Universidade Estadual de Campinas

Instituto de Física "Gleb Wataghin"

Leandro Raffhael da Silva Mendes

Structure of States Saturating the Bounded Strong Sub-additivity and Quantum Channels

Estrutura de Estados que Saturam a Subaditivitdade Forte Limitada e Canais Quânticos

CAMPINAS
2016

Leandro Raffhael da Silva Mendes

Structure of States Saturating the Bounded Strong Sub-additivity and Quantum Channels

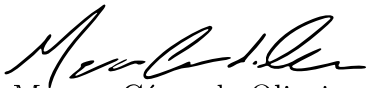
Estrutura de Estados que Saturam a Subaditivitdade Forte Limitada e Canais Quânticos

Dissertation presented to the Institute of Physics "Gleb Wataghin" of the University of Campinas in partial fulfillment of the requirements for the degree of Master in Physics

Dissertação apresentada ao Instituto de Física "Gleb Wataghin" da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Mestre em Física.

Supervisor: Dr. Marcos César de Oliveira
Co-supervisor: Dr. José Antonio Roversi

Este exemplar corresponde à versão final da dissertação defendida pelo aluno Leandro Raffhael da Silva Mendes e orientada pelo Prof Dr. Marcos César de Oliveira



Marcos César de Oliveira

CAMPINAS
2016

Agência(s) de fomento e nº(s) de processo(s): CAPES, 1247649/2013

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Física Gleb Wataghin
Lucimeire de Oliveira Silva da Rocha - CRB 8/9174

M522s

Mendes, Leandro Raffhael da Silva, 1990-
Structure of states saturating the bounded strong sub-additivity and quantum channels / Leandro Raffhael da Silva Mendes. – Campinas, SP : [s.n.], 2016.

Orientador: Marcos César de Oliveira.
Coorientador: José Antonio Roversi.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Física Gleb Wataghin.

1. Informação quântica. 2. Emaranhamento quântico. 3. Entropia quântica. I. Oliveira, Marcos César de,1969-. II. Roversi, José Antonio,1947-. III. Universidade Estadual de Campinas. Instituto de Física Gleb Wataghin. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Estrutura de estados que saturam a subaditividade forte limitada e canais quânticos
Palavras-chave em inglês:
Quantum information
Quantum entanglement
Quantum entropy
Área de concentração: Física
Titulação: Mestre em Física
Banca examinadora:
Marcos César de Oliveira [Orientador]
Márcio Fernando Cornélio
Marcus Vinicius Segantini Bonança
Data de defesa: 21-03-2016
Programa de Pós-Graduação: Física

MEMBROS DA COMISSÃO JULGADORA DA DISSERTAÇÃO DE MESTRADO DE **LEANDRO RAFFHAEL DA SILVA MENDES - RA 151606** APRESENTADA E APROVADA AO INSTITUTO DE FÍSICA "GLEB WATAGHIN", DA UNIVERSIDADE ESTADUAL DE CAMPINAS, EM 21 / 03 / 2016.

COMISSÃO JULGADORA:

- Prof. Dr. Marcos Cesar de Oliveira – Orientador – DFMC/IFGW/UNICAMP
- Prof. Dr. Márcio Fernando Cornélio – IF/UFMT
- Prof. Dr. Marcus Vinicius Segantini Bonança – DFMC/IFGW/UNICAMP

OBS.: Informo que as assinaturas dos respectivos professores membros da banca constam na ata de defesa já juntada no processo vida acadêmica do aluno.

CAMPINAS
2016

Abstract

We studied the structure of states that saturate the bounded strong subbaditivity of von Neumann entropy. This was done by rearranging the form of the measures presented in the inequality, in such a way that the Petz theorem could be used. After the application of a recovery map we see that the resulting states require the entanglement of formation for a tripartite and bipartite case to be equal, or in other words, it requires monogamy of the entanglement of formation. We also analyzed the implications of the bounded relation into the quantum data processing inequality. It is seen that a bound is extended from the strong subbaditivity to the data processing inequality, but with different terms, with further manipulations we show that the bound can be expressed in terms of the net flow of locally inaccessible information in the first stage and the net flow on the second stage. Were the difference between the coherent information relative to two parties in the process of transmitting a state is lower bounded by the difference on the net flows.

Keywords: Quantum information, Strong subadditivity, quantum channels.

Resumo

Estudamos a estrutura de estados que saturam a desigualdade de subaditividade forte da entropia de von Neumann. Isto foi feito rearranjando a forma das medidas apresentadas na desigualdade, de tal maneira que o teorema de Petz pudesse ser utilizado. Após a aplicação de um mapa de recuperação, vemos que os estados resultantes requerem que o emaranhamento de formação para um estado tripartido e para um estado bipartido sejam iguais, ou em outras palavras, exige a existência de monogamia do emaranhamento de formação. Também foram analisadas as implicações da relação de subaditividade na desigualdade de processamento de dados quântica. Nós vemos que o limitante existente na relação anterior é estendido à desigualdade de processamento de dados, mas com uma forma diferente. Manipulando o limitante nós conseguimos escreve-lo como sendo a diferença entre o fluxo resultante de informação localmente inacessível na primeira fase do processamento de dados e o fluxo resultante no segundo estágio do processo. Isto mostra que a diferença entre a informação coerente em relação a duas partes que estão processando um estado é limitada inferiormente pela diferença desses dois fluxos.

Palavras-chave: Informação quântica, subaditividade forte, canais quânticos.

Agradecimentos

Agradeço primeiramente a minha mãe pelo esforço e apoio durante os anos, mesmo nas vezes que tinhamos opiniões contrárias. A minha namorada pelo suporte que mesmo longe sempre esteve lá. Aos amigos que fiz durante o mestrado por tornar o tempo em Barão Geraldo mais agradável. Ao meu orientador Marcos César de Oliveira, por ter acreditado em mim e pelas horas de discussão, aprendi muito durante estes dois anos. Também ao meu coorientador José Antônio Roversi pela simpatia e disponibilidade. Sem estes dois esta dissertação não teria sido feita. E finalmente à CAPES pelo apoio financeiro.

Contents

Chapter 1

Introduction

Finding a way to send and receive messages is a primal factor for any society, from military applications, safe bank transfers to simple communication between parts. So it is a logical step to look for more efficient ways for the transmission of required information. For that it is necessary to better understand the nature of information and the fundamental laws that its processing obeys independently of the physical system employed. The first time that a mathematical treatment for the transmission of information was presented was in Claude Shannon's work entitled "The Mathematical Theory of Communication" [1]. In this work Shannon defines what is important in a general theory of information, stating what is a communication system by its different parts:

- The source for information that will create the message;
- The transmitter that is going to transmit the message using some device;
- The method by which it is going to be sent and
- The receiver of the message.

For Shannon every message could be broken into simple *yes* or *no* questions, expressed by the *bit*. The other important contribution was a quantity to measure the information produced or the rate of the information. This measure is known today as the Shannon entropy

$$H(p_1, p_2..p_n) = -\sum_i^n p_i \log p_i, \tag{1.0.1}$$

being function of the probabilities for a certain random variable outcomes. This function was chosen due to the properties that are expected from a measure of information. It is continuous in the probabilities; it is a monotonic increasing function in n when $p = \frac{1}{n}$; and in a succession of events, when one event is broken down into equal probabilities, the entropy $H(p_1, p_2..p_n)$ is the weighted sum of the Shannon entropy of each value, given by the probabilities. In the recent

years the interest on the capabilities for communication employing quantum systems grew larger, giving origin to the field of quantum information science, that encompasses quantum computation, quantum information theory and others. It is common to refer to Shannon's work as the classical part of the field of information. The quantum part also shares similar elements from the classical part, needing a source for the states that are going to be sent, a way to sent those, that are referred as quantum channels, channel or simply by maps. Also in quantum information the agent is not the bit but the quantum bit, or simply the *qubit*, with the main difference being that thanks to the superposition principle [2] the coding is not only represented in terms of *yes* or *no* questions but in every possible superposition of them. The channel or map are superoperators that take the states represented by density matrices to density matrices. We are not going to give much attention to the classical part, besides for intuition, since the quantum domain is the main focus of this work. Also, like the classical part, quantum information has a measure of information, the von Neumann entropy,

$$S(\rho) = -\mathrm{Tr}\rho \log \rho. \tag{1.0.2}$$

This function has similar properties to the Shannon entropy, but in relation to the density operator ρ. Just to list a few, it is a concave function, it is nonnegative (were it is equal to zero only if ρ is a pure state) and is an additive function.

Even though they share various similarities the differences that they hold give rise to unique phenomena and turn the von Neumann entropy into an interesting measure. A lot of research was done focusing on the properties of the von Neumann entropy, since those properties are directly connected with the possibilities in quantum information theory, such as the proofs in channel capacities [3], finding lower bound on the free energy [4], reconstruction of states [5] and so on. Many properties were first presented by Delbrück and Molìiere [6] but the one in particular that drew a great deal of attention, was the property of strong subadditivity. This relation is an inequality relating the subparts of a tripartite system among themselves and in relation to the global state. It was elusive for some time, first conjectured in 1968 [39], due to the difficulty to perform a proof, even though it was easy for the Shannon entropy. It was only demonstrated to hold for the von Neumann entropy in 1975 [41]. It is not very intuitive at first sight but the strong subadditivity inequality turned to be very important because it establishes connections to several other inequalities and results in quantum information theory and it is even referred to as the only inequality in quantum information theory [9]. Recently with the result of Omar Fawzi and Renato Renner [7] new interest arose for the conditional quantum mutual information, which is equivalent to the strong subadditivity inequality.

It was in Hayden et al [8] that they studied the structure of states that would saturate this important inequality. From the Markov condition for the tripartite state of a system and using a recovery channel, they could describe the structure of the states that would saturate with

equality the strong subadditivity. It was later seen that one of the corollaries of the result of Hayden et. al. is the only known inequality to not come directly from the strong subadditivity. It is a constrained inequality that is only true when certain conditions are met for any four part system [9].

In 2011 the strong subadditivity was presented in a different way. Studying the monogamy relations of Winter et al. [47], Fanchini et al [46] obtained the same relation with the addendum of a possible lower bound for the inequality. This bound was dependent on the balance of quantum correlations shared between subsystems of a tripartite state, measured by the entanglement of formation and the quantum discord of those subsystems. The two measures are related to different phenomena: the entanglement of formation is related to the entanglement on the subsystems; and the quantum discord is associated to the quantumness presented on the subsystems[1]. The latter is a measure on how much a bipartite quantum system is affected by local measurements that can exist even in separable states, fact that is not possible with entanglement measures. So the possibility of the lower bound depends on the difference of the quantum correlations that are shared among parts of the subsystems in relation to those measures. As the entanglement of formation can be greater, equal or less than the quantum discord, this varies according to the state in question.

In this work it is asked the question: what is the structure of states that is going to saturate the strong subadditivity given that bound that was achieved? We do that following a similar reasoning to the work of Hayden et al. making use of a recovery channel after obeying equality conditions due to a theorem from Dénes Petz [8]. We also analyze the implications of the bounded relation on the data processing inequality [12]. The data processing inequality states that during the processing of information, a process that can be characterized by the coding, sending and decoding of a certain message, will always decrease the quantum correlations that are carried during the transmission of that message [14, 15].

Now we are going to describe the content of each Chapter: In Chapter 2 we give an overview of the classical and quantum theory of information. It introduces the Shannon and von Neumann entropies, the conditional entropy, relative entropy and mutual information establishing the base for the following chapters and results. In Chapter 3 we present the concept of entanglement and quantum discord as a whole and how it is related to the quantum theory of information. Some important measures of quantum correlations such the entanglement of formation, entanglement cost, distillable entanglement and the context for their definition, shown in terms of protocols of purification are also described. Chapter 4 is where we show the development for the quantum operations formalism, through the trace of the environment after the dynamics occurred to the description of the Kraus operators. We also introduce in this chapter the concept of quantum channels and the quantum data processing inequality. Chapter 5 holds

[1] See however [32]

the original results that were developed during this work, where we show the strong subadditivity with bounds exploring the structure of states that saturates the inequality. We also see the implications of this new bounded strong subadditivity in the quantum data processing inequality. The last chapter is used to conclude this dissertation.

Chapter 2

Entropies

2.1 Von Neumann Entropy

In order to better understand the von Neumann entropy, as the other entropies, we are always going to start with its classical part, so we begin talking about the Shannon entropy. This quantity is the answer for a number of questions, specifically if there is a way of conveying a message with the shortest possible length of a string on average. More important to us is that the Shannon entropy measures the information that we gain in learning the value of some random variable X or analogously, the uncertainty that we have about X prior to learning its value (also on average). A random variable is different from the normal variables that we encounter because it does not take one single value but represents a set of different possible values and each of those have probabilities associated with them. One simple example is a random event like a coin toss where the possible results are heads or tails, if the coin is fair each associated probability is 1/2, if not that changes. For a little more sophisticated example lets suppose that we have a source that transmits messages in form of a random sequence $\{x_1, .., x_n\}$ and associated with every element of this sequence we have a probability distribution $\{p_1, .., p_n\}$. Then the Shannon entropy of the random variable X that represents our random sequence is given by

$$H(X) \equiv -\sum_i p_i \log p_i, \tag{2.1.1}$$

where the logarithm is taken in base 2 since the messages will have binary representation and for convention $0 \log 0 \equiv 0$. Further let us give values to that sequence, so suppose that we have four events represented by the sequence $\{x_1, x_2, x_3, x_4\}$ and for each event the respective probability $\{1/3, 1/6, 1/4, 1/4\}$. We wish to send this sequence to another party. One possible scheme could be

$$x_1 \to 00, x_2 \to 10, x_3 \to 01, x_4 \to 11$$

so if we send the following message,

$$x_1 x_2 x_1 x_4 x_3 x_1,$$

we would have to send the string

$$001000110100.$$

But is that the best possible string? The answer is no, we could use the likelihood of appearance of each event to shorten our message in a process that is called data compression. One possible way we could do that is in the following way

$$x_1 \to 0, x_2 \to 111, x_3 \to 10, x_4 \to 01,$$

then our string would be,

$$0111001100,$$

which is in fact smaller than the first one. Calculating the expected length of both strings we see that the expected length of the second string is 1.8 bits as opposed to the first string that was of 2 bits on average. Here we must notice that although this string is smaller than the first calculating the Shannon entropy for it gives us a value of ≈ 1.95 which reflects the fact that this string is not uniquely determined by the encoding that was done turning it not secure. We should also note that $H(X) \geq 0$ and that $H(X)$ is a concave function.

There is a generalization of the Shannon entropy for quantum states and it is called von Neumann entropy. For a density matrix ρ that lives in a Hilbert space H we have

$$S(\rho) \equiv -\mathrm{Tr}\rho \log \rho, \tag{2.1.2}$$

where now the density operator ρ takes the place of the probability distribution p. It is easy to see the relation between the Shannon entropy and the von Neumann entropy, one just need to choose a base for the density matrix in which the density matrix is diagonal. In this base it can be written in the form $\rho = \sum_i p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$, then the equation (2.1.2) becomes

$$S(\rho) = -\sum_i p_i \log p_i, \tag{2.1.3}$$

which has the same form of the Shannon entropy.

The interpretation of the von Neumann entropy is very close to that that was given for the

Shannon entropy. So let us consider two parties, Alice and Bob, each one being in different laboratories. One of the parties, let us say Alice, can then prepare a state that we are going to define ρ_i^B according to some probability distribution p_i. Before Bob receives the state his expected density matrix is $\rho^B = \sum_i p_i \rho_i^B$, so we see that the uncertainty of Bob is quantified by the von Neumann entropy $S(\rho^B)$. Some interesting properties [15] of the von Neumann entropy are:

- $S(\rho) \geq 0$ for any density matrix;
- $S(\rho) = 0$ only when ρ is pure;
- $S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$, the von Neumann entropy is additive;
- $S(\rho)$ is concave, i.e $S(\sum_i p_i \rho_i^B) \geq \sum_i p_i S(\rho_i^B)$.

As we can have the marginal entropy for one of the systems we also can evaluate the entropy of a joint state for a density matrix ρ_{AB} which lives in a bipartite Hilbert space $H_{AB} = H_A \otimes H_B$. For this situation we have

$$S(\rho_{AB}) \equiv -\mathrm{Tr}\rho_{AB} \log \rho_{AB}. \tag{2.1.4}$$

To get from the the joint entropy of our system to the marginal entropy of a subsystem it is required to take a partial trace over one of the subsystems. The partial trace is going to be denoted by a subscript that represents the space where the trace is acting, i.e, $S(\rho_A) = \mathrm{Tr}_B\{S(\rho_{AB})\}$ and $\rho_A = \mathrm{Tr}_B\{\rho_{AB}\}$. Another characteristic of the von Neumann entropy is that for a joint system described by ρ_{AB} the entropy is subadditive

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B), \tag{2.1.5}$$

where the equality is achieved if and only if $\rho_{AB} = \rho_A \otimes_B$, meaning that our systems are not correlated. A useful and surprising property of the joint entropy is that $S(\rho_{AB})$ can be less than the marginal entropies $S(\rho_A)$ and $S(\rho_B)$. This is surprising since the Shannon entropy (classical entropy) of a joint probability distribution $H(X, Y)$ is always greater or equal to the entropy of its marginals $H(X)$ and $H(Y)$. For the proof we are going to need the conditional Shannon entropy, a measure that is going to be presented in the next section.

Proof. *Knowing that the conditional entropy is non-negative [14]* $H(X|Y) \geq 0$*, we have by the*

definition of the conditional entropy that

$$\begin{aligned} H(X|Y) &= -\sum_{x,y} p(x,y)\log p(x|y) \\ &= -\sum_{x,y} p(x,y)\log \frac{p(x,y)}{p(y)} \\ &= -\sum_{x,y} p(x,y)[\log p(x,y) - \log p(y)] \\ &= -\sum_{x,y} p(x,y)\log p(x,y) + \sum_{y} p(y)\log p(y) \\ &= H(X,Y) - H(Y) \geq 0, \end{aligned} \tag{2.1.6}$$

thus

$$H(X,Y) \geq H(Y). \quad \square \tag{2.1.7}$$

So one would expect that to hold for the quantum case. In fact if the state ρ_{AB} is pure we have that $S(\rho_{AB}) = 0$ and $S(\rho_A) = S(\rho_B)$. This is because of the form of the spectral decomposition that is taken by the marginal states. If $|\rho_{AB}\rangle$ (with $\rho = |\rho\rangle\langle\rho|$) can be written as [15]

$$|\rho_{AB}\rangle = \sum_i \sqrt{c}\, |x_i\rangle_A |y_i\rangle_B , \tag{2.1.8}$$

where the kets $|x_i\rangle_A$ and $|x_i\rangle_B$ are orthonormal sets of vectors on systems A and B respectively, then the reduced density matrices ρ_A and ρ_B are

$$\rho_A = \sum_i c_i |x_i\rangle_A \langle x_i|_A , \tag{2.1.9}$$

$$\rho_B = \sum_i c_i |y_i\rangle_B \langle y_i|_B , \tag{2.1.10}$$

so the spectral decomposition admits the same eigenvalues. This is a general property of the joint entropy being respected not only for bipartite systems. We have that for a quadripartite system where $|\rho\rangle_{ABCD}$ is pure that:

$$S(\rho_A) = S(\rho_{BCD}), \tag{2.1.11}$$

$$S(\rho_{AB}) = S(\rho_{CD}), \tag{2.1.12}$$

and

$$S(\rho_{ABC}) = S(\rho_D). \tag{2.1.13}$$

2.1.1 Conditional Entropy

Usually we can have events that depend on the order in which we acquire the information. For example, if we have a box with a certain number of red and blue balls the probability with which we take each ball changes the probability for the next ball to be taken. We can describe the box with red and blue balls using the random variables X and Y respectively, so that our surprise on discovering the outcome of each measurement - the color of the ball - after each ball that is taken, on average, is given by the classical conditional entropy

$$H(X|Y) = \sum_x p_x H(Y = y), \tag{2.1.14}$$

or expressing it in a more useful form

$$H(X|Y) = H(XY) - H(Y). \tag{2.1.15}$$

In the quantum scenario we can also measure the entropy of knowing the values of one of the subsystems prior to knowing the value of the other part of the system, this measure is called quantum conditional entropy. There are two distinct shapes for the conditional entropy, one that is similar to the classical conditional entropy and other that takes into account the measurements done over the system. Firstly we are going to talk about the second version.

Like we said before the conditional entropy measures the uncertainty that we have about a state, let us say A, after we learned the value of a second state B [1]. There is nothing wrong with this scenario classically, but when we are dealing with quantum mechanics this statement is unclear [16] because we first need to establish the set of states B that are going to be measured. So if we perform a measurement on the subsystem B that can be described by a complete von Neumann measurement, $\{\Pi_j^B\}$ [2] we will have as the result the state

$$\rho_{A|\Pi_j^B} = \frac{\Pi_j^B \rho_{AB} \Pi_j^B}{\mathrm{Tr}[\Pi_j^B \rho_{AB} \Pi_j^B]}, \tag{2.1.16}$$

with the probability being $p_j = \mathrm{Tr}[\Pi_j^B \rho_{AB} \Pi_j^B]$. And the states $\rho_{A|\Pi_j^B}$ are then conditioned to the result of the measurement done. Then we could define the conditional entropy as

$$S(\rho_A|\{\Pi_j^B\}) = \sum_j p_j S(\rho_A^j), \tag{2.1.17}$$

where the $S(\rho_A^j)$ is the information of the system A that we do not possess and the probability gives the weight of each measurement. The problem with this definition is that there are infinite

[1] There is a discussion where it is made a connection to the classical conditional entropy and the uncertainty of the measures and its link with classical discord in [32].

[2] This way of seeing things is part of a more general view of quantum operations, that is going to be examined more carefully in Chapter 3.

ways that we could define the measurement. One solution is to find the best possible set of operators or, in other words, performing a minimization over all possible measurements, and in doing so, removing the base dependence.

As said before, the other form is a generalization of the classical conditional entropy for two random variables X and Y but for the density operators of our system

$$S(A|B) = S(\rho_{AB}) - S(\rho_B), \tag{2.1.18}$$

and it is very useful because a lot of properties of the classical conditional entropy also hold for that form of the quantum version, such as chaining rules, and the fact that conditioning does not increase entropy [14]. The first departure of the classical theory also arises with the quantum conditional entropy, the difference being that the quantum conditional entropy admits negative values [13]. This is a divergence from the classical Shannon theory because classically for two random variables X and Y the following inequality is true $H(XY) \geq H(X)$ and we can't get $H(X)$ or $H(Y)$ greater than the joint Shannon entropy. But this is not true for the quantum realm; we can have more knowledge about the whole than we could have for the parts and that is what happens for pure entangled states. In this situation the quantum conditional entropy will be negative and the fact that is negative is also a sufficient criteria for non-separability of a state. This fact is so important that the negative form of the quantum conditional entropy received its own name, the coherent information:

$$I_c(A\rangle B) = S(B) - S(AB) = -S(A|B),\ if\ S(A|B) < 0. \tag{2.1.19}$$

This measure first appeared in [12] as a measure of quantum correlations of a state in various stages of a process, having a similar meaning to the classical mutual information. In specific the type of quantum correlations that was addressed was the entanglement. Because of the nature of the coherent information, since it is the negative of the conditional entropy when the coherent information is positive is signal that the state is entangled, as it was said before. A more complete explanation of the coherent information will be given in Chapter 3 after introducing quantum channels.

2.1.2 Mutual Information

The quantum mutual information is the standard measure of correlation, this implies both classical and quantum correlation that the subsystems share. The form used here will be the one that is analogous to the classical form of the mutual information given by

$$I(X;Y) = H(X) + H(Y) - H(XY). \tag{2.1.20}$$

It is immediately seen that this quantity is symmetric on the exchange between X and Y, after all, we will learn as much about X measuring Y as we would going to discover about Y measuring X. Replacing each Shannon entropy by the von Neumann entropy we have

$$I(A;B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}). \tag{2.1.21}$$

It is also relevant to say that the quantum mutual information can be conditioned in obtaining knowledge of a third system C. So for a tripartite state ρ_{ABC} the information gained about ρ_{AB} in knowing ρ_C is represented by the quantum conditional mutual information

$$I(A;C|B) = S(\rho_A|\rho_B) + S(\rho_C|\rho_B) - S(\rho_{AC}|\rho_B), \tag{2.1.22}$$

or expanding the conditional entropies

$$I(A;C|B) = S(\rho_{AB}) + S(\rho_{BC}) - S(\rho_{ABC}) - S(\rho_B). \tag{2.1.23}$$

We can note that the last two parts of the mutual information (2.1.21) are in fact the quantum conditional entropy, replacing it we get

$$I(A;B) = S(\rho_A) - S(A|B). \tag{2.1.24}$$

In the previous section we saw that there are a couple of different ways to represent the conditional entropy due to the strange character of quantum mechanics, that means that we could write the conditional entropy seen in the mutual information to be measurement dependent. So from the equation (2.1.17) we have

$$I = J(\rho_{AB}) = S(\rho_A) - \sum_j p_j S(\rho_A^j). \tag{2.1.25}$$

This new quantity is called classical correlation (CC) J and it was first presented by [11] as a good measure for classical correlations because it respects certain expected properties for its purposes. $J = 0$ for separable states, as separable states take the form of a product state $\rho = \rho_A \otimes \rho_B$ they do not carry correlations[3]. The CC is non-increasing under local operations, after all local transformations should not increase classical correlations and change in basis won't affect J. One example is for the state

$$\rho_{AB} = \sum_x p_x \left|x_A\right\rangle \left\langle x_A\right| \otimes \rho_B^x, \tag{2.1.26}$$

as it is a separable state there is zero entanglement and the mutual information for this par-

[3]We are going to see further on that in fact there are separable states that exhibit quantum correlations, but for completeness the argument will be sustained in this section.

ticular state is given by

$$I(A;B) = S(\rho_B) - \sum_x p_x S(\rho_B^x). \tag{2.1.27}$$

So as we know it the quantum mutual information measures the total correlations in a state, for a state that do not have quantum correlations, the only thing that it shows is the classical part of the correlations and it takes the same form of the CC that it was presented.

2.1.3 Relative Entropy

The quantum mutual information presented in the previous section is nothing but a particular case of a more general measure, the quantum relative entropy. Being ρ and σ two density matrices we have that the quantum relative entropy is

$$S(\rho||\sigma) = \mathrm{Tr}\{\rho \log \rho - \rho \log \sigma\}. \tag{2.1.28}$$

The relative entropy can be seen as a measure of the distance or the distinguishability between two states even though it is not a real measure of distance since it does not respect the triangle inequality and $S(\rho||\sigma) \neq S(\sigma||\rho)$, in other words, it is not a symmetric measure. Also the quantum relative entropy is only well defined if the support[4] of ρ is contained in the support of σ, supp $\rho \subseteq$ kernel σ, otherwise $S(\rho||\sigma) = +\infty$. This could be understood as follows, think about a case where we have two states that are almost orthogonal to each other i.e $\langle\phi|\,\eta\,|\phi\rangle = \alpha$ where α is really small and the quantum states are $|\phi\rangle$ and η. As the relative entropy is a sort of distance between states this means that those semi-orthogonal states are as far apart as they could be without being completely different, this indicates that the relative entropy will be fairly big and as the difference grows smaller the entropy tends to ∞. Ensuring that the support of ρ will be a subset of the support of σ takes care of that problem.

We can see that for the special case where $\rho = \rho_{AB}$ and $\sigma = \rho_A \otimes \rho_B$, where $\rho_A$and ρ_B are reduced density matrices from $\rho_{AB}$the quantum relative entropy is

$$\begin{aligned} S(\rho_{AB}||\rho_A \otimes \rho_B) &= \mathrm{Tr}\{\rho_{AB}\log\rho_{AB} - \rho_{AB}\log\rho_A\otimes\rho_B\} \\ &= -\mathrm{Tr}\rho_{AB}\log\rho_A - \mathrm{Tr}\rho_{AB}\log\rho_B + \mathrm{Tr}\rho_{AB}\log\rho_{AB} \\ &= S(\rho_A) + S(\rho_B) - S(\rho_{AB}). \end{aligned} \tag{2.1.29}$$

The last line is exactly one of the definitions for the quantum mutual information (2.1.21). Viewing like this the mutual information would be the difference between a certain bipartite state ρ_{AB} and a separable state $\rho_A \otimes \rho_B$. But perhaps one of the most important properties

[4]The support of a function is the vector space spanned by all non-zero values of that function.

of the quantum relative entropy is that it is always positive, this is expressed in the theorem below usually known as Klein's inequality [10].

Theorem 1 (Klein's inequality)**.** *The quantum relative entropy $S(\rho||\sigma)$ is positive for any two density operators ρ and σ.*

$$S(\rho||\sigma) \geq 0,$$

with equality if and only if $\rho = \sigma$.

Proof 1. *We start with two decomposed states $\rho = \sum_i p_i |i\rangle \langle i|$ and $\sigma = \sum_j q_j |j\rangle \langle j|$ and using (2.1.28) we have*

$$\begin{aligned}
S(\rho||\sigma) &= Tr\sum_i p_i |i\rangle \langle i| \log(\sum_{i'} p_{i'} |i'\rangle \langle i'|) - Tr\sum_i p_i |i\rangle \langle i| \log(\sum_j q_j |j\rangle \langle j|) \\
&= Tr\sum_i p_i |i\rangle \langle i| (\sum_{i'} \log p_{i'} |i'\rangle \langle i'|) - Tr\sum_i p_i |i\rangle \langle i| (\sum_j \log q_j |j\rangle \langle j|) \\
&= \sum_i p_i \log p_i - \sum_{ij} p_i |\langle i|j\rangle|^2 \log q_j \\
&\geq \sum_i p_i \log p_i - \sum_i p_i \log t_i \\
&= \sum_i p_i \log \frac{p_i}{t_i} \qquad (2.1.30) \\
&= -\sum_i p_i \log \frac{t_i}{p_i} \qquad (2.1.31) \\
&\geq \log \left[\sum_i p_i \frac{t_i}{p_i}\right] = 0, \qquad (2.1.32)
\end{aligned}$$

where $t_i = \sum_j |\langle i|j\rangle|^2 q_j$ and $|\langle i|j\rangle|^2$ is taken as one conditional probability of i conditioned to j and it was used the fact that the logarithmic function is concave $\log(\sum_x p_x q_x) \geq \sum_x p_x \log q_x$. □

Chapter 3

Quantum Operations

3.1 Measurements

In the previous Chapter we used on a few times some notions from measurement theory, without explaining what we really meant. Here we are going to give a brief overview of it, firstly, let us consider the measurement postulate of quantum mechanics [15]:

Definition. *Quantum measurements are described by a set of operators* $\{M_k\}$ *that act on the state space of the system that is going to be measured. Each index* k *refers to the possible outcomes of an experiment, due to the measurement. Then if the state of the quantum system is* $|\psi\rangle$ *before the measurement the probability that* k *is the result is given by*

$$p_k = \langle\psi| M_k^\dagger M_k |\psi\rangle , \tag{3.1.1}$$

the state of the system after the measurement is

$$\frac{M_k |\psi\rangle}{\sqrt{\langle\psi| M_k^\dagger M_k . |\psi\rangle}} \tag{3.1.2}$$

where the measurement operator M_k *form a complete set.*

$$\sum_k M_k^\dagger M_k = \mathbb{1}. \tag{3.1.3}$$

3.1.1 Projective measurements

The measurement postulate of quantum mechanics given in this form is a more general description of measurements than what we need. Those of our interest are two important special cases that are going to be discussed next, the von Neumann or projective measurements and positive operator valued measurement or POVM.

Definition. *A projective measurement is characterized by a Hermitian operator M, that has a spectral decomposition*

$$M = \sum_k kP_k. \tag{3.1.4}$$

The projector P_k acts on the eigenspace of the Hermitian operator M with eigenvalue k. As it is said in the measurement postulate of quantum mechanics, the possible results correspond to the values of k. The probability of getting such an outcome k, given the state of our system $|\psi\rangle$ is

$$p_k = \langle\psi| P_k |\psi\rangle, \tag{3.1.5}$$

and the state of the system after that measurement, with outcome k, is

$$\frac{P_k |\psi\rangle}{\sqrt{\langle\psi| P_k |\psi\rangle}}. \tag{3.1.6}$$

It is a special case of the measurement postulate in the sense that the operators are orthogonal in relation to each other, or in other words, they follow $M_{k'}M_k = \delta_{k',k}M_k$ and as commented are Hermitian. It is useful to write this formalism in terms of density operators, considering unitary evolutions for simplicity and for the state $|\psi\rangle$

$$\rho = \sum_i p_i |\psi\rangle \langle\psi|, \tag{3.1.7}$$

with the evolution represented by U we would have

$$\rho' = U\rho U^\dagger. \tag{3.1.8}$$

If we are going to perform measurements described by the operators P_k, the probability of getting k is

$$\begin{aligned} p_k &= \sum_i p_{k|i} p_i \\ &= \sum_i p_i \langle\psi_i| P_k |\psi_i\rangle \\ &= \sum_i p_i \mathrm{Tr}\{P_k |\psi_i\rangle \langle\psi_i|\} \\ &= \mathrm{Tr}\{P_k \rho\}. \end{aligned} \tag{3.1.9}$$

With this we now can ask about the density matrix of the state after the result k. Even getting the result k, we still have an ensemble of states weighted by the probability $p_{i|k}$ for the indexes i, with this the density matrix is

$$\begin{aligned}
\rho_k &= \sum_i p_{i|k} \left|\psi_i\right\rangle_k \left\langle\psi_i\right| \\
&= \sum_i p_{i|k} \frac{P_k \left|\psi_i\right\rangle \left\langle\psi_i\right| P_k}{\left\langle\psi_i\right| P_k \left|\psi_i\right\rangle} \\
&= \sum_i \frac{p_{k|i} p_i}{p_k} \frac{P_k \left|\psi_i\right\rangle \left\langle\psi_i\right| P_k}{\left\langle\psi_i\right| P_k \left|\psi_i\right\rangle} \\
&= \sum_i \frac{p_{k|i} p_i}{\mathrm{Tr}(P_k \rho)} \frac{P_k \left|\psi_i\right\rangle \left\langle\psi_i\right| P_k}{p_{k|i}} \\
&= \sum_i p_i \frac{P_k \left|\psi_i\right\rangle \left\langle\psi_i\right| P_k}{\mathrm{Tr}(P_k \rho)} \\
&= \frac{P_k \rho P_k}{\mathrm{Tr}\{P_k \rho\}}.
\end{aligned} \tag{3.1.10}$$

In the third line it was used that $p_{i|k} = \frac{p_i p_{k|i}}{p_k}$, on the fourth line the equation (3.1.9) and that $p_{k|i} = \left\langle\psi_i\right| P_k \left|\psi_i\right\rangle$.

3.1.2 POVM

Projective measurements are useful as they give the post-measurement state, but it is not always what we want, need or even can know the post-measurement state. Also the projective measurements can be done innumerous times, and if for the first time the outcome was k, for next it will be k and so on. In quantum information theory there are a lot o processes that do not share this quality as the transmision of classical information through quantum channels [14] and the optimal way to distinguish quantum states [15]. For those and other instances it is used the formalism of POVM, we can define

$$F_k \equiv M_k^\dagger M_k. \tag{3.1.11}$$

This is a complete set of operators $\{F_k\}$

$$\sum_k F_k = \mathbb{1}, \tag{3.1.12}$$

and positive,

$$F_k \geq 0. \tag{3.1.13}$$

Also the probability of a certain outcome is going to be

$$p_k = \mathrm{Tr}\{F_k \rho\}, \tag{3.1.14}$$

where ρ represents some mixed state. But this set is not necessarily orthogonal (i.e. in general $\mathrm{Tr}\{F_k F_{k'}\} \neq 0$) this is the only thing that really differs in terms of the properties between the von Neumann measurements, or the "normal" view of measurements, and the POVM formalism. It is interesting that the POVM formalism is associated to that of quantum operations being in fact a precursor of what is going to be shown next. The part of quantum operations, in general, appears because in nature we rarely will have a system that is isolated from the rest, the environment. Usually some kind of interaction will occur and that interaction is represented by noise. Knowing how to deal with the noise present in operations is essential to achieve reliable quantum processing systems. And for that we need the formalism of quantum operations, or more specifically for our purposes the formalism of quantum channels.

3.2 Classical Case

Before we talk about the quantum representation of certain processes is interesting to introduce the classical part, usually referred as Markov processes.

3.2.1 Markov Processes

Let us start with the definition of a stochastic process:

Definition. *A stochastic process is a family of functions $f(X,t)$ where each function depends on two variables X and t and X is a random variable and $t \in \mathbb{R}$.*
There are two ways of using stochastic processes. Those processes can be viewed as a family of realizations $f(t)$ -where the variable is the time- or a family of random variables $f(X)$ -where each event is a variable- [23]. We also can have two types of stochastic processes

- Purely Random Processes;

in which each value that the function $f(t)$ may assume is independent from the other realizations. That means that if you have a certain probability distribution $p(x_1,..,x_n;t_1,..t_n)$ them

$$p(x_1,..,x_n;t_1,..t_n) = p(x_1,t_1)p(x_2,t_2)...p(x_n,t_n), \tag{3.2.1}$$

or they can be

- Markov Processes;

In that case the probability distribution will be

$$p(x_n,tn|x_1,..,x_{n-1};t_1,..t_{n-1}) = p(x_n,tn|x_{n-1},t_{n-1}), \tag{3.2.2}$$

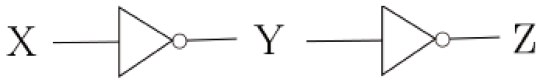


Figure 3.1: A circuit with two NOT-gates and their outputs

thus each event is independent of what happened before with the exception from the event that just preceded it, in other words, the value of the conditional probability in t_n will only depend on the values of x_{n-1} and t_{n-1}. In a certain way it is a memoryless process. In this scenario we have what is called a Markov chain denoted by:

$$X \to Y \to Z$$

being X, Y and Z random variables. They are connected by some stochastic process that lead one to another, a physical example may help with the understanding. From Figure 3.1 suppose we want to send a message to another party but the only way we can do this is with a compromised circuit that will add noise to the system and the input is represented by the random variable X that has to pass by one of the elements of the circuit, a NOT-gate, which cannot work properly. The function of this logically gate is to transform $0 \to 1$ and $1 \to 0$. In passing through that gate it is going to be generated a bit represented by a random variable Y, further this bit will pass through another NOT-gate, that also can or not work properly, generating Z. As each gate is independent from the other this sequence is going to be a Markov chain. In the theory of Markov chains we can describe the output of this random process using a matrix T with the transition probabilities of each event called transition matrix. This would look like

$$\vec{p} = T\vec{q}. \tag{3.2.3}$$

We can see that there is a linear relationship between the output probability $\vec{p}$ and the input probability $\vec{q}$. In general we would expect that if we sum the elements of each row or column the result of the sum must be 1. Of course each of those representations must accompany a change in multiplication of the probability vectors and the matrices, that must be true, for the matrix to represent a valid probability distribution.

3.3 Quantum Case

Noise in quantum system is going to work in a similar way that it does classically, with some operator acting on your initial state ρ and resulting in some output state ρ', resulting in a

equation like (3.2.3)

$$\rho' = \mathcal{E}(\rho). \tag{3.3.1}$$

There are two different views that in essence are equivalent. The first one is a little more intuitive and the other a little more mathematical, but also more general.

3.3.1 Tracing the Environment

Imagine that we have a system represented by a density matrix ρ_A and some kind of interaction occurs between our state and the environment so that we can consider the initial state as a product state $\rho_A \otimes \rho_E$, where ρ_E represents the state of the environment. We can represent the interaction between our state and the environment with an operator U, that belongs to the Hilbert space $H_A \otimes H_E$, that act on the product state. After this we want to know what happened with our state, not what happened with the product state, that means that the environment part is irrelevant to us. Not being of interest we can eliminate the environment. That is done by performing a trace operation on the extraneous part. The product of those manipulations are our final state, Figure 3.2. In mathematical terms this will look like

$$\mathcal{E}(\rho) = \mathrm{Tr}_E \left[U(\rho \otimes \rho_E) U^\dagger \right]. \tag{3.3.2}$$

This describes the dynamics that are occurring on the system, which not necessarily is unitary. It is good to clarify that the state ρ_E, the environment, is composed of the rest of the universe besides our system in a way that together they are a closed system. As it is seeing above we do not really care about the mechanism of the interaction, we only mind about the resulting state and that is enough for this representation. Another remark is that a sufficient condition that the operation (3.3.2) needs to characterize the transformation of the initial state to the output state, is that given that the initial state lives in a Hilbert space with dimension n the environment must live in a Hilbert space with no more than n^2 dimensions [15]. We can see an example [15] of this, let us say that our system is one qubit and the environment is initially $|\phi_E\rangle = |0\rangle$ considering that the operator that acts on the system takes the form of $U = P_0 \otimes \mathbb{1} + P_1 \otimes X$. This form is known also to be the representation of a control not gate (CNOT) which acts on a two qubit system by flipping the second qubit if the first qubit is in the state $|1\rangle$. Them by (3.3.2) we would have

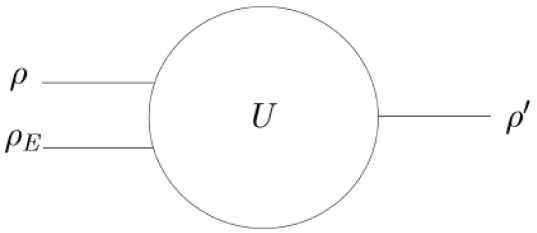


Figure 3.2: Schematic representation of quantum open system

$$\begin{aligned}
\mathcal{E}(\rho) &= \mathrm{Tr}_E\left[U(\rho\otimes\rho_E)U^\dagger\right] \\
&= \mathrm{Tr}_E\left[(P_0\otimes\mathbb{1}+P_1\otimes X)(\rho\otimes|0\rangle\langle 0|)(P_0\otimes\mathbb{1}+P_1\otimes X)\right] \\
&= \mathrm{Tr}_E\left[P_0\rho P_0\otimes|0\rangle\langle 0|+P_0\rho P_1\otimes|0\rangle\langle 0|X+P_1\rho P_0\otimes X|0\rangle\langle 0|+P_1\rho P_1\otimes X|0\rangle\langle 0|X\right] \\
&= \mathrm{Tr}_E\left[P_0\rho P_0\otimes|0\rangle\langle 0|+P_0\rho P_1\otimes|0\rangle\langle 1|+P_1\rho P_0\otimes|1\rangle\langle 0|+P_1\rho P_1\otimes|1\rangle\langle 1|\right] \\
&= P_0\rho P_0+P_1\rho P_1. \qquad (3.3.3)
\end{aligned}$$

We can know show the connection that was mentioned before, between the POVM formalism and that of quantum operations. Since the trace is invariant under cyclic permutations we can move the operator in (3.3.2) and the probability will be

$$P(x)=\mathrm{Tr}_E\left[(\rho\otimes\rho_E)U^\dagger(\mathbb{1}\otimes E_x)U\right]. \qquad (3.3.4)$$

The operator $(\mathbb{1}\otimes E_x)$ describes the measurement that is done on the system. If we say that $|\chi\rangle$ is an orthonormal base for the system, and $|\beta\rangle$ an orthonormal base to the environment. The probability will then be

$$\begin{aligned}
P(x) &= \sum_{\beta\chi}\langle\beta|\langle\chi|\left[(\rho\otimes\rho_E)U^\dagger(\mathbb{1}\otimes E_x)U\right]|\chi\rangle|\beta\rangle \\
&= \sum_{\chi}\rho\left(\sum_{\beta}\langle\beta|\langle\chi|\left[(\mathbb{1}\otimes\rho_E)U^\dagger(\mathbb{1}\otimes E_x)U\right]|\beta\rangle\right)|\chi\rangle \\
&= \sum_{\chi}\langle\chi|\rho F_x|\chi\rangle = \mathrm{Tr}\{\rho F_x\}. \qquad (3.3.5)
\end{aligned}$$

Which is the same of the probability for the POVM presented before.

3.3.2 Kraus Operators

We can show that the relation presented above to deal with noise evolution of quantum systems is equivalent to another relation, called operator sum representation or Kraus representation. Starting from the last relationship

$$\rho' = \mathrm{Tr}_E \left[U(\rho \otimes \rho_E) U^\dagger \right], \tag{3.3.6}$$

and taking the partial trace

$$\begin{aligned} \rho' &= \sum_\epsilon \left[\langle \epsilon | \, U(\rho \otimes \rho_E) U^\dagger \, | \epsilon \rangle \right] \\ &= \sum_\epsilon \left[\langle \epsilon | \, U(\rho \otimes |0\rangle \langle 0|) U^\dagger \, | \epsilon \rangle \right] \\ &= \sum_\epsilon \left[\langle \epsilon | \, U \, |0\rangle \, \rho \, \langle 0| \, U^\dagger \, | \epsilon \rangle \right] \\ &= \sum_\epsilon M_\epsilon \rho M_\epsilon^\dagger. \end{aligned} \tag{3.3.7}$$

Where $M_\epsilon = \langle \epsilon | \, U \, |0\rangle$ are known as Kraus operators. Since the operator U is unitary, $UU^\dagger = \mathbb{1}$, the set of Kraus operators are complete

$$\begin{aligned} \sum_\epsilon M M^\dagger &= \sum_\epsilon \langle \epsilon | \, U \, |0\rangle \, \langle 0| \, U^\dagger \, | \epsilon \rangle \\ &= \langle 0| \, U^\dagger U \, |0\rangle = \mathbb{1}. \end{aligned} \tag{3.3.8}$$

Equation (3.3.7) defines a map, a linear map, that takes density matrices to density matrices. The dynamics presented above are what is called trace preserving because of the property of equation (3.3.8), a broader requirement would be that the set of operators can be smaller than unity

$$\sum_\epsilon M M^\dagger \leq \mathbb{1}, \tag{3.3.9}$$

and we say that those operators are non-trace preserving, that happens in instances that additional knowledge is gained from the measurement apparatus [24]. A usual nomenclature used in quantum information theory to differentiate those two sets are *quantum operations* for those that do not preserve trace and *quantum channels* for those that do preserve the trace. Apart from that both are completely positive. Positivity is a characteristic that every map should have, this guarantees that the output $\mathcal{E}(\rho)$ is going to be a positive operator when its input ρ is also a positive operator. This ensures that the map is always going to take density matrices

to density matrices. Completely positive maps reflect the fact that a map of the form $(\mathbb{1}_i \otimes \mathcal{E})\rho$ for any k that is finite, where $H_A \otimes H_B$ and $\mathbb{1}_i$ lives in H_B and $\mathcal{E}$ lives in H_A is going to be a positive operator if the input ρ is a positive operator. This requirement for a quantum channel to be completely positive comes from the fact that if we have a density matrix on a bipartite system $H_A \otimes H_B$ and for some reason the system H_A evolves while H_B does not, then we expect that the channel take the initial density matrix to a final density matrix.

As our interest lies in quantum channels we are going to delve further on completely positive trace preserving (CPTP) maps.

3.4 Quantum Channels

Quantum channels are used to transmit information among parties, with this information being coded by quantum or classical ways. Also they represent the most general representation of the evolution of a quantum state. The equation presented earlier is an example of a quantum channel

$$\mathcal{E}(\rho) = \mathrm{Tr}_E \left[U(\rho \otimes \rho_E) U^\dagger \right]. \tag{3.4.1}$$

From this equation we can see that a trace preserving quantum operation can always be understood in terms of a unitary evolution where the system interacts with an environment. It is reasonable to ask if something happens with the information that is transmitted through a channel and this will depend on what type of channel is going to be used. More specifically it will depend on what kind of operation that it is going to perform. Two canonical examples are the bit flip and the phase flip channels, the bit flip is represented by the operators, respectively.

$$E_0 = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$E_1 = \sqrt{1-p} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

As a result of those operators the y axis and z axis of the representation of the density operator of our system in a Bloch Sphere are compressed while the x axis is left as it is. The phase flip is represented by

$$E_0 = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$E_1 = \sqrt{1-p} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

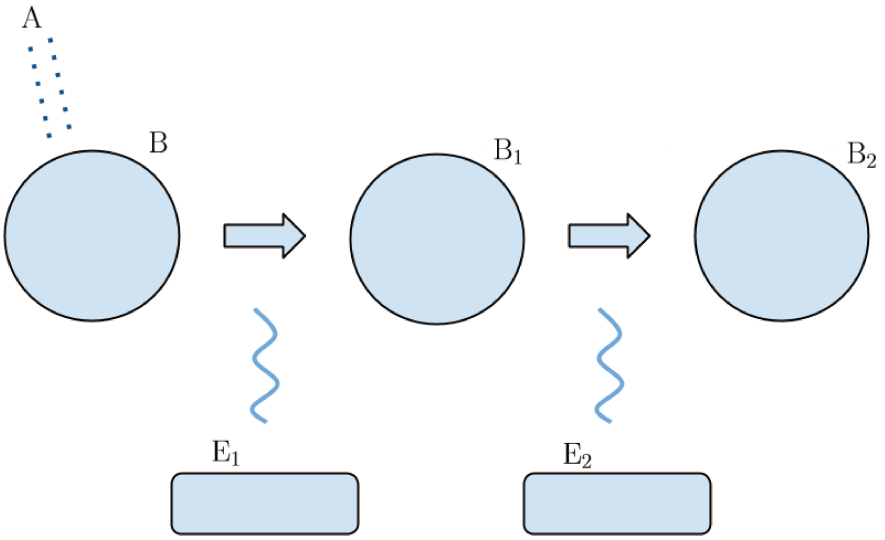


Figure 3.3: Representation of a quantum channel consisted of two stages, where Bob decides to process his part of the system.

It effect is a little different from the bit flip, where it leaves the z axis unchanged, and compress the diagonal elements x and y of the Bloch Sphere. One important characteristic of quantum channels in general is that they obey a quantum data processing inequality.

The quantum data processing inequality was first introduced by Schumacher and Nielsen [12], where they introduce a measure for quantum correlations, the coherent information

$$I_c(A\rangle B) = S(AB) - S(B). \tag{3.4.2}$$

The coherent information is a measure of entanglement since its form is equal to the negative of a quantity known as conditional information. In classical information theory this quantity will always be greater than zero, but in quantum information theory that does not hold, as it was commented in Chapter 2. When the coherent information is positive it is a sign of "quantumness" in the system. In the work of Schumacher and Nielsen it is argued that the coherent information is the quantum analogue of mutual information. One of the main points is that the mutual information obeys a data processing inequality for three random variables that form a Markov chain, and they show that the coherent information also obeys a inequality for a noisy quantum channel

$$I_c(A\rangle B_1) - I_c(A\rangle B_2) \geq 0. \tag{3.4.3}$$

In Figure 3.3 it is shown a two stage process where Alice and Bob share a bipartite quantum system ρ_{AB}. For some reason Bob decides to operate in his part of the system where it interacts with a environment E_1, in what we are going to call first stage of the processing, this could be

represented by a encoding some message in his part of the state. After that the state is sent to the second stage of the processing, where it is going to interact with another environment E_2, this part can be the decoding of the message. In essence the inequality (3.4.3) shows that processing our quantum system will always decrease quantum correlations. It is good to note that the initial state shared between Alice and Bob is pure and in each stage the evolution of the state is unitary, with environments initially in pure states. Thanks to that we can assure that in each stage the state is pure, this fact is important to obtain the quantum data processing inequality as it is going to be important in Chapter 5 where we are going to discuss our results.

Chapter 4

Quantum correlation

4.1 What is entanglement

A pure bipartite state $|\phi_{AB}\rangle$ living in H_{AB} is said to be separable, if it can be written as a product state of pure states $|\phi_A\rangle$ and $|\phi_B\rangle$ living in H_A and H_B respectively

$$|\phi_{AB}\rangle = |\phi_A\rangle \otimes |\phi_B\rangle \,. \tag{4.1.1}$$

Of course this definition can be extended for multipartite mixed states, so in a more general fashion, for a quantum state ρ that lives in $H = \bigotimes_{j=1}^{N} H_j$ and for each H_j is associated a sequence of density operators ρ_j^N for each N and each j and with a sequence of probabilities p_j, we have that

$$\rho = \sum_{i=0}^{k} p_i(\rho_i^1 \otimes \rho_i^2 \otimes .. \otimes \rho_i^{N-1} \otimes \rho_i^N). \tag{4.1.2}$$

Any state that cannot be expressed in the same manner is called *entangled* [18]. Entanglement reflects a purely quantum phenomena, in other words, an entangled state reflects nonclassical correlations that are shared between two systems A and B. Examples of entangled states are the Bell states

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{4.1.3}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{4.1.4}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{4.1.5}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4.1.6}$$

The Bell states form a family of mutually orthogonal states and each one of those are maximally entangled. Maximally entangled means that if those states represent the spin of a particle measuring the spin in any given axis will give a random outcome, meaning that it is equally likely to obtain a component up as it is to obtain the down component. It is readily seen that those states are entangled for our incapability to decompose them in product states. If the have two states represented by

$$\alpha_1 |0\rangle + \alpha_2 |0\rangle \tag{4.1.7}$$

and

$$\beta_1 |1\rangle + \beta_2 |1\rangle , \tag{4.1.8}$$

the tensor product of both is going to depend upon the product of the α and β coefficients

$$\alpha_1\beta_1 |00\rangle + \alpha_1\beta_2 |01\rangle + \alpha_2\beta_1 |10\rangle + \alpha_2\beta_2 |11\rangle , \tag{4.1.9}$$

states like the Bell states would require some of the cross products to be zero while the other not, so we can not guarantee that $|\alpha_1|+|\alpha_2|= 1$ while $|\beta_1|+|\beta_2|= 1$.

With product states we can always make a measurement in a certain fashion that if we are describing a measure by the operator $P_{AB} = P_A \otimes P_B$ the result is that each part of the operator in the product state is only going to act on the state that lives in the respective Hilbert space (i.e if $P|x\rangle = |y\rangle$ then $P_A |x\rangle_A \otimes |x\rangle_B = |y\rangle \otimes |x\rangle_B$). So we can see each state separately of each other. That does not mean that they cannot be correlated with each other, but for entanglement this correlation is different. For entangled states like the Bell states every measure done in one part of the state is going to affect the other part of the state, but this effect on the other part cannot be explained by classical ways. Any kind of correlation that cannot be described by just classical probability theory will then be pertained as quantum correlation. It is not always simple to check if a certain state is or is not separable and for that there exists separability tests such as the *Peres–Horodecki criterion* [19, 20].

It is of interest within quantum information to quantify entanglement and there are many different forms of doing that. Each of them has an operational meaning since entanglement is viewed as a resource to be used in several protocols. For each measure of entanglement it is demanded that they satisfy certain properties, one important property is that entanglement between two systems cannot be increased without quantum interactions. If there are two parties and they are separated physically the entanglement they share cannot increase even if they are allowed to communicate classically (e.g. via telephone), this scenario have a name

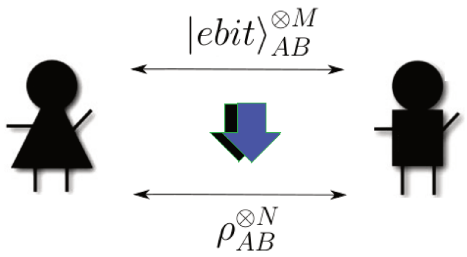


Figure 4.1: Representation of two parties Alice and Bob that want to transform M ebits in N arbitrary mixed states ρ_{AB} by LOCC.

Local Operations and Classical Communication or simply LOCC. Now we are going to present a few measures of entanglement.

4.1.1 Entanglement of Formation

There also exist a difference between measures of entanglement for pure and mixed states, for clarity, let us consider first the pure state case. Let us call again for two parties, Alice and Bob, as is represented in Figure 4.1. In this scheme Alice and Bob share various copies of maximally entangled pure states that we are going to call ebits. The ebits are going to work as the unit for entanglement in the sense that it represents a state with entanglement equal to one, or the state that have one ebit of entanglement, and every other pure state can be related to that state by some fraction of the entanglement contained in the qubit. Sharing those copies Alice and Bob can ask themselves how many copies of the ebits that they share, they need to create n copies of another pure state $|\phi\rangle_{AB}$. The restriction are the ones given by LOCC protocols, only classical communication is allowed between Alice and Bob and they manipulate their part of the states locally. It turns out that the answer is that they are going to need $nS(\phi_A)$ [28], where $S(\phi_A)$ is the von Neumann entropy of one of the reduced density matrices of the state that they want to create.

Now we can see that if $S(\phi_A) = \frac{1}{4}$ then to create 2000 copies of the pure state Alice and Bob are going to need 500 singlets. But if they are trying to create many copies of an arbitrary mixed state ρ_{AB} the von Neumann entropy is not a good measure anymore because even though the entropy of the subsystems are greater than zero the system is not necessarily entangled, leading to the wrong result. What they can do is to write a decomposition of the mixed state ρ_{AB} in terms of pure states

$$\rho_{AB} = \sum_{i}^{N} p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|, \tag{4.1.10}$$

for each index they are going to create n pure states $|\phi_i\rangle$ weighted by the probability of those. By the same reasoning used before they will use $np_iS(\phi_i)$ singlets. In the beginning it was said that the objective was to obtain a final mixed state, so any knowledge about the state must be erased. This is done by "forgetting" the indexes. Then the number of singlets used must take into account that the pure states could have any of the indexes so

$$Number\ of\ Singlets = \sum_i^N np_iS(\phi_i)$$

But as commented in Chapter 2, quantum states can be decomposed in several ways, so the number of singlets could in principle change for each decomposition. This is not a desired characteristic for a measure of entanglement. The solution is to perform a minimization over all pure state ensembles, in this way the entanglement of formation is defined as the conversion rate between the number of singlets used m and the number of singlets obtained n to perform this conversion of quantum states

$$E_f(\rho_{AB}) = \min \sum_i^N p_iS(\phi_i). \tag{4.1.11}$$

4.1.2 Entanglement Cost

The motivation behind the entanglement cost is the same that was presented for the entanglement of formation. We wish to convert m Φ^+ initial states into ρ n mixed final states by applying a certain LOOC operation defined by Λ. For those large numbers m and n the ratio of conversion will be $r = \frac{m}{n}$, so the largest ratio possible will give the entanglement content of the two states. This processing can be done considering perfect transformations that would be represented by r_e this restriction is very demanding, although interesting results can be obtained by studying this case. So it is better to consider non perfect transformation and demand that in the asymptotic limit when $n \to \infty$ they become precise, in such a way that the errors can be neglected. The rate r will be called achievable if for the conversion of those $\rho^{\otimes n}$ initial states, that will reach a final state, the end state is very close to the desired final state for large m. In this case the entanglement cost is

$$E_C(\rho) = \inf \left\{ r : \lim_{n\to\infty} \left(\inf_{\Lambda} \mathrm{Tr}|\rho^{\otimes n} - \Lambda(\Phi^+_{2^{rn}})| \right) = 0 \right\}, \tag{4.1.12}$$

where it is used the trace norm distance as a measure of difference between both states i.e. $D(\alpha, \beta) = \mathrm{Tr}|\alpha - \beta|$. The relation between entanglement of formation and the entanglement cost was established in [21] where it was shown that the entanglement cost is equal to the

regularized version of the entanglement of formation

$$E_C = E_f^{\infty} = \lim_{n\to\infty} \frac{E_f}{n}. \tag{4.1.13}$$

This is connected with the problem of additivity of the entanglement of formation. For a long time it was thought that this measure was additive i.e $E(\sigma^{\otimes n}) = nE(\sigma)$ although a proof was not known, if turned out to be true in general, it would imply that the entanglement of formation is equal to the entanglement cost. But in [22] was proved using a counterexample that in fact this conjecture was not true. The entanglement cost automatically, by being the regularized version of the entanglement of formation, satisfies the additivity criteria. In fact the regularization of various measures is used as an artifact to solve the problems with additivity as with some others "problems".

4.1.3 Distillable Entanglement

It is feasible to ask about the reverse problem considered for the entanglement of formation and the entanglement cost. In other words, given n mixed initial states (the final states from the previous case) is it possible to get m pure maximally entangled states being this conversion rate arbitrarily good in the asymptotic limit? The measure that gives this rate is called distillable entanglement [25]

$$E_D(\rho) = \inf\left\{ r : \lim_{n\to\infty} \left(\inf_{\Lambda} \mathrm{Tr}|\Lambda(\rho^{\otimes n}) - \Phi_{2^{rn}}^{+}| \right) = 0 \right\}. \tag{4.1.14}$$

Again the trace norm distance is used, and it is easy to see the similarity between both definitions. Of course as it is for the entanglement of formation and entanglement cost this measure is equal to the von Neumann entropy for pure states [26]. Also, it is known that the distillable entanglement is going to be less or equal to the entanglement cost $E_C \geq E_D$, revealing some kind of irreversibility in processes that convert ebits to mixed states and mixed states to ebits [27]. The process that can achieve the result of converting mixed states into pure maximally entangled states is called entanglement distillation, entanglement concentration or even entanglement purification protocols [28].

4.1.4 Purification protocol

The first purification protocol was presented in [29] where they propose a protocol that uses the four Bell states (4.1.3) as basis in a LOCC protocol. In this protocol two experimenters Alice and Bob start by converting a bipartite mixed state ρ into a Werner state [30]. Given that a bipartite state with dimensions $d \times d$, a Werner state is a state that is invariant under

unitary operations of the kind $U \otimes U$. The transformation in done applying random bilateral rotations composed by the operators I, B_x, B_y and B_z resulting in

$$W_F = F\left|\psi^-\right\rangle\left\langle\psi^-\right| + \frac{1-F}{3}\left(\left|\psi^+\right\rangle\left\langle\psi^+\right| + \left|\phi^-\right\rangle\left\langle\phi^-\right| + \left|\phi^+\right\rangle\left\langle\phi^+\right|\right). \tag{4.1.15}$$

The effects of the bilateral rotation on each Bell state is represented on Table 4.1. On the above state we have $F = \left\langle\psi^-\right|\rho\left|\psi^-\right\rangle$ as the fidelity of the state in respect to the singlet state. This means that for a fidelity close to one $F \approx 1$ the state in question is going to be very close to the singlet state. This vision of fidelity is general and it is used to see the proximity of different states in comparison with each other. For example if we had $F = \frac{1}{3}$ the state would read

$$W_{\frac{1}{3}} = \frac{1}{3}\left|\psi^-\right\rangle\left\langle\psi^-\right| + \frac{2}{9}\left(\left|\psi^+\right\rangle\left\langle\psi^+\right| + \left|\phi^-\right\rangle\left\langle\phi^-\right| + \left|\phi^+\right\rangle\left\langle\phi^+\right|\right), \tag{4.1.16}$$

meaning that this Werner state can be regarded as a mixture of $\frac{1}{3}$ of a singlet state and $\frac{2}{3}$ of a triplet state, a classical mixture. We could say that the Werner state is different from the initial state used and consequently this process would not be valid. But as the singlet is invariant under bilateral rotations and the Werner state is symmetric the fidelity of both states is the same. Also for two different mixed states if they can be represented by the same density matrix they are also physically identical, since if we measure a mixed state σ in a orthonormal basis $|\chi\rangle$ the outcome will be $|\chi\rangle$ with probability $\langle\chi|\sigma|\chi\rangle$.

Table 4.1: Bilateral rotations

Source		B_x	B_y	B_z
ψ^+	$\rightarrow$	ϕ^+	ϕ^-	ψ^+
ϕ^-	$\rightarrow$	ϕ^-	ψ^+	ϕ^+
ψ^-	$\rightarrow$	ψ^-	ψ^-	ψ^-
ϕ^+	$\rightarrow$	ψ^+	ϕ^+	ϕ^-

Besides the Bilateral Rotation or $\pi/2$ rotations other operation are used on this purification protocol. Unilateral Pauli Rotations or rotation of π radians that are represent by the Pauli matrices (σ_x, σ_y, σ_z) are used too, their action is shown on Table 4.2. And Bilateral XOR operations Table 4.3, this operation is a controlled NOT gate that is applied bilaterally by both parts in the protocol. Using a source state depending on its spin orientation the chosen target state is going to have its spin flipped. And it is bilateral because it is going to operate in two pairs shared between the two members Alice and Bob, where one of the parts (Alice) can act upon spins 1 and 3 and the second part (Bob) on spins 2 and 4. As an example if we have a source state $|\psi^-\rangle$ and the target state $|\phi^+\rangle$ like $|\psi^-\rangle|\phi^+\rangle$, applying the Bilateral XOR (BXOR) operation will proceed:

$$
\begin{aligned}
BXOR[|\psi^-\rangle\,|\phi^+\rangle] &= \frac{1}{2}BXOR(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle)(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) \\
&= \frac{1}{2}BXOR(|0\rangle\,|1\rangle\,|0\rangle\,|0\rangle + |0\rangle\,|1\rangle\,|1\rangle\,|1\rangle - |1\rangle\,|0\rangle\,|0\rangle\,|0\rangle - |1\rangle\,|0\rangle\,|1\rangle\,|1\rangle) \\
&= \frac{1}{2}(|0\rangle\,|1\rangle\,|0\rangle\,|1\rangle + |0\rangle\,|1\rangle\,|1\rangle\,|0\rangle - |1\rangle\,|0\rangle\,|1\rangle\,|0\rangle - |1\rangle\,|0\rangle\,|0\rangle\,|1\rangle) \\
&= \frac{1}{2}(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle)(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle) \\
&= |\psi^-\rangle\,|\psi^+\rangle\,. \qquad (4.1.17)
\end{aligned}
$$

Recalling that the spin 1 will only act on spin 3 and spin 2 only on spin 4. Our two experimenters Alice and Bob will also measure their system along the z axis. The utility of performing this measurement on this axis is because it allows Alice and Bob to differentiate between the states ψ and ϕ. So it follows that they first perform a unilateral rotation along the y axis on two pairs in accord with the Table 4.2. This will convert any ψ^- states into ϕ^+, after that a BXOR will be performed on the ϕ^+ states followed by local measurements on the z axis of the target pair. If this results in parallel spin

Table 4.2: Unilateral Pauli rotations

Source		σ_x	σ_y	σ_z
ψ^+	$\rightarrow$	ϕ^+	ϕ^-	ψ^-
ϕ^-	$\rightarrow$	ψ^-	ψ^+	ϕ^+
ψ^-	$\rightarrow$	ϕ^-	ϕ^+	ψ^+
ϕ^+	$\rightarrow$	ψ^+	ψ^-	ϕ^-

Table 4.3: Action of the bilateral XOR rotations according to the source and target states

Source	Target		Source after	Target after
ψ^+_-	ψ^+	$\rightarrow$	ψ^+_-	ψ^+
ϕ^+_-	ψ^+	$\rightarrow$	ϕ^+_-	ϕ^+
ϕ^+_-	ψ^-	$\rightarrow$	ϕ^-_+	ϕ^-
ψ^+_-	ψ^-	$\rightarrow$	ψ^-_+	ψ^-
ψ^+_-	ϕ^+	$\rightarrow$	ψ^+_-	ϕ^+
ϕ^+_-	ϕ^+	$\rightarrow$	ϕ^+_-	ψ^+
ϕ^+_-	ϕ^-	$\rightarrow$	ϕ^-_+	ψ^s
ψ^+_-	ϕ^-	$\rightarrow$	ψ^-_+	ϕ^-

it means that the states are ϕ^+ states. Being that true, Alice or Bob, depending on which hold the source and target pair, can send a message by classical means to the other party informing

the result. If they are ϕ^+ states the source pair is kept if not it is going to be discarded, because it is a ϕ state. Originally this was done because the state ϕ^+ is invariant under BXOR when used as source or target, and being invariant makes the calculations easier. So if the state was kept, another Pauli rotation σ_y would be perform to convert the ϕ^+ to a ψ^-, them this singlet would be made symmetric by bilateral rotations. This process alone guarantees that if $F > \frac{1}{2}$ then $F' > F$ and the fidelity of the final state equal to

$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}. \tag{4.1.18}$$

At that point this initial procedure does not give a significant yield in the asymptotic limit, but if after getting those prepurified states ϕ^+ and start a BXOR test the yield can be assured. This test works like a parity test to distinguish the states and find the ψ states. So the protocol consists of applying the BXOR operation on part of the source states that weren't transformed by the previous steps to find every ψ states, them by them performing unilateral rotations σ_y Alice and Bob transform all ψ to ϕ states. Notice that they do not know if the states are $\overset{+}{-}$ but as the former states are all related to the later states by those rotations we can guarantee to have only $\overset{+}{\phi^-}$ after that. But it is desired to obtain only ϕ^+ so the next step is to find those states among the $\overset{+}{\phi^-}$, applying Bilateral rotations B_y on this set will change every ϕ^- to ψ^+ but won't change the ϕ^+ states. Finally the ψ^+ are found by doing a BXOR test and transformed into ϕ^+ by σ_x rotations. The yield obviously is given by the ratio of initial and final states $r = \frac{m}{n}$. Since them a lot of other purification protocols have been made like the *One way hashing protocol* or more general protocols [31].

4.2 Quantum Discord

In Chapter 2 we discussed about two measures of correlations. The quantum mutual information would represent the total correlations of a certain bipartite system and the classical correlations, like the name suggest, would be the classical correlations of a certain system when you extract the information due to measurements on part of the system. As it was mentioned those two measures are different in general and the difference between those two ways of writing the mutual information is a measure known as Quantum Discord (QD) [34]. For a bipartite quantum system H_{AB}

$$\delta(\rho^{\leftarrow}_{AB}) = I(\rho_{AB}) - J(\rho^{\leftarrow}_{AB}). \tag{4.2.1}$$

The quantum discord is considered a pure quantum mechanical quantity and defines the quantumness present on a system, or the total quantum correlations that exist on that system, the $\leftarrow$ indicates the direction of the operation so that in the equation above B is performing the

measurements. The later definition of discord is straightforward since the quantum mutual information quantifies the total correlations on a bipartite system and the classical correlation the total classical correlations on the same system. Taking the difference must result on the quantum correlations that are present. As the shape of the state depends on the base that we choose to take the measurement that quantity can give different values for different decompositions, so we are always concerned with the set of operators $\{\Pi_i^B\}$ that are going to minimize the discord

$$\delta(\rho_{AB}^{\leftarrow}) = \min_{\Pi_i^B}[I(\rho_{AB}) - J(\rho_{AB}^{\leftarrow})]. \tag{4.2.2}$$

This concern open up the second interpretation for discord, that discord represents how affected by measurements one state is, so doing the minimization guarantees to find the measurement that is going to disturb the least the chosen state but at the same time is capable of extracting information from it.

We can remember that entanglement is also a measure of the quantum type present on nonseparable states. Quantum Discord on the other hand differs from entanglement on that aspect because even separable states can manifest discord. An example is given on the original paper from Harold Ollivier and Wojciech H. Zurek [34], for the Werner state

$$\rho = z\left|\psi^-\right\rangle\left\langle\psi^-\right| + \frac{1-z}{4}\mathbb{1}, \tag{4.2.3}$$

with $0 \leq z \leq 1$. In Figure 4.2 is shown a reproduction of the behavior of the quantum discord for the Werner state above varying the parameter z. It is know that for that specific Werner state its separability depends on the value of the parameter z. We can see that for values smaller than $z = \frac{1}{3}$ the state is separable and for values greater than $z = \frac{1}{3}$ the state is not separable, or in other words, entangled. It is clearly shown that, even thought being smaller in the region corresponding to the separable Werner state than it is for nonseparable part, the state still exhibit discord for both regimes of the Werner state, that is separated by the vertical dotted line. It is good to notice that for this state discord is not going to depend on the basis of measurement since the Werner state used is invariant under rotations.

We will present a few properties of discord that are worth of mentioning, the first one is that discord is nonnegative

$$\delta(\rho_{AB}^{\leftarrow}) \geq 0. \tag{4.2.4}$$

This follows from the fact that [34]

$$\sum_i p_i S(\rho_B^i) \geq S(\rho_{AB}) - S(\rho_B). \tag{4.2.5}$$

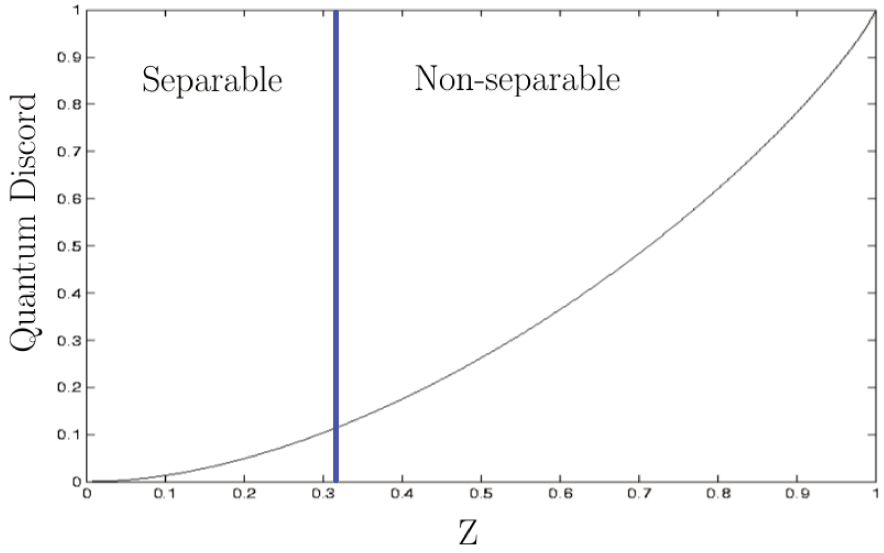


Figure 4.2: The values of quantum discord for the Werner state (4.2.3), varying the parameter z. The blue line marks the value for which the state in question stops being separable. Adapted from [34].

So the nonnegativity follows.

And discord is zero only when there are no quantum correlations on the state. The following proof and theorem are due to [35]

Theorem 2. *$\delta(\rho^{\leftarrow}_{AB}) = 0$ if and only if the state ρ_{AB} is block diagonal in its own eigenbasis, that is*

$$\rho_{AB} = \sum_i P_i \rho_{AB} P_i$$

Proof 2. *We can write a decomposition of the Hilbert space H_B as*

$$\mathbb{1}_B = \sum_\epsilon \Pi_\epsilon = \sum_\epsilon \Pi_{\epsilon L} \otimes \Pi_{\epsilon R}$$

With $\Pi_\epsilon \Pi_\lambda = \delta_{\epsilon\lambda}\Pi_\lambda$, so given a ρ_{ABC} that is invariant under the exchange of B and C, we can use Theorem 5 this state is

$$\rho_{ABC} = \sum_\epsilon q_\epsilon \rho_{A|\epsilon} \otimes \rho^\epsilon_{BC}$$

so for projectors

$$\Pi_\epsilon = \sum_i |F_{\epsilon i}\rangle \langle F_{\epsilon i}| \otimes |H_{\epsilon i}\rangle \langle H_{\epsilon i}|$$

we have

$$\rho^{\epsilon}_{BC} = \Pi_{\epsilon}\rho_{BC}\Pi_{\epsilon} = \sum_{i,j} \rho^{\epsilon}_{ij} \left|F_{\epsilon i}\right\rangle \left\langle F_{\epsilon j}\right| \otimes \left|H_{\epsilon i}\right\rangle \left\langle H_{\epsilon j}\right|$$

and

$$\rho_{AB} = \sum_{\epsilon,i} \rho^{\epsilon}_{j} q_{\epsilon} \otimes \left|F_{\epsilon i}\right\rangle \left\langle F_{\epsilon i}\right|$$

By undoing the measurements we get

$$\rho_{AB} = \sum_{\epsilon} q_{\epsilon}\rho_{A|\epsilon} \otimes \rho^{\epsilon}_{B}$$

so we them diagonalize ρ^{ϵ}_{B} *and relabel the indices*

$$\rho_{AB} = \sum_{i} p_i\rho_{A|i} \otimes \left|\lambda_i\right\rangle \left\langle \lambda_i\right| \tag{4.2.6}$$

□

In [37] Vedral et. al. proved that this last relation can be further generalized by showing that the condition (4.2.6) can be expressed as

$$\sum_{n=1}^{L} c_n(\sum_{k} \Pi_k S_n \Pi_k) \otimes F_n = \sum_{n=1}^{L} c_n S_n \otimes F_n, \tag{4.2.7}$$

with $S_n = \sum_{n'} U_{nn'} A_{n'}$ and $F_m = \sum_{m'} W_{mm'} B_{m'}$. So they write the state ρ in a new basis where: it assumes the form $\rho = \sum_{n=1}^{L} c_n S_n \otimes F_n$; U and W are orthogonal square matrices; and $n = 1...d_A^2$ and $m = 1...d_B^2$, being d_A^2 the dimension of U and d_B^2 the dimension of W. With all this the condition (4.2.7) is obtained, and it is equivalent to

$$\sum_{k} \Pi_k S_n \Pi_k = S_n, \;\; n = 1...L. \tag{4.2.8}$$

As the set $\{S_n\}$ have eigenbasis defined by $\{\Pi_k\}$. The condition $\delta(\rho^{\leftarrow}_{AB}) = 0$ happens if and only if

$$[S_n, S_m] = 0, \;\; n, m = 1...L. \tag{4.2.9}$$

The two last things that are good to mention is that quantum discord can be larger, equal or smaller than the entanglement of formation [36]; even though there is no entanglement if there is zero discord.

Usually in the classical case the discord is going to be zero because there is no difference on the conditional information as it is usually written and taken into account in measurements. This means that it is accepted that classical systems are not vastly affected by measurements on one's system. So how Bob would choose to measure his part of a bipartite system shared

with Alice, in principle should not affect greatly the amount of information that Alice could obtain from her part of the system conditioned to Bob's part. But this is not generally true since we cannot say that all possible measurements that Bob can perform are perfect, it is possible to take into account imperfect measurements due to noise, creating a classical discord [32].

4.3 Locally Inaccessible Information

There is yet another way to think about the quantum discord. Depending on the choice of basis that we could choose, the amount of information extracted from a system can vary. Even when the choice of basis is really good it is possible to not being able to access all the information shared between subsystems. The measure used for that is the quantum mutual information. So we see that there are different kinds of information that are locally accessible for each party and locally inaccessible, were both are present on the mutual information. The thing is that the classical correlation for its character is a measure that represents the locally accessible information present in a subsystem. It is straightforward to see that the quantum discord must them be the amount of locally inaccessible information (LII) from the subsystem that is performing the measurement. For

$$\delta(\rho_{AB}^{\leftarrow}) = \min_{\Pi_i^B}[I(\rho_{AB}) - J(\rho_{AB}^{\leftarrow})], \tag{4.3.1}$$

or even rephrasing in terms of the conditional entropies the discord is

$$\delta(\rho_{AB}^{\leftarrow}) = S(\rho_{AB}|\{\Pi_j^B\}) - S(A|B). \tag{4.3.2}$$

It is easy to see the if all information about A is locally accessible through measurements by B the conditional entropies are going to be equal. The less that the system is disturbed by this measurement the smaller the discord is corroborating with the interpretation given before.

The measurements do not need to be done only by one side, this could be done by the opposite side

$$\delta(\rho_{BA}^{\leftarrow}) = \min_{\Pi_i^A}[I(\rho_{BA}) - J(\rho_{BA}^{\leftarrow})] \tag{4.3.3}$$

But the discord is not a symmetric function $\delta(\rho_{AB}^{\leftarrow}) \neq \delta(\rho_{BA}^{\leftarrow})$ and we see that the information that is not accessible through local measurements from A is different from the inaccessible information from B's point of view. Given a tripartite system H_{ABE} it is possible to perform sequential measurements, Figure 4.3, in a closed form i.e. $E \rightarrow B \rightarrow A$ or in the opposite

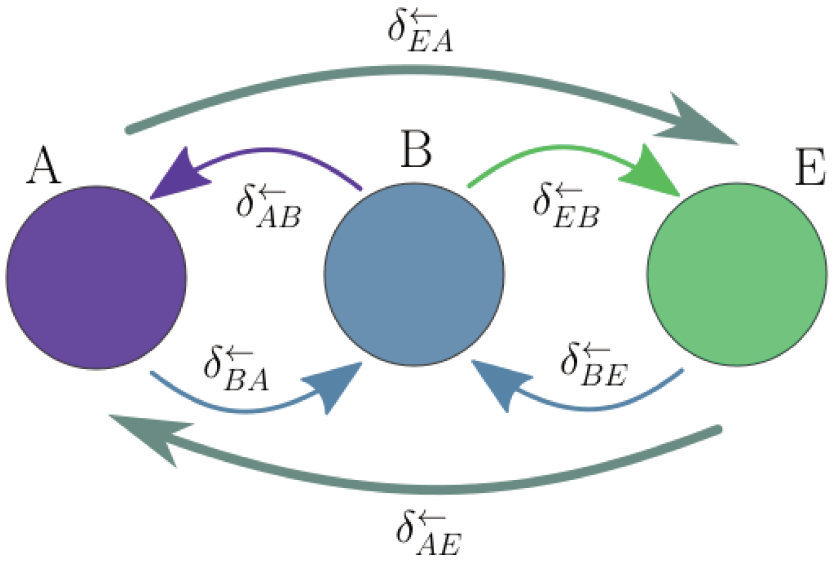


Figure 4.3: Illustration of the flux of locally inaccessible information due to pairwise measurements from and to different systems measured by quantum discord in a tripartite system.

direction i.e. $A \to B \to E$ of the quantum discord for pairwise contributions

$$\mathcal{L}_{E\to B\to A} = \delta^{\leftarrow}_{BE} + \delta^{\leftarrow}_{AB} + \delta^{\leftarrow}_{EA}, \tag{4.3.4}$$

$$\mathcal{L}_{A\to B\to E} = \delta^{\leftarrow}_{BA} + \delta^{\leftarrow}_{EB} + \delta^{\leftarrow}_{AE}. \tag{4.3.5}$$

As the quantum discord reflects the locally accessible information the sequential measurements from one system to other will them represent the flux of locally inaccessible information $\mathcal{L}$ on the tripartite system. These last forms will be relevant for interpretation given in the next chapter.

Chapter 5

Bounded Strong Subadditivity

5.1 From weak monotonicity to b-SSA

Among all those properties of the von Neumann entropy there is one in particular that is very important, it relates subsystem in a tripartite system characterized by the state ρ_{ABC}. The strong subadditive of the von Neumann entropy (SSA):

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC}). \tag{5.1.1}$$

Some further understanding of the meaning of this inequality can come if we rewrite it in terms of the conditional entropies

$$S(A|B) \geq S(A|BC), \tag{5.1.2}$$

we see that the uncertainty about system A is not decreased by knowing the system C if we already had knowledge about the system B [17]. Its importance comes from the fact that we can get all quantum information inequalities from it. So its applications go from the Holevo bound [38] to the quantum data processing inequality, and channel capacities. Until now there is only one inequality not been related to it [9]. The SSA was conjectured first in 1968 in [39] a few years before the appearance of its actual proof by Lieb and Ruskai in 1973 [40] and [41]. The proof relied on a theorem proved by Lieb [42] about the concavity of functions of hermitian matrices. There are various ways of demonstrating the strong subadditivity property of the von Neumann entropy, one of those is by using the fact that the quantum relative entropy is monotone under quantum operations. This is also known as Ulhmann's theorem as follows

Theorem 3. *For any two states ρ_{AB} and σ_{AB} the quantum relative entropy $S(\rho_{AB}||\sigma_{AB})$ can only decrease under the application of a noisy map Γ*

$$S(\rho||\sigma) \geq S(\Gamma\rho||\Gamma\sigma). \tag{5.1.3}$$

But we are not going to take this path for the proof since originally the monotonicity of the quantum relative entropy was proven at a later point than the strong subadditivity, so we are going to preserve the chronological order and give the original proof. Starting with the concavity theorem of Lieb, as it is an important step for the proof of the SSA.

Theorem 4. *For any three R,S,T > 0*

$$Tre^{\log R-\log S+\log T} \leq Tr\int_0^\infty R\frac{1}{S+x\mathbb{1}}T\frac{1}{S+x\mathbb{1}}dx,$$

where it is not necessary that R,S and T commute, for the equality condition to happen.

Proof 3. *We know that for any hermitian matrix K the following function*

$$F(A) = Tre^{K+\log A}, \tag{5.1.4}$$

is concave in A > 0. But if F(A) is concave and homogeneous (i.e. F(xA)=xF(A)) we have that

$$\lim_{x\to 0}\frac{F(A+xB)-F(A)}{x} \geq F(B), \tag{5.1.5}$$

making the substitutions A = S, B=T e K = log R - log S we get

$$Tre^{\log R-\log S+\log T} \leq \lim_{x\to 0}\frac{Tre^{\log R-\log S+\log(S+xT)} - TrR}{x}. \tag{5.1.6}$$

For simplicity let us define

$$Z_1 \equiv \log(S+xT) - log(S) = \int_0^\infty \frac{1}{S+u\mathbb{1}}xT\frac{1}{S+xT+u\mathbb{1}}du. \tag{5.1.7}$$

Then we will end up with

$$Tre^{\log R-\log S+\log T} \leq \lim_{x\to 0}\frac{Tre^{\log R+Z_1} - TrR}{x}. \tag{5.1.8}$$

Separating the exponential and doing a Taylor expansion, we see that

$$Tre^{\log R+Z_1} = TrR + TrR\int_0^\infty \frac{1}{S+u\mathbb{1}}xT\frac{1}{S+u\mathbb{1}}du, \tag{5.1.9}$$

therefore

$$Tre^{logR-logS+logT} \leq Tr\int_0^\infty R\frac{1}{S+u\mathbb{1}}T\frac{1}{S+u\mathbb{1}}du \quad \square \tag{5.1.10}$$

This theorem is the right expansion for a tripartite system of the Golden-Thompson-Symanzik inequality [43–45].

$$\mathrm{Tr}e^{A+B} \leq \mathrm{Tr}e^A e^B, \tag{5.1.11}$$

where A and B are Hermitian matrices and now the equality is only satisfied if A and B commute. Armed with this result we can tackle the strong subadditivity.

Proof 4 (Strong Subadditivity)**.** *The elements of the SSA are*

$$S(\rho_{AB}) + S(\rho_{BC}) - S(\rho_{ABC}) - S(\rho_B). \tag{5.1.12}$$

Rewritting it in terms of their definitions we get

$$Tr_{ABC}\rho_{ABC}[\log \rho_{ABC} + \log \rho_B - \log \rho_{AB} - \log \rho_{BC}]. \tag{5.1.13}$$

The Klein's theorem have as one of its consequences the following inequality

$$Tr\rho(\log \rho - \log \sigma) \geq Tr(\rho - \sigma). \tag{5.1.14}$$

Making $\rho = \rho_{ABC}$ *and* $e^{\log \rho_{AB} - \log \rho_B + \log \rho_{BC}}$ *we get*

$$Tr\rho_{ABC}(\log \rho_{ABC} - \log e^{\log \rho_{AB} - \log \rho_B + \log \rho_{BC}}) \geq Tr(\rho_{ABC} - e^{\log \rho_{AB} - \log \rho_B + \log \rho_{BC}}), \tag{5.1.15}$$

as we seen the elements in (5.1.12) take the form of the quantum conditional mutual information (2.1.23) so we have that

$$I(A;C|B) \geq Tr_{ABC}[\rho_{ABC} - e^{\log \rho_{AB} - \log \rho_B + \log \rho_{BC}}]. \tag{5.1.16}$$

Applying the concavity theorem from Lieb

$$I(A;C|B) \geq Tr_{ABC}\rho_{ABC} - Tr_{ABC} \int_0^\infty \rho_{AB} \frac{1}{\rho_B + x\mathbb{1}} \rho_{BC} \frac{1}{\rho_B + x\mathbb{1}} dx, \tag{5.1.17}$$

and taking the partial trace on systems A and C

$$I(A;C|B) \geq 1 - Tr_2 \int_0^\infty \rho_B \frac{1}{\rho_B + x\mathbb{1}} \rho_B \frac{1}{\rho_B + x\mathbb{1}} dx. \tag{5.1.18}$$

Therefore

$$I(A;C|B) \geq 1 - Tr_B\rho_B = 1 - 1 = 0. \tag{5.1.19}$$

Then is straightforward to see that

$$S(\rho_{AB}) + S(\rho_{BC}) \geq S(\rho_{ABC}) + S(\rho_B). \quad \square \tag{5.1.20}$$

We can see that the fact that the von Neumann entropy is subadditive implies the positivity of the quantum conditional mutual information. This is an important remark and shall be used

again. The last important result was obtained in [8] and it describes the structure of states that saturates the strong subadditivity of the von Neumann entropy.

Theorem 5. *A state ρ_{ABC} on $H_A \otimes H_B \otimes H_C$ satisfies strong subadditivity with equality if and only if there is a decomposition of system B as*

$$H_B = \bigoplus_j H_{b_j^L} \otimes H_{b_j^R},$$

into a direct sum of tensor products, such that

$$\rho_{ABC} = \bigoplus_j q_j \rho_{Ab_j^L} \otimes \rho_{b_j^R C},$$

with states $\rho_{Ab_j^L}$ on $H_A \otimes H_{b_j^L}$ and $\rho_{b_j^R C}$ on $H_{b_j^R} \otimes H_C$, and probability distribution $\{q_j\}$.

The requirement for this structure of states may be a bit elusive for the reader, further information about those requirements can be found in Appendix A. Also for completeness we will give an example for one of the applications for this theorem, that can be found on the original paper [8]. Rephrasing the coherent information in terms of a pure entangled state σ, an operation ϕ that acts on just half of σ and η^σ that is a purification of σ to system A we have

$$I_c(\sigma\rangle\phi(\sigma)) = S(\phi(\sigma)) - S((\mathbb{1}_A \otimes \phi)\eta^\sigma). \tag{5.1.21}$$

If and only $I_c(\sigma\rangle\phi(\sigma)) = S(\sigma)$ it is know to exist a quantum operation $\hat{\phi}$ for which

$$(\mathbb{1}_A \otimes \hat{\phi}\phi)\eta^\sigma = \eta^\sigma. \tag{5.1.22}$$

We can express the coherent information and the von Neumann entropy in a such a way that $I_c(\sigma\rangle\phi(\sigma)) = S(\sigma)$ is going to be satisfied if and only if $I(A;BC) = I(A:B)$. By the theorem above we know that for states of the form

$$\rho = \bigoplus_j q_j \rho_{Ab_j^L} \otimes \rho_{b_j^R C}, \tag{5.1.23}$$

The relation $I(A;BC) = I(A:B)$ will be satisfied and this problem, that is related with quantum error correction and the capability of perfectly reversing a quantum operation, is solved.

As it was stated this is a very important inequality and in [46], two relations that were first brought up by Koashi and Winter [47] were studied further. The first one is an equality relating the entanglement of formation (Eof), the Classical Correlations (CC) and the von Neumann entropy of the commom subsystem, in a tripartite pure state ρ_{ABC}

$$E_{AB} + J^{\leftarrow}_{AC} = S(\rho_A). \tag{5.1.24}$$

It is possible to see that this relation imposes restrictions on the amount of correlation that system A can share in a tripartite system H_{ABC}. If a system can hold up to $S(\rho_A)$ of correlation, the amount of quantum correlations, measured by entanglement with BC, that the system can share with other parts is limited by the classical correlations present on that system. Adding the mutual information of the subsystem H_{AC}, the $I(\rho_{AC})$, on both sides of the equation we get

$$E_{AB} = \delta^{\leftarrow}_{AC} + S(A|C), \tag{5.1.25}$$

which also can be written in terms of others parts of our tripartite pure state ρ_{ABC}. For example, if we write it in terms of system B, substituting the system A, we get $E_{AC} = \delta^{\leftarrow}_{AB} + S(A|B)$. Those relations reveals some connection between the entanglement of formation of a bipartition of any tripartite state and the quantum discord of one of the subsystems, of the same bipartition, in relation to the third part of the global state that was not taken into account for the entanglement of formation. Or in other words, the amount of entanglement in a bipartite state limits the quantum discord that can be shared by those systems with a third. Since the state is pure

$$S(A|C) = S_{AC} - S_C = S_B - S_{AB} = -S(A|B), \tag{5.1.26}$$

where it was used the property of the joint entropy (2.1.11). Adding the expression (5.1.25) taken into consideration the systems A and C and A and B it is obtained

$$E_{AB} + E_{AC} = \delta^{\leftarrow}_{AB} + \delta^{\leftarrow}_{AB}. \tag{5.1.27}$$

This is argued to be a conservation relation for the distribution of the entanglement and the quantum discord in a pure tripartite system. According to the authors [46]: Given an arbitrary tripartite pure system, the sum of all possible bipartite entanglement shared with a particular subsystem, as given by the EOF, can not be increased without increasing, by the same amount, the sum of all QD shared with this same subsystem. A very similar analysis can be done to the same relation (5.1.24), with one differential, the global state now is mixed. When this is the case the Koashi-Winter relation ceases to be an equality, becoming:

$$E_{AB} \leq \delta_{AC} + S(A|C). \tag{5.1.28}$$

Again it is possible to write the relation above switching the state B for the state C. If both inequalities, the one with the entanglement of formation in terms of the state ρ_{AB} and the one with the entanglement of formation in terms of the state ρ_{AC} are summed, we are going to have

$$S_C + S_B + E_{AB} + E_{AC} - \delta_{AC} - \delta_{AB} \leq S_{AC} + S_{AB}, \tag{5.1.29}$$

defining the difference between the Eof and the QD as Δ we get

$$S_C + S_B + \Delta \leq S_{AC} + S_{AB}. \tag{5.1.30}$$

This inequality is the weak monotonicity of the von Neumann entropy [15], besides the Δ which serves as a bound. The weak monotonicity is known to be equivalent to the more interesting inequality the strong subadditivity. If there is an equivalence between those two inequalities there must be a equivalency from the equation (5.1.30) to a bounded strong subadditivity. The next step then is to derive the SSA with the new bound. We start by expanding the tripartite system ρ_{ABC} to a quadripartite pure state ρ_{ABCR} so that for the tripartite part of the state ρ_{ABR} we have

$$S_R + S_B + E_{AB} + E_{AR} - \delta_{AR} - \delta_{AB} \leq S_{AR} + S_{AB}. \tag{5.1.31}$$

With this we can manipulate the entropies of the weak monotonicity changing $S_R = S_{ABC}$ and $S_{AR} = S_{BC}$, resulting in

$$S_{ABC} + S_B + E_{AB} + E_{AR} - \delta_{AR} - \delta_{AB} \leq S_{BC} + S_{AB}. \tag{5.1.32}$$

We can see that the entropies already agree with the form of the SSA, but we still have to deal with the balance of quantum correlations Δ. For this we use the conservation relation (5.1.27) for the pure tripartite state $\rho_{A(BC)R}$ resulting in

$$\begin{aligned} E_{AR} + E_{A(BC)} &= \delta^{\leftarrow}_{AR} + \delta^{\leftarrow}_{A(BC)}, \\ E_{AR} - \delta^{\leftarrow}_{AR} &= \delta^{\leftarrow}_{A(BC)} - E_{A(BC)}. \end{aligned} \tag{5.1.33}$$

Then the equation (5.1.32) turns into

$$S_{ABC} + S_B + E_{AB} + \delta^{\leftarrow}_{A(BC)} - E_{A(BC)} - \delta_{AB} \leq S_{BC} + S_{AB}. \tag{5.1.34}$$

Defining a new delta Δ' for the balance of quantum correlations as

$$\Delta' = E_{AB} + \delta^{\leftarrow}_{A(BC)} - E_{A(BC)} - \delta_{AB}, \tag{5.1.35}$$

we get

$$S_{ABC} + S_B + \Delta' \leq S_{BC} + S_{AB}. \tag{5.1.36}$$

This relation is the strong subadditivity lower bounded by Δ', that translates to a lower bounded

quantum conditional mutual information

$$I(A;C|B) \geq \Delta'. \tag{5.1.37}$$

It is good to point out that in principle Δ can be greater, smaller, or equal to zero. This is due to the fact that for some states the entanglement of formation of a given bipartite state can surpass the quantum discord for the same state, this can depend on the type of the state or the mixing, for example in certain Werner or Quasi-Werner states where the factor F is the mixing. Depending on the distribution of quantum correlations the bound gives different conditions for the equation (5.1.36). In the case that the Eof is equal to QD the bound becomes $\Delta = 0$ and we recover the usual strong subadditivity; if the Eof is greater than QD we have $\Delta > 0$, then we can get a stronger SSA, stronger is considered in the sense that the usual inequality only states that the quantum conditional mutual information must be greater than zero, and a value above that implies on a more restrictive bound, therefore, a stronger bound. Or a weaker SSA, when the Eof smaller than QD and $\Delta < 0$, where weaker means that every value below zero is already considered in the original inequality, then it can render less restrictive bounds. With Δ' we have a similar situation but the balance shifts and the positivity is dependent on the difference between the QD, since the difference in entanglement for this case is going to give a value smaller than zero.

5.2 Structure of States

Given that the result obtained by Hayden et al. [8], about the structure of states that saturates the SSA and the SSA gave rise to a lot of important results it is of interest to see what type of states will saturate the inequality (5.1.36). We start by noticing that the strategy applied by Hayden et al. was based on the quantum relative entropy and the theorem [51, 52] below.

Theorem 6 (Petz's theorem)**.** *Given two density operator ρ and σ,*

$$S(\rho||\sigma) = S(T\rho||T\sigma),$$

if and only if, there exists a quantum operation $\hat{T}$, such that

$$\hat{T}T\rho = \rho,$$

and

$$\hat{T}T\sigma = \sigma.$$

The quantum operation $\hat{T}$ for the density operators ρ and σ, explicitly, is

$$\hat{T}\rho = \sigma^{\frac{1}{2}} T^{\dagger}((T\sigma)^{\frac{1}{2}}\rho(T\sigma)^{\frac{1}{2}})\sigma^{\frac{1}{2}}. \tag{5.2.1}$$

We will explore a little further this theorem up ahead.

With this approach in mind we shall find representations for the quantities of equation (5.1.36) in terms of relative entropies. Then the above mentioned theorem will be useful to determine the states that will saturate the b-SSA by applying the right quantum operation $\hat{T}$. There are three elements that need to be investigated for this, the quantum conditional mutual information, the entanglement of formation and the quantum discord. The quantum conditional mutual information follows trivially since

$$I(A;C|B) = S(\rho_{ABC}||\rho_A \otimes \rho_{BC}) - S(\rho_{AB}||\rho_A \otimes \rho_B). \tag{5.2.2}$$

So let us first turn our attention to the quantum discord, remembering that the quantum discord for a bipartite system is

$$\delta(\rho_{AB}^{\leftarrow}) = \min_{\Pi_i^B}[I(\rho_{AB}) - J(\rho_{AB}^{\leftarrow})]. \tag{5.2.3}$$

Again the mutual information comes easy as it is a special case for the relative entropy, $I(\rho_{AB}) = S(\rho_{AB}||\rho_A \otimes \rho_B)$. For the classical correlation

$$J(\rho_{AB}^{\leftarrow}) = \max_{\{\Pi_B^i\}}[S_A - \sum_i p_i S(\rho_A^i|\Pi_B^i)], \tag{5.2.4}$$

it is possible to use the states $\Phi_B(\rho_B) = \sum_i p_i \left|\psi\right\rangle_B \left\langle\psi\right|$ and $\Phi_B(\rho_{AB}) = \sum_i p_i \rho_A^i \otimes \left|\psi\right\rangle_B \left\langle\psi\right|$

$$\begin{aligned} J(\rho_{AB}^{\leftarrow}) &= S(\rho_A) - \sum_i p_i S(\rho_A^i|\Pi_B^i) \\ &= S(\rho_A) - \sum_i p_i S(\rho_A^i|\Pi_B^i) + H(X) - H(X) \\ &= S_A + S(\phi_B(\rho_B)) - S(\phi_B(\rho_{AB})) \\ &= S(\phi_B(\rho_{AB})||\rho_A \otimes \phi_B(\rho_B)), \end{aligned} \tag{5.2.5}$$

where $H(X)$ is the Shannon entropy written in terms of the probability distributions p_i. Then the QD is going to be

$$\delta(\rho_{AB}^{\leftarrow}) = \min_{\Pi_i^B}[S(\rho_{AB}||\rho_A \otimes \rho_B) - S(\phi_B(\rho_{AB})||\rho_A \otimes \phi_B(\rho_B))], \tag{5.2.6}$$

and with a very similar analysis we can get the QD to the extended system

$$\delta(\rho^{\leftarrow}_{A(BC)}) = \min_{\Pi_i^{BC}}[S(\rho_{ABC}||\rho_A \otimes \rho_{BC}) - S(\phi_{BC}(\rho_{ABC})||\rho_A \otimes \phi_B(\rho_{BC}))]. \tag{5.2.7}$$

Now we turn our eyes to the entanglement of formation

$$E_f(\rho_{AB}) = \min_{\{p_i,|\psi_i\rangle\}} \sum_i p_i S(\rho_A^i). \tag{5.2.8}$$

From the previously development we already know that the RHS of equation (5.2.8) is

$$\begin{aligned}\sum_i p_i S(\rho_A^i) &= S(\phi_B(\rho_B)) - S(\phi_B(\rho_{AB})) \\ &= -[S(\phi_B(\rho_{AB})) - S(\phi_B(\rho_B))] \\ &= -S(\phi_B(\rho_A)|\phi_B(\rho_B)).\end{aligned} \tag{5.2.9}$$

This is not exactly the form that we want, it is necessary to connect the conditional entropy and the relative entropy. We are going to use the next relation for that purpose

$$S(\phi_B(\rho_A)|\phi_B(\rho_B)) = -S(\phi_B(\rho_{AB})|\mathbb{1}_A \otimes \phi_B(\rho_B)), \tag{5.2.10}$$

Proof. *We start expanding the conditional entropy (5.2.9)*

$$\begin{aligned}S(\phi_B(\rho_A)|\phi_B(\rho_B)) &= S(\phi_B(\rho_{AB})) - S(\phi_B(\rho_B)) \\ &= -Tr[\phi_B(\rho_{AB}) \log \phi_B(\rho_{AB})] + Tr[\phi_B(\rho_B) \log \phi_B(\rho_B)],\end{aligned} \tag{5.2.11}$$

adding and subtracting $Tr[\phi_B(\rho_B) \log \mathbb{1}_A \otimes \phi_B(\rho_B)]$*:*

$$\begin{aligned}S(\phi_B(\rho_A)|\phi_B(\rho_B)) = &-Tr[\phi_B(\rho_{AB}) \log \phi_B(\rho_{AB})] + Tr[\phi_B(\rho_B) \log \phi_B(\rho_B)] \\ &+ Tr[\phi_B(\rho_B) \log \mathbb{1}_A \otimes \phi_B(\rho_B)] - Tr[\phi_B(\rho_B) \log \mathbb{1}_A \otimes \phi_B(\rho_B)],\end{aligned} \tag{5.2.12}$$

and using that $\log \mathbb{1}_A \otimes \phi_B(\rho_B) = \log(\mathbb{1}_A) \otimes \mathbb{1}_B + \mathbb{1}_A \otimes \log(\rho_B)$ *we get*

$$\begin{aligned}S(\phi_B(\rho_A)|\phi_B(\rho_B)) &= -Tr[\phi_B(\rho_{AB}) \log \phi_B(\rho_{AB})] + Tr[\phi_B(\rho_B) \log \phi_B(\rho_B)] \\ &+ Tr[\phi_B(\rho_B) \log \mathbb{1}_A \otimes \phi_B(\rho_B)] - Tr_B[\log \phi_B(\rho_B) Tr_A[\phi_B(\rho_{AB})]] \\ &= -Tr[\phi_B(\rho_{AB}) \log \phi_B(\rho_{AB})] + Tr[\phi_B(\rho_{AB}) \log \mathbb{1}_A \otimes \phi_B(\rho_B)] \\ &= -\{Tr\phi_B(\rho_{AB})[\log(\rho_{AB}) + \log \mathbb{1}_A \otimes \phi_B(\rho_B)]\} \\ &= -S(\phi_B(\rho_{AB})|\mathbb{1}_A \otimes \phi_B(\rho_B)).\end{aligned} \tag{5.2.13}$$

With this we have both our relations for the Eof

$$E_f(\rho_{AB}) = S(\phi_B(\rho_{AB})|\mathbb{1}_A \otimes \phi_B(\rho_B)), \tag{5.2.14}$$

and for the extended system

$$E_f(\rho_{A(BC)}) = S(\phi_{BC}(\rho_{ABC})|\mathbb{1}_A \otimes \phi_{BC}(\rho_{BC})). \tag{5.2.15}$$

We are omitting the minimizations of the entanglement of formation and for the quantum discord, because the form obtained for both measures, as the derivation of those forms is independent of the minimizations performed. It is possible to realize the minimizations over the respective operators, but it is not necessary for the continuity of our discussion. Uniting equations (5.2.6), (5.2.7), (5.2.14) and (5.2.15) back into (5.2.9) we get:

$$\begin{aligned} I(A;C|B) \geq & S(\Phi_B(\rho_{AB})||\mathbb{1}_A \otimes \Phi_B(\rho_B)) - S(\Phi_{BC}(\rho_{ABC})||\mathbb{1}_A \otimes \Phi_{BC}(\rho_{BC})) \\ & + [S(\rho_{ABC}||\rho_A \otimes \rho_{BC}) - S(\Phi_{BC}(\rho_{ABC})||\rho_A \otimes \Phi_{BC}(\rho_{BC}))] \\ & - [S(\rho_{AB}||\rho_A \otimes \rho_B) - S(\Phi_B(\rho_{AB})||\rho_A \otimes \Phi_B(\rho_B))]. \end{aligned} \tag{5.2.16}$$

Now we can ask when does that inequality will be saturated. We notice that when the conditions that

$$S(\Phi_B(\rho_{AB})||\rho_A \otimes \Phi_B(\rho_B)) = S(\Phi_{BC}(\rho_{ABC})||\rho_A \otimes \Phi_{BC}(\rho_{BC})), \tag{5.2.17}$$

and

$$S(\Phi_B(\rho_{AB})||\mathbb{1}_A \otimes \Phi_B(\rho_B)) = S(\Phi_{BC}(\rho_{ABC})||\mathbb{1}_A \otimes \Phi_{BC}(\rho_{BC})), \tag{5.2.18}$$

are satisfied for the bounded relation, it will render saturation. Now we are in position to apply Petz's theorem, by finding the quantum operation that will make equations (5.2.17) and (5.2.18) happen. The quantum operation $\hat{T}$ that is considered in Petz's theorem is called a transpose channel or more usually a recovery map [51] $R_{B\to BC}$ that takes the system B to BC, as the notation implies. For the state in question $\phi_B(\rho_{AB})$, that was utilized in the conversion of the measures into relative entropy forms we are going to have

$$\begin{aligned} R_{B\to BC}[\phi_B(\rho_{AB})] &= R_{B\to BC}\left[\sum_i p_i \rho_A^i \otimes |\psi\rangle_B \langle\psi|\right] \\ \Phi_{BC}(\rho_{ABC}) &= \bigoplus_j q_j \sum_i p_{j|i} \rho_A^i \otimes |\tilde{\psi}_j\rangle_{b_i^L} \langle\tilde{\psi}_j| \otimes \omega_{b_i^R C}, \end{aligned} \tag{5.2.19}$$

where $\omega_{b_i^R C} \in H_{b_i^R} \otimes H_C$, $|\tilde{\psi}_j\rangle_{b_i^L} \in H_{b_i^L}$ and $H_B = H_{b_i^L} \otimes H_{b_i^R}$. This is the state which gives

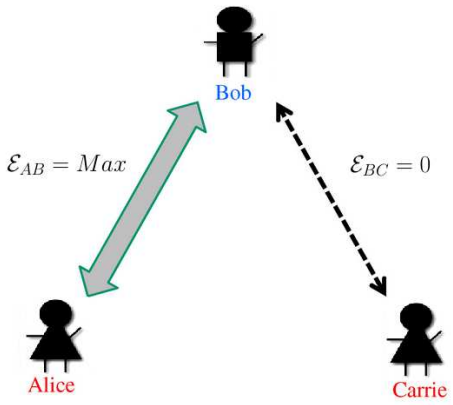


Figure 5.1: Diagram to represent the monogamy of entanglement between Alice and Bob given a third part Carrie. Adapted from [49].

saturation to the bounded SSA. We can see that saying that the state $\phi_{BC}(\rho_{ABC})$ is recoverable from the state $\phi_B(\rho_{AB})$ may be considered a sufficient condition to name states of this kind as short quantum Markov chains, fact shared to the structure of states conceived by Hayden et al. for the unbounded SSA. Reviewing the conditions (5.2.17) and (5.2.18) they are in fact requiring that $E_f(\rho_{A(BC)}) = E_f(\rho_{AB})$ and that $J(\rho^{\leftarrow}_{A(BC)}) = J(\rho^{\leftarrow}_{AB})$. The later relation states that the classical correlation between A and BC remain equal to A and B, which is not unheard of, but the former establishes the same ties to the entanglement of formation of those bipartitions. This implies, especially for cases where this relation is nearly achieved, certain limitations in how the entanglement of A can be shared among the subsystems B and C revealing a monogamous character [48] for the entanglement of formation.

Monogamy of measures that express quantum correlations, is the implication that we cannot share those correlations as we wish between various parties. In a way that if there is some amount o quantum correlations that is divided between two parties the amount that we can share with a third party is limited (this can be seen in Figure 5.1). The picture contains Bob, who shares an entangled state with Alice and there is Carrie who wants to share an entangled state with Bob. If the state that is shared between Alice and Bob is maximally entangled then Bob cannot share his entangled state with Carrie, but if it is not then some amount of entanglement can be shared depending on how much his part is entangled with Alice's part. Of course this property is valid for every part in the scheme above. Monogamy is a useful quality for quantum cryptography, like in quantum key distribution [50], where we want to limit the access of third parties in two way communications. As this state may exhibit monogamy it may be useful in quantum cryptography protocols.

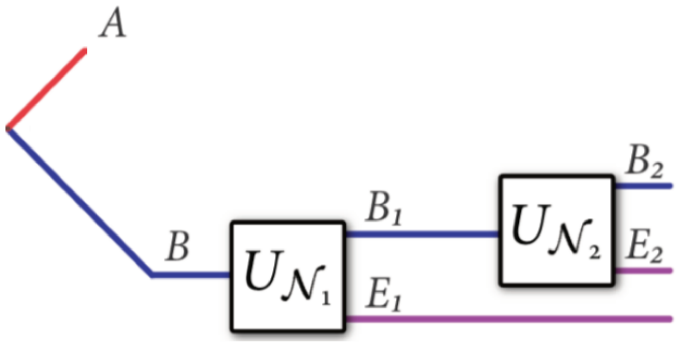


Figure 5.2: Representation o a bipartite state where one of the parts, Bob, decides to operate in his part of system. Adapted from [14]

5.3 Quantum channels with bounds

Now we are going to look to the implication of the bounded strong subadditivity in the quantum data processing inequality. As said before the quantum data processing inequality is

$$I_c(A\rangle B_1) \geq I_c(A\rangle B_2). \tag{5.3.1}$$

This inequality shows that processing a quantum system through a channel will always decrease quantum correlations. And the aim is to determine how the bound on the SSA will affect this inequality. The first step is to deduce the quantum data processing inequality from the strong subadditivity using a suitable notation. For the first stage of the process we will have the global state as AB_1E_1, for the second stage it will be $AB_2E_1E_2$, and the indexes are used to establish which part of the processing is been considered. Then E_1 and E_2 are going to represent the first and second environments respectively, B_i is going to represent Bob's state the operations in the first stage, $i = 1$, and the second stage $i = 1$. As the state from Alice is not been operated on, different pats of the processing are not going to change Alice's state and the indexes will not be used. Defining the state that we are going to take into consideration as the tripartite state $\rho_{AE_1E_2}$, the quantum conditional mutual information is

$$I(A; E_2|E_1) = S_{AE_1} + S_{E_1E_2} - S_{E_1} - S_{AE_1E_2}, \tag{5.3.2}$$

with the same ordering of equation (5.2.9). Since the global state $\rho_{AB_1E_1}$ on the first stage after B processed his part of the system is pure we can write the coherent information between the system A and B as

$$I_c(A\rangle B_1) = S_{B_2} - S_{AB_1} = S_{AE_1} - S_{E_1}, \tag{5.3.3}$$

and the same is valid for the second state of the processing, $\rho_{AB_2E_1E_2}$ is pure, and the coherent

information from system A and B after the second stage will be

$$I_c(A\rangle B_2) = S_{B_2} - S_{AB_1} = S_{AE_1E_2} - S_{E_1E_2}. \tag{5.3.4}$$

Were again the notation used is to clarify when we are talking about the first part of the processing, by using a 1 index, and the second part of the processing where we use a 2 index. Uniting equations (5.3.3) and (5.3.4) it is clear that

$$I_c(A\rangle B_1) - I_c(A\rangle B_2) = I(A; E_2|E_1). \tag{5.3.5}$$

Paying close attention to the parts of the stages that are pure, we can use the conservation relation (5.1.27) leaving the quantum discord and the entanglement of formation in terms of the same systems of the coherent information. Therefore

$$E_{AE_1} - E_{A(E_1E_2)} + \delta^{\leftarrow}_{A(E_1E_2)} - \delta^{\leftarrow}_{AE_1} = E_{AB_2} - E_{AB_1} - \delta^{\leftarrow}_{AB_2} + \delta^{\leftarrow}_{AB_1}. \tag{5.3.6}$$

Substituting the results above in equation (5.2.9) we obtain

$$I_c(A\rangle B_1) - I_c(A\rangle B_2) \geq E_{AB_2} - E_{AB_1} - \delta^{\leftarrow}_{AB_2} + \delta^{\leftarrow}_{AB_1}, \tag{5.3.7}$$

or reordering the terms on the RHS

$$I_c(A\rangle B_1) - I_c(A\rangle B_2) \geq (E_{AB_2} - \delta^{\leftarrow}_{AB_2}) - (E_{AB_1} - \delta^{\leftarrow}_{AB_1}). \tag{5.3.8}$$

The bound on the strong subadditivity will then translate into a lower bound for the quantum data processing inequality, bound that is the difference between the quantum discord and entanglement of formation for the first stage and the difference between those measures in the second stage. As it was said, it is not clear whether or not the difference in parentheses in equation (5.3.8) is positive, zero or negative. If we have a balance of quantum correlations such that the lower bound is greater than zero for the quantum data processing inequality would make a stricter bound than the usual implying that the quantum correlations carried trough different stages would improve along with the processing of quantum data, in other words, it would suggest that the processing of quantum states through channels can be improved. As there is an independent proof for the quantum data processing inequality, perhaps quantum discord has something to contribute on the exchange of correlations during such process, in a way that could compensate for the loss of entanglement and the improvement could be achieved, or this result is simply not physical when the bound resumes to a stricter value than zero. Let us go further on the difference between those two measures. Using yet again the conservation

relation, but for different parts of the global pure state $\rho_{AB(E_1E_2)}$

$$E_{AB_2} + E_{A(E_1E_2)} = \delta^{\leftarrow}_{AB_2} + \delta^{\leftarrow}_{A(E_1E_2)}, \tag{5.3.9}$$

$$E_{B_2A} + E_{B_2(E_1E_2)} = \delta^{\leftarrow}_{B_2A} + \delta^{\leftarrow}_{B_2(E_1E_2)}, \tag{5.3.10}$$

and

$$E_{(E_1E_2)A} + E_{B_2(E_1E_2)} = \delta^{\leftarrow}_{(E_1E_2)A} + \delta^{\leftarrow}_{B_2(E_1E_2)}. \tag{5.3.11}$$

Adding those relations we get

$$\begin{aligned} 2(E_{AB_2} - \delta^{\leftarrow}_{AB_2}) &= \delta^{\leftarrow}_{B_2A} - \delta^{\leftarrow}_{AB_2} + \delta^{\leftarrow}_{A(E_1E_2)} - \delta^{\leftarrow}_{(E_1E_2)A} + \delta^{\leftarrow}_{B_2(E_1E_2)} - \delta^{\leftarrow}_{(E_1E_2)B_2} \\ E_{AB_2} - \delta^{\leftarrow}_{AB_2} &= \frac{1}{2}\left(\mathcal{L}_{(E_1E_2)\to A\to B} - \mathcal{L}_{B\to A\to(E_1E_2)}\right). \end{aligned} \tag{5.3.12}$$

Where it was used the definitions (4.3.4) and (4.3.5). The $\mathcal{L}_{E_1E_2\to A\to B}$ is the flux of locally inaccessible information that is going out the environment after both stages and the $\mathcal{L}_{B\to A\to(E_1E_2)}$ is the flux of locally inaccessible information into the environment. Then the difference between the measures is equal to the difference of the LII, in that way we can define the net flow of locally inaccessible information in the second stage as

$$\mathcal{L}_{R\{E_1E_2\}} \equiv \frac{1}{2}(\mathcal{L}_{E_1E_2\to A\to B} - \mathcal{L}_{B\to A\to E_1E_2}). \tag{5.3.13}$$

Then the relation (5.3.8) can be written as

$$I_c(A\rangle B_1) - I_c(A\rangle B_2) \geq \mathcal{L}_{R\{E_1E_2\}} - \mathcal{L}_{R\{E_1\}}. \tag{5.3.14}$$

Relation (5.3.14) brings some intuition, because it shows that the quantum data processing inequality is lower bounded by the net flux of locally inaccessible information through both stages when measurements are performed in Bob's system. It is expected that the difference in flow of the locally inaccessible information is greater if taken into account both stages of the processing, because through the processing of the state on both stages the information that Bob can extract locally should be less than the information only extractable in the first stage. Of course that it depends on how we choose to measure our states on each step of the processing, or equivalently, how much the state in question is going to be disturbed by those measurements. Being true this tells the bound should be positive and the data processing greater than zero. If the net flux is zero between both stages than the normal bound, zero, is recovered.

Chapter 6

Conclusions

The strong subadditivity is a key inequality in quantum information theory being the link among multiple inequalities and non trivial results inside quantum information and apart, for example, in many-body physics. The investigation of the structure of states that would saturate this inequality was done by Hayden et al. were they find the structure to be of the short quantum Markov chains, this result was far-reaching given the importance of the strong subadditivity itself.

In examining the two Koashi-Winter monogamic relations Fanchini et al. brought to light a conservation relation between the entanglement of formation and the quantum discord in a tripartite pure state that show that for any bipartition of a tripartite pure state the entanglement of formation would decrease or increase by the same amount that the quantum discord of the same bipartition would. Together with that result a different proof for the weak monotonicity of the von Neumann entropy appeared but bringing a possible lower bounds with it. The structure of states that saturated the SSA helped with other results, since the weak monotonicity is a equivalent inequality to the SSA it was asked in this work what is the structure of states that are going to saturate the equivalently bounded SSA.

We first derived a bounded strong subadditivity from that inequality, this bound depended on the balance of quantum correlations that are shared in a system measured by the entanglement of formation and the quantum discord. We saw that if the Eof is equal to the QD the bounded SSA becomes again the SSA, if the Eof is greater than the QD the bounded SSA gets more strict than the usual inequality, and if the Eof is smaller than the QD that bound is weaker. We then investigated the structure of states that render the bounded strong subadditivity of the von Neumann entropy with equality. For this firstly we found a way to express the whole inequality in terms of relative entropies. This included the two measures for quantum correlations: the entanglement of formation and the quantum discord. With that result we used the Petz's theorem to find the condition for equality among the measures, and applying a recovery map we found the states that would saturate the bounded inequality. Those states

like the states that saturates the SSA can be called short quantum Markov chains, in the sense that the tripartite state can be completely recovered by acting on one system of the bipartite state. Also those states require the entanglement of formation to respect monogamic relations. Monogamy of entanglement limits the amount of entanglement that can be distributed among different parties, if maximum entanglement is shared between Alice and Bob further entanglement, from Alice or Bob, cannot be shared with a third party Carrie. This is an important element in a quantum cryptographic scenario, where we want to limit the access of alien parties on two way protocols.

We saw that the bound on the SSA is translated on a bound on the data processing inequality, a lower bound dependent on the difference between the entanglement measured by the entanglement of formation and the quantum discord on the first and second stages of the processing of quantum information. It is not clear whether or not this difference, the lower bound, is going to be positive, negative or zero. For the two latter cases not much is acquired because it is already expected that the data processing inequality is a non-negative inequality, but if the bound is positive that would imply in a processing of quantum information that would strengthen the quantum correlations when passing a state trough a channel. With this quantum correlation being maybe an exchange of entanglement for discord. But since there is a separate proof for the quantum data processing inequality, it is possible that this is not a physical case. We also find that this inequality is connected by a lower bound with the net flow of the locally inaccessible information in and out of the environment that is used in each stage of the process of sending a certain state. This brings an intuition that, depending on the measurements performed in each step it is possible to increase or decrease the lower bound of the inequality.

A few questions arise from the work, like in which protocols the above state can be implemented? Can the lower bounded conditional mutual information be used in some protocol of state redistribution? We also infer that the bound on that strong subadditivity can be connected with the reason behind the monogamy of the squashed entanglement. And why it is so that the bound in the data processing inequality cannot be greater than zero, since there are situations were the quantum discord is greater than the entanglement of formation.

Appendix A

Koashi-Imoto Theorem

In this Appendix our main objective is to give context for the derivation of the Theorem 5, elucidating the form taken by the states, by showing a proof for the Koashi-Imoto theorem [53]. This result is the backbone for the structure of states which was presented, and the proof will follow similarly to the one given in [21], and for all the calculations the Hilbert spaces used will be considered to have finite dimension.

A.1

We start with the definition given in [21] for the result of Koashi-Imoto:

Theorem 7 (Koashi-Imoto)**.** *Associated to the states $\rho_1, ...\rho_k$ there exists a decomposition of H as*

$$H = \bigoplus_j J_j \otimes K_j$$

into a direct sum of tensor products, such that the states ρ_k decompose as

$$\rho_k = \bigoplus_j q_{j|k}\rho_{j|k} \otimes \omega_j,$$

where $\rho_{j|k}$ is a state on J_k, ω_j is a state on K_j and $q_{j|k}$ is a probability distribution. And for every T which leaves the ρ_k invariant, every associated unitary has the form

$$U = \bigoplus_k \mathbb{1}_{J_j} \otimes U_{K_j\mathcal{E}},$$

with unitaries $U_{K_j\mathcal{E}}$ that satisfy

$$\forall j \;\; Tr_{\mathcal{E}}(U_{K_j\mathcal{E}}(\omega_j \otimes \epsilon)U^*_{K_j\mathcal{E}}) = \omega_j.$$

The structure of states saturating the bounded-SSA as the structure of states saturating the regular SSA is based on the condition that we can recover the density matrix in question using a quantum operator G that can be described as part of a set

$$\mathbf{G} = \{G : \forall k \; G\rho_k = \rho_k\}, \tag{A.1.1}$$

of all those operators that leave the states ρ_k invariant. For each G is associated another set $\mathcal{A}_\mathcal{G}$

$$\mathcal{A}_\mathcal{G} = \{X \in \mathcal{B}(H) : F^*(X) = X\}, \tag{A.1.2}$$

formed by all the operators X that are not changed by the action of G^*. The quantum operation G will have a conditional expectation of the form

$$P^* = \lim_{M\to\infty} \frac{1}{M} \sum_{m=1}^{M} (G^*)^m, \tag{A.1.3}$$

in case the set defined by $\mathcal{A}_\mathcal{G}$ is a *-subalgebra of $\mathcal{B}(H)$. It is possible to see that $\mathcal{A}_\mathcal{G}$ is in fact a *-subalgebra, using the Kraus representation. First we notice that $G^*(X) = X$ and $(G^*(X))^* = X^*$, applying the inequality

$$G^*(X^*X) \geq G^*(X^*)G^*(X), \tag{A.1.4}$$

that is a Schwarz type inequality [54] we get that

$$G^*(X^*X) - X^*X \geq 0. \tag{A.1.5}$$

Then utilizing a faithful state, or in other words, a state that has strictly positive eigenvalues that is also invariant, makes $G^*(X^*X) = X^*X$ as well $X^*X = 0$ and the inequality above equal to zero. Which in turn tells that the set $\mathcal{A}_\mathcal{G}$ is a *-subalgebra of $\mathcal{B}_H$.

For Hilbert spaces with finite dimension $\mathcal{A}_\mathcal{G}$ has a representation in form of a direct sum [55], such that, for the decomposition of the Hilbert spaces

$$H_\beta = \bigoplus_j H_{\beta,1} \otimes H_{\beta,2}, \tag{A.1.6}$$

we have

$$A_\beta = \bigoplus_j \mathcal{B}(H_{\beta,1}) \otimes \mathbb{1}_{\beta,2}. \tag{A.1.7}$$

With any CP-map from $\mathcal{B}(H_{\beta,1})$ to A_β having the form

$$P^*(X) = \bigoplus_j \mathrm{Tr}_{\beta,2}(\Pi_j X \Pi_j (\mathbb{1}_{\beta,1} \otimes \omega_j)) \otimes \mathbb{1}_{\beta,2}. \tag{A.1.8}$$

For one given element of $G_0 \in \mathbf{G}$, is possible to associate one element of $\mathcal{A}_0 \in \mathcal{A}_\mathcal{G}$, that is an intersection of every $\mathcal{A}_{G_n}$ and of course a P_0. For this element we have

$$A_0 = \bigoplus_j \mathcal{B}(H_{b_j^L}) \otimes \mathbb{1}_{b_j^R}, \tag{A.1.9}$$

so that for the density matrices ρ_k

$$\rho_k = P_0(\rho_k) = \bigoplus_j \mathrm{Tr}_{b_j^R}(\Pi_j \rho_k \Pi_j) \otimes \omega_j = \bigoplus_j q_j \rho_{j|k} \otimes \omega_j. \quad \square \tag{A.1.10}$$

Bibliography

[1] Claude E. Shannon, Warren Weaver. The Mathematical Theory of Communication. Univ of Illinois Press, 1949.

[2] Shankar R. Principles of Quantum Mechanics (Springer, 2nd edition, 1994).

[3] P. W. Shor, "Additivity of the Classical Capacity of, J. Math. Phys., vol. 43, pp. 4334–4340, 2002.

[4] David Poulin and Matthew B. Hastings, Phys. Rev. Lett. 106, 080403 – Published 24 February 2011

[5] Fernando G.S.L. Brandao, Aram W. Harrow, Jonathan Oppenheim, Sergii Strelchuk, Phys. Rev. Lett. 115, 050501 (2015)

[6] Mary Beth Ruskai J. Math. Phys. 43, 4358 (2002).

[7] Omar Fawzi, Renato Renner. Communications in Mathematical Physics December 2015, Volume 340, Issue 2, pp 575-611.

[8] P. Hayden, R. Jozsa, D. Petz, A. Winter, Commun. Math. Phys. 246, 359 (2004)

[9] Noah Linden, Andreas Winter. Communications in Mathematical Physics October 2005, Volume 259, Issue 1, pp 129-138

[10] O. Klein, "Zur Quantenmechanischen Begründung des zweiten Hauptsatzes der Wärmelehre" Z. Physik 72, 767-775 (1931).

[11] L Henderson and V Vedral 2001 J. Phys. A: Math. Gen. 34 6899

[12] B.W. Schumacher and M.A. Nielsen, Phys. Rev. A54,2629 (1996).

[13] N.J. Cerf and C. Adami "Negative Entropy and Information in Quantum Mechanics" PhysRevLett.79.519/4

[14] M. M. Wilde, Quantum Information Theory (Cambridge University Press, Cambridge, 2013).

[15] Nielsen, M. A., and I. L. Chuang, 2000, Quantum Computation and Quantum Information (Cambridge University Press, Cambridge)

[16] H. Ollivier and W. Zurek, Phys. Rev. Lett., 88, 017901 (2001)

[17] Nielsen, M. A., and Denes Petz "A simple proof of the strong subadditivity inequality" http://arxiv.org/pdf/quant-ph/0408130v3.pdf

[18] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki Rev. Mod. Phys. 81, 865 – Published 17 June 2009.

[19] A. Peres, Phys. Rev. Lett. 77, 1413 (1996).

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

[21] P. Hayden, M. Horodecki, Barbara M. T. J. Phys. A: Math. Gen. 34(35):6891-6898, 2001.

[22] M. B. Hastings, Nature Physics 5, 255 - 257 (2009)

[23] https://www.math.uwaterloo.ca/ mscott/Little_Notes.pdf

[24] Irene Bongioanni, Linda Sansoni, Fabio Sciarrino, Giuseppe Vallone, and Paolo Mataloni Phys. Rev. A 82, 042307 (2010)

[25] Plenio, M. B. Virmani, S. Quant. Inf. Comput. 7, 1–51 (2007).

[26] Horodecki M, Horodecki P and Horodecki R 1998 Acta Phys. Slov. 48 141

[27] Marcio F. Cornelio, Marcos C. de Oliveira, and Felipe F. Fanchini, Phys. Rev. Lett. 107, 020502 (2011)

[28] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A 53 (1996) 2046.

[29] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 1996.

[30] Reinhard F. Werner (1989). Physical Review A 40 (8): 4277–4281.

[31] M. Horodecki, P. Horodecki, and R. Horodecki, Report No. quant-ph/9607009.

[32] Vlad Gheorghiu, Marcos C. de Oliveira, and Barry C. Sanders Phys. Rev. Lett. 115, 030403 2015.

[33] F F Fanchini, L K Castelano, M F Cornelio and M C de Oliveira. New Journal of Physics, Volume 14, January 2012

[34] Harold Ollivier and Wojciech H. Zurek, Phys. Rev. Lett. 88, 017901 (2001)

[35] http://arxiv.org/pdf/0807.4490v1.pdf

[36] Li-Xiang Cen, Xin-Qi Li, Jiushu Shao, and YiJing Yan Physical Review A 83, 054101 (2011)

[37] orivoje Dakic, Vlatko Vedral, and Caslav Brukner Phys. Rev. Lett. 105, 190502 2010

[38] Holevo, Alexander S. (1973). Problems of Information Transmission 9: 177–183

[39] O. Lanford and D. Robinson, "Mean Entropy of States in Quantum Statistical Mechanics" J. Math. Phys. 9, 1120-1125 (1968).

[40] E. Lieb and M.B. Ruskai, "A Fundamental Property of Quantum Mechanical Entropy" Phys. Rev. Lett. 30, 434-436 (1973)

[41] E. Lieb and M.B. Ruskai, "Proof of the Strong Subadditivity of Quantum Mechanical Entropy" J. Math. Phys. 14, 1938–1941 (1973).

[42] E. Lieb, Convex Trace Functions and the Wigner-Yanase-Dyson conjecture" Adv. Math. 11, 267

[43] S. Golden, Phys. Rev. 137 (1965), B1127–B1128.

[44] C.J. Thompson, J. Math. Phys. 6 (1965) 1812–813.

[45] K. Symanzik, J. Math. Phys. 6 (1965), 1155–1156.

[46] F. F. Fanchini, M. F. Cornelio, M. C. de Oliveira, A. O. Caldeira, Phys. Rev. A **84**, 012313 (2011).

[47] M. Koashi A. Winter Phys. Rev. A 69(2):022309, 2004

[48] Valerie Coffman, Joydip Kundu, and William K. Wootters, Phys. Rev. A 61, 052306 (2000)

[49] http://quantumfrontiers.com/2013/04/29/a-public-lecture-on-quantum-information/

[50] Bennett, C., "Quantum cryptography using any two nonorthoganol states.", Phys. Rev. Lett. 68, 1992, pp. 3121-3124.

[51] Dénes Petz. Quarterly Journal of Mathematics, 39(1):97–108, 1988.

[52] Dénes Petz. Communications in Mathematical Physics, 105(1):123–131, March 1986.

[53] Masato Koashi and Nobuyuki Imoto, Physical Review A, 66, 022318, 2002

[54] Göran Lindblad. Letters in Mathematical Physics 47: 189–196, 1999

[55] M. Takesaki: Theory of Operator Algebras I. NewYork–Heidelberg–Berlin: Springer–Verlag, 1979