (j = 1, ..., |E|^2)$. Thus, if j is not known to Bob, he obtains a state $\mathcal{N}(\rho)^B \otimes \frac{1}{|E|^2}\mathbb{1}^E$. The extra system E does not provide any information to Bob so the channel $\tau^k_{\mathcal{N}}$ is informationally equivalent to $\mathcal{N}$. We will show however, that if $\tau^k_{\mathcal{N}}$ is used together with another channel, the randomized system E can make a significant difference for the joint capacity of both channels.

3.3 The violation of additivity of the private capacity

Theorem 3. *Suppose we have a channel $\mathcal{N}$ which maps $A \to BE$, an integer k and a function $\delta(k) = \frac{1}{k}(5 + 4\log|E|)$. For any channel Ψ it holds that*

$$\chi(\mathcal{N} \otimes \Psi) \le \chi(\tau^k_{\mathcal{N}} \otimes \Psi) \le \chi(\mathcal{N} \otimes \Psi) + \delta(k).$$

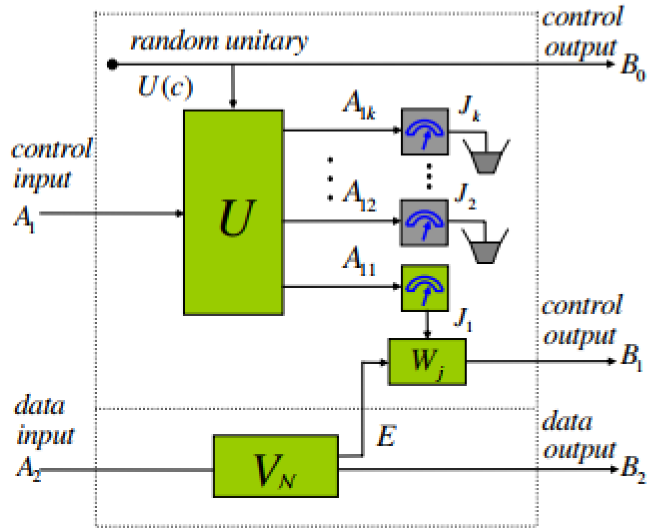

Figure 3.1: The scheme of the channel $\tau_{\mathcal{N}}^k$ (image taken from [2])

As a result,

$$C(\mathcal{N}) \leq C(\tau_{\mathcal{N}}^k) \leq C(\mathcal{N}) + \delta(k).$$

Proof. The proof of this theorem is somewhat involved and can be found in [2]. □

Using known inequalities for the relationship between types of capacities

$$C(\mathcal{N}) \leq \mathcal{P}(\mathcal{N}) \leq \mathcal{Q}(\mathcal{N}),$$

we can apply the theorem above to the obtain

$$\mathcal{P}(\tau_{\mathcal{N}}^k) \leq C(\tau_{\mathcal{N}}^k) \leq C(\mathcal{N}) + o(1)$$

what will be useful in a moment. Now, we will introduce a certain communication scenario which will give us a relationship between $\mathcal{P}(\tau_{\mathcal{N}}^k \otimes \mathcal{A})$, $\mathcal{Q}(\tau_{\mathcal{N}}^k \otimes \mathcal{A})$ and $\mathcal{Q}_E(\mathcal{N})$, where $\mathcal{A}$ is again a 50%-erasure channel.

Let us consider channels $\tau_{\mathcal{N}}^k$ and $\mathcal{A}$. For the channel $\tau_{\mathcal{N}}^k$ we will use labels as in Fig. 3.1. Assume that we have a maximally entangled state Φ^{A_1C} with each half fed into A_1 and C respectively, where C is an input to a channel $\mathcal{A}$. Another state ρ_{A_2} with a purification $|\varphi\rangle^{AA_2}$ is fed into A_2 and A is kept by a sender. Thus, our full input state is $\sigma^{A_1A_2C} = \Phi^{A_1C} \otimes \rho^{A_2}$. We can express the transmitted state as

$$\omega^{AB_0B_1B_2CD} = (\mathbb{1}_A \otimes \tau_{\mathcal{N}}^k \otimes \mathcal{A}_C)(\Phi^{A_1C} \otimes \varphi^{AA_2}).$$

We are interested in evaluating the coherent information I_c with respect to this state because I_c is a lower bound on the quantum capacity which is a lower bound on a private capacity. We have

$$I_c(\sigma^{A_1A_2C}, \tau_{\mathcal{N}}^k \otimes \mathcal{A}) = H(B_1B_2CD|B_0) - H(AB_1B_2CD|B_0).$$

Using the same trick as in the previous chapter, we may consider the coherent information in cases which depend on whether the 50%-erasure channel transmitted a state successfully or with an error

$$I_c(\sigma^{A_1A_2C}, \tau_{\mathcal{N}}^k \otimes \mathcal{A}) = \frac{1}{2}(I_c^{erased} + I_c^{not-erased}).$$

If the 50%-erasure channel erases its input, then systems C, B_0 and B_1 convey no information to Bob. It means that systems B_2 and CB_0B_1 are decoupled. In this case, the coherent information is

$$I_c^{erased} = H(B_2) - H(AB_2) = H(\mathcal{N}(\rho)) - H((\mathbb{1} \otimes \mathcal{N}) \left|\varphi\right\rangle \left\langle\varphi\right|^{AA_2}).$$

If the 50%-erasure channel transmits its input with no error, then Bob has a possibility to correct errors which occurred in the transmission through the channel $\mathcal{N}$. The register B_0 has information on which unitary transformation was applied to A_1 and the measurement of C in a proper basis can reveal a parameter j which will allow him to apply $W_j^\dagger$ to B_1 and revert the randomization. It means that at the end of this protocol, Bob possesses both the output of $\mathcal{N}$ and the related environment which are undisturbed inputs (a perfect transmission occurred). We note that in this scenario systems AB_1B_2 and B_0C are decoupled, therefore

$$I_c^{not-erased} = H(B_1B_2) - H(AB_1B_2) = H(\rho^{A_2}).$$

Having considered both bases, we may write

$$I_c(\sigma^{A_1A_2C}, \tau_{\mathcal{N}}^k \otimes \mathcal{A}) = \frac{1}{2}(H(\mathcal{N}(\rho)) - H((\mathbb{1} \otimes \mathcal{N}) \left|\varphi\right\rangle \left\langle\varphi\right|^{AA_2}) + H(\rho^{A_2})).$$

In [12] it was shown by Bennett, Shor, Smolin and Thapliyal that

$$\mathcal{Q}_E(\mathcal{N}) = \max_\rho I_c(\Phi \otimes \rho, \tau_{\mathcal{N}}^k \otimes \mathcal{A}).$$

Therefore, we can write the following relationship

$$\mathcal{P}(\tau_{\mathcal{N}}^k \otimes \mathcal{A}) \geq \mathcal{Q}(\tau_{\mathcal{N}}^k \otimes \mathcal{A}) \geq \mathcal{Q}_E(\mathcal{N}),$$

where we used the fact that $\mathcal{Q}(\tau_{\mathcal{N}}^k \otimes \mathcal{A})$ is known to be lower bounded by the coherent information. Let us consider channels for which $Q_E(\mathcal{N}) > C(\mathcal{N})$ (an example is a d-dimensional Depolarizing Channel). Then, using the relationship above, Theorem (3) and $\mathcal{P}(\tau_{\mathcal{N}}^k) \leq C(\tau_{\mathcal{N}}^k) \leq C(\mathcal{N}) + o(1)$ derived before, we have

$$\mathcal{P}(\tau_{\mathcal{N}}^k \otimes \mathcal{A}) \geq \mathcal{Q}(\tau_{\mathcal{N}}^k \otimes \mathcal{A}) > \mathcal{P}(\tau_{\mathcal{N}}^k) \geq Q(\tau_{\mathcal{N}}^k),$$

where k is chosen to be large enough so that above holds. If we recall that the symmetric channel $\mathcal{A}$ has both no quantum and private capacity, we clearly see the violation of the additivity of private capacity and quantum capacity as well.

Chapter 4

Summary

We described first results which exposed the non-additivity of the capacities of quantum channels. Violations of additivity were shown by constructing specific examples of channels and computing their single and combined capacities. We learned that both private and quantum capacities are not additive. This counter-intuitive phenomenon brings even more questions to the area of quantum communication. For instance, we should be interested in learning more about classes of zero-capacity channels, developing a more comprehensive categorization of such channels and understanding reasons for having no quantum capacity. Hopefully, doing more research in this matter will let us better understand the field of quantum communication.

Bibliography

[1] G. Smith, J. Yard, *Science* **321**, 1812-1815 (2008).

[2] K. Li, A. Winter, X.Zou, G. Guo, *Physical Rev. Lett.* **103**, 120501 (2009).

[3] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).

[4] P. Horodecki, *Phys. Lett. A* **232**, 333 (1997).

[5] G. Smith, J. Smolin, A. Winter, The quantum capacity with symmetric side channels. `arXiv:quant-ph/0607039`.

[6] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *Phys. Rev. Lett.* **94**, 160502 (2005).

[7] K. Horodecki, L. Pankowski, M. Horodecki, P. Horodecki, *IEEE Trans. Inform. Theory* **54**, 2621 (2008).

[8] I. Devetak, *IEEE Trans. Inform. Theory* **51**, 44 (2005).

[9] A. S. Holevo, IEEE Trans. Inf. Theory **44**:269 (1998); B. Schumacher, M. D. Westmoreland, Phys. Rev. A **56**:131 (1997).

[10] S. Lloyd, Phys. Rev. A **55**:1613 (1997).

[11] P. W. Shor, http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/.

[12] C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal, Phys. Rev. Lett. **83**:3081 (1999) and IEEE Trans. Inf. Theory **48**:2637 (2002).