



ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΜΕΤΑΠΤΥΧΙΑΚΕΣ ΣΠΟΥΔΕΣ ΣΤΑ ΜΑΘΗΜΑΤΙΚΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**ΕΝΤΡΟΠΙΑ ΚΑΙ ΣΥΣΧΕΤΙΣΕΙΣ ΣΕ ΣΥΣΤΗΜΑΤΑ
QUBIT: ΜΙΑ ΜΕΛΕΤΗ ΤΗΣ ΕΝΤΡΟΠΙΑΣ VON
NEUMANN ΚΑΙ ΤΗΣ ΑΜΟΙΒΑΙΑΣ ΠΛΗΡΟΦΟΡΙΑΣ**

ΓΕΩΡΓΙΟΣ ΣΤΑΥΡΟΠΟΥΛΟΣ

**ΕΠΙΒΛΕΠΟΝΤΕΣ ΚΑΘΗΓΗΤΕΣ:
ΜΙΧΑΗΛ ΑΝΟΥΣΗΣ
ΑΝΔΡΕΑΣ ΑΡΒΑΝΙΤΟΓΕΩΡΓΟΣ**

**ΠΑΤΡΑ
ΣΕΠΤΕΜΒΡΙΟΣ, 2026**

Περίληψη

Η Κβαντική Θεωρία Πληροφορίας (ΚΘΠ) παρέχει ένα μαθηματικό πλαίσιο βασισμένο στη θεωρία πληροφορίας για την περιγραφή κβαντικών συστημάτων και των στατιστικών τους ιδιοτήτων. Σκοπός της παρούσας Μεταπτυχιακής Διπλωματικής Εργασίας είναι η ανάπτυξη βασικών εννοιών της ΚΘΠ, ξεκινώντας από το μαθηματικό πλαίσιο της ΚΘΠ και καταλήγοντας στην εισαγωγή της εντροπίας von Neumann και της αμοιβαίας πληροφορίας ως ποσοτικών μέτρων του μέσου πληροφοριακού περιεχομένου και των συνολικών συσχετίσεων μεταξύ των υποσυστημάτων ενός σύνθετου κβαντικού συστήματος, αντίστοιχα. Η μαθηματική γλώσσα των τελεστών πυκνότητας παρουσιάζεται ως η γενική μαθηματική γλώσσα των κβαντικών καταστάσεων, ενσωματώνοντας τόσο τις καθарές όσο και τις μεικτές καταστάσεις εντός ενός κοινού μαθηματικού φορμαλισμού. Η πληροφοριακή περιγραφή των κβαντικών καταστάσεων αναπτύσσεται πάνω σε αυτό το θεμέλιο, μέσω της παρουσίασης της εντροπίας von Neumann και των βασικών μαθηματικών της ιδιοτήτων· ιδιαίτερη έμφαση δίνεται στην δεσμευμένη εντροπία και την σχετική εντροπία, των οποίων οι βασικές ιδιότητες καθορίζονται και ερμηνεύονται στο πλαίσιο της ΚΘΠ. Το τελικό μέρος της Μεταπτυχιακής Διπλωματικής Εργασίας είναι αφιερωμένο στην παρουσίαση της αμοιβαίας πληροφορίας von Neumann· παρουσιάζονται οι βασικές μαθηματικές της ιδιότητες, μαζί με ισοδύναμες εκφράσεις της αμοιβαίας πληροφορίας von Neumann ως προς την εντροπία von Neumann, την δεσμευμένη εντροπία και τη σχετική εντροπία, από τις οποίες προκύπτει η ερμηνεία της αμοιβαίας πληροφορίας von Neumann ως ένα μέτρο των συνολικών συσχετίσεων σε ένα σύνθετο κβαντικό σύστημα. Αντιπροσωπευτικά παραδείγματα που περιλαμβάνουν τανυστικά γινόμενα καταστάσεων, διαχωρίσιμες καταστάσεις, και μέγιστα εμπλεγμένες καταστάσεις Bell, αναδεικνύουν τη συμπεριφορά της αμοιβαίας πληροφορίας von Neumann για διαφορετικές κλάσεις κβαντικών καταστάσεων. Οι έννοιες της ΚΘΠ, που αναπτύσσονται καθ' όλη τη διάρκεια της Μεταπτυχιακής Διπλωματικής Εργασίας παρέχουν απαραίτητες προϋποθέσεις για πιο προχωρημένα θέματα στην ΚΘΠ, συμπεριλαμβανομένων των εφαρμογών της στην κβαντική θεωρία μέτρησης, και στο ευρύτερο πεδίο της θεμελίωσης της κβαντικής θεωρίας.

Hellenic Open University
School of Science and Technology
Postgraduate Studies in Mathematics
Master's Thesis

Entropy and Correlations in Qubit Systems: A study of the von Neumann Entropy and Mutual Information

Georgios Stavropoulos

Supervisors:

Dr. Michael Anousis
Dr. Andreas Arvanitogeorgos

Dissertation submitted to the Hellenic Open University
in partial fulfillment of the requirements for the Degree of:

Master of Science in Mathematics

June, 2026

Abstract

Quantum Information Theory (QIT) provides an information-theoretic mathematical framework for the description of quantum systems and their statistical properties. The purpose of the present Master's Thesis is to develop essential concepts of QIT, beginning from the mathematical framework of QIT, and culminating in the introduction of the von Neumann entropy and mutual information as quantitative measures of the average information content and of the total correlations between by the subsystems of a composite quantum system. The language of density operators is presented as the general language of quantum states, accommodating both pure and mixed states within a common mathematical formalism. The information-theoretic description of quantum states is developed upon this foundation, through the presentation of the von Neumann entropy and its essential mathematical properties; specific emphasis is placed on the conditional entropy and the relative entropy, whose essential properties are established and interpreted within the context of QIT. The final part of the Thesis is devoted to the presentation of the von Neumann mutual information; its essential mathematical properties are presented, along with equivalent formulations of the von Neumann mutual information in terms of the von Neumann entropy, the conditional entropy, and the relative entropy, from which the interpretation of the von Neumann mutual information as a measure of the total correlations in a composite quantum system emerges. Representative examples involving product states, separable states, and maximally entangled Bell states, highlight the behaviour of the von Neumann mutual information, for different classes of quantum states. The concepts of QIT developed throughout the Thesis provide essential prerequisites for more advanced topics in QIT, including its applications to the quantum theory of measurement, and the to broader field of the foundations of quantum theory.

Contents

Overture	1
1 Motivation and Introduction	5
1.1 Context and Motivation for Quantum Information Theory	5
1.2 The concepts of von Neumann Entropy and Mutual Information in Quantum Information Theory	5
1.3 The ideal case of Quantum States of Qubit Systems	6
1.4 Purpose and Structure of the Master's Thesis	6
2 Mathematical Framework of Quantum Information Theory	7
2.1 Quantum Systems and Quantum States	7
2.1.1 Quantum States	8
2.1.2 Composite Quantum Systems	9
2.2 Qubit Systems and States	10
2.2.1 Composite Qubit Systems	11
3 The von Neumann Entropy	13
3.1 Definition of the von Neumann Entropy	13
3.1.1 The Range of the von Neumann Entropy	14
3.2 The von Neumann Entropy for qubit States	15
3.2.1 Product 2-qubit States	15
3.2.2 Separable and Entangled 2-qubit States	15
3.3 The Conditional and the Relative Entropy for 2-qubit States	16
3.3.1 The Conditional Entropy for 2-qubit States	16
3.3.2 The Relative Entropy for 2-qubit States	16
3.4 Mathematical Properties of the von Neumann Entropy	17
3.4.1 The Subadditivity Theorems	17
3.4.2 Entanglement and the Conditional Entropy	18
3.4.3 Distinguishability and the Relative Entropy	20
3.4.4 Concavity of the von Neumann Entropy	21
4 The von Neumann Mutual Information	23
4.1 Definition of the von Neumann Mutual Information	23
4.1.1 The Sign of the von Neumann Mutual Information	25
4.2 Mathematical Properties of the von Neumann Mutual Information	25
4.2.1 The Symmetry of the von Neumann Mutual Information	25

4.2.2	The Relation between the von Neumann Mutual Information and the von Neumann Relative Entropy	25
4.3	The von Neumann Mutual Information for typical qubit States	27
4.3.1	Product 2-qubit states	27
4.3.2	Separable 2-qubit States	27
4.3.3	Entangled 2-qubit States: The canonical example of the Bell States	28

5	Conclusions and Future Perspectives	30
----------	--	-----------

Overture

It is the author's understanding that we live in an era that is characterised by emerging and developing unscientific views, and especially by views of distrust of, or even hostility towards, scientific methodology, and science, in general. It is also the author's opinion that the general causes of this cognitive decline are evident, and that its effects are certainly detrimental, and potentially destructive, to civilisation; such a discussion being, however, certainly well beyond the purpose of the current presentation. With regard to the general topic of the present Master's Thesis, inside the multitude of diverse examples of such fallacious and reprehensible unscientific views, there exists a distinctive class of specific cases of misconceptions relating to quantum theory. These cases vary between expositions of usually well-intentioned, yet untenable, "alternative" interpretations of the formalism of quantum theory, often endeavouring to undermine the irreducibility of the probabilistic character of quantum theory, and instances of predominantly profit-seeking, blatant conceptual abominations, customarily striving to fuse quantum theory with various delusional superstitions. Taking into account the potentially dire situation regarding the typical public acceptance of scientific methodology, the author considers at least a brief statement on the general and essential issues of scientific methodology, to be imperative. Although, throughout this Master's Thesis, general or more special philosophical and methodological issues are not explicitly considered, the presentation of the essential concepts of QIT is consistent with critical scientific realism generally, and specifically emergent materialism, as it is documented in [1]. In that capacity, through consideration of objective reality as existence independently of any form of consciousness, and of quantum systems as the elements of the ontology of quantum theory, the author generally accepts the objective reality of quantum systems, as well as of all the properties and motion in quantum systems, and specifically accepts the objective reality of space-time, as the form of existence in quantum systems, that is to say, accepts quantum systems as material entities. Accordingly, all concepts that are contained in this Master's Thesis, are considered to reflect objectively real features of quantum systems.

Chapter 1

Motivation and Introduction

1.1 Context and Motivation for Quantum Information Theory

Quantum Information Theory (QIT) is a discipline that studies the information content of quantum theory, by extending and, thus, generalising concepts from the traditional, classical information theory, in order to describe the statistical structure and properties of quantum states. Due to the fundamentally and irreducibly probabilistic character of quantum theory, classical information theory, being a systematic combination of probability theory, statistics, and statistical mechanics, offers a natural candidate of a mathematical framework to be extended and generalised for the purpose of its application to the description of the statistical structure and the various statistical properties of quantum states, and, thus, for the deeper comprehension of the various concepts of quantum theory.

Since its emergence near the middle of the 20th century, knowledge of QIT is in the process of becoming indispensable for quantum scientists in general, whether their interest lies in applied or in more theoretical aspects of quantum mechanics. The highly anticipated applications of QIT, with quantum computation as the prime example, fuelled the scientific interest and endeavour of physicists and mathematicians alike in QIT, originating, consequently, the various specialised disciplines that constitute the general, and rapidly developing, technological field of quantum engineering. The conceptual depth, and accordingly, the significance of QIT, is naturally highly diverse; this is, of course, to be expected, as it is certainly true for both of its theoretical components, namely classical information theory, and quantum theory. A distinguished example, illustrating this conceptual depth of QIT, is its generalisation of the concept of entropy, by the formalisation of the concept of entropy in a systematic manner, and in relation with the statistical structure of quantum states.

1.2 The concepts of von Neumann Entropy and Mutual Information in Quantum Information Theory

The concept of entropy is essential to QIT. The von Neumann entropy, being the quantum extension and generalisation of the Shannon entropy of classical information theory, naturally expresses the average information content of quantum states [2]. It can be proved that the value of the average information content of a quantum state is inextricably linked to the degree of the purity

(or, conversely, of the mixedness) of the quantum state, which, thus, may also be quantified by the value of the von Neumann entropy [3]. The importance of the von Neumann entropy is highly manifest in the case of composite quantum systems as well, as certain quantum states of such systems may possess various degrees of quantum entanglement. Quantum entanglement is a property of certain quantum states of any composite quantum system, that expresses the existence of quantum correlations between its subsystems; this property of quantum entanglement is one of the most characteristic properties of certain quantum states of composite quantum systems, as it is a property, which is purely quantum, that is to say, which has no classical counterpart. Various derived types of entropy, which are defined through the von Neumann entropy, are measures of the various aspects of the quantum entanglement of a quantum state of a quantum system; the prime examples of these derived types of entropy are the conditional von Neumann entropy, the von Neumann mutual information, and the relative entropy, all three of which express different, yet linked, relational aspects of the von Neumann entropy of the quantum state of a composite quantum system and the von Neumann entropies of the quantum states of its various subsystems. Notably, the von Neumann mutual information, being the quantum extension and generalisation of the Shannon mutual information of classical information theory, is a measure of the total correlations, both classical as well as due to quantum entanglement, between the subsystems of a composite quantum system, in a certain quantum state; the von Neumann mutual information is, thus, a central indicator of the statistical structure and the various statistical properties of quantum states.

1.3 The ideal case of Quantum States of Qubit Systems

The qubit (quantum+bit) is the quantum analogue of the classical bit; that is to say, the qubit is the quantum extension and generalisation of the classical bit. All the possible, quantum states of qubit systems, that is to say, of simple or composite quantum systems consisting solely of qubits, constitute a certain qubit - Fock subspace of the universal Hilbert space of quantum theory. The members of this qubit - Fock subspace possess a relatively less complex statistical structure and properties; thus, they seem ideal for a relatively clearer presentation, lacking in heavy calculations, of the general, and essential, concepts of QIT. Therefore, throughout this Master's Thesis, the author, preferring conceptual clarity to computational prowess, will consider mainly quantum states of qubit systems, though all of the essential mathematical facts, in this Master's Thesis, which are relative to quantum states of qubit systems, may be appropriately generalised for quantum states of any quantum system in a straightforward manner.

1.4 Purpose and Structure of the Master's Thesis

The main purpose of this Master's Thesis is a clear, concise, and relatively independent, presentation of the von Neumann entropy and mutual information in qubit systems. The current presentation is structured as follows: Chapter 2 is a short introduction to the main aspects of the mathematical framework of QIT, with specific reference to quantum states of qubit systems. Chapter 3 is devoted to the presentation of the von Neumann entropy, including its properties in quantum states of single qubit systems and of 2-qubit systems. Chapter 4 is an exposition of classical and quantum correlations in quantum states of 2-qubit systems, after identifying the von Neumann mutual information, as a measure of the total correlations in a quantum state. Finally, Chapter 5 is a summary of the concepts that are contained in the current Master's Thesis, indicating the significance of its contents, and mentioning its potential expansions.

Chapter 2

Mathematical Framework of Quantum Information Theory

The purpose of this Chapter is to introduce the essential mathematical framework of QIT required for the study of the von Neumann entropy and mutual information in qubit systems. To this end, the fundamental definitions regarding generally quantum systems and their states, and specifically qubits, are presented, which form the foundation for the concepts that are contained in the subsequent Chapters. Indeed, this Chapter is not intended as a complete exposition of quantum theory; in fact, several important, yet irrelevant to the purposes of this Thesis, notions of quantum theory, such as measurement, have been omitted. The structure and notation used in this Chapter follows that of [2], to a certain measure.

2.1 Quantum Systems and Quantum States

A *quantum system* may be most generally regarded as a mathematical abstraction of a physical system, which is capable of storing store quantum information, that is to say, as a *register* [2]. Appropriately, for any description of a quantum system, a complex vector space, along with its dual space, and a relative index set, may be considered to be associated to the quantum system. In the context of QIT, such complex vector spaces are, typically, finite-dimensional complex Euclidean spaces, anti-isomorphic to their dual spaces, and determine the mathematical setting, in which quantum states may be defined; naturally, subsets of $\mathbb{N}$ may, without loss of generality, be used as index sets relative to these complex vector spaces, or even relative to any space associated to them, in any respect, and they will be used as such implicitly throughout this Thesis.

A n -dimensional complex Euclidean space, denoted by $\mathbb{C}^n$, is a vector space over the field of complex numbers, $\mathbb{C}$. The inner product on $\mathbb{C}^n$ is defined as a function:

$$\langle \bullet, \bullet \rangle: \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}$$

satisfying the properties of linearity and conjugate-symmetry; in particular, the inner product on $\mathbb{C}^n$ is conjugate-linear in the first and linear in the second argument. This inner product induces a positive-definite norm:

$$\forall x \in \mathbb{C}^n \quad (\|x\| := \sqrt{\langle x, x \rangle} \geq 0)$$

where $\|x\| = 0 \Leftrightarrow x := 0$. An orthonormal basis of $\mathbb{C}^n$ is denoted by $\{e_k\}$.

Operators over $\mathbb{C}^n$

The set of all operators over $\mathbb{C}^n$, mapping $\mathbb{C}^n$ to subsets of itself, is denoted by $\mathcal{L}(\mathbb{C}^n)$. Five special subsets of $\mathcal{L}(\mathbb{C}^n)$ are the following:

I. The subset of normal operators, which is denoted by $\mathcal{N}(\mathbb{C}^n)$, that is defined as:

$$\mathcal{N}(\mathbb{C}^n) := \{N \in \mathcal{L}(\mathbb{C}^n) : N^*N = NN^*\} \quad (2.1)$$

II. The subset of self-adjoint operators, which is denoted by $\mathcal{S}(\mathbb{C}^n)$, that is defined as:

$$\mathcal{S}(\mathbb{C}^n) := \{S \in \mathcal{L}(\mathbb{C}^n) : S^* = S\} \quad (2.2)$$

III. The subset of positive semi-definite operators, which is denoted by $Pos(\mathbb{C}^n)$, that is defined as:

$$Pos(\mathbb{C}^n) := \{P \in \mathcal{L}(\mathbb{C}^n) : (\exists X \in \mathcal{L}(\mathbb{C}^n) : P = X^*X)\} \quad (2.3)$$

IV. The subset of density operators, which is denoted by $\mathcal{D}(\mathbb{C}^n)$, that is defined as:

$$\mathcal{D}(\mathbb{C}^n) := \{\rho \in Pos(\mathbb{C}^n) : Tr(\rho) = 1\} \quad (2.4)$$

V. The subset of projection operators, which is denoted by $\mathcal{P}(\mathbb{C}^n)$, that is defined as:

$$\mathcal{P}(\mathbb{C}^n) := \{\Pi \in Pos(\mathbb{C}^n) : \Pi^2 = \Pi\} \quad (2.5)$$

Evidently, it holds that: $\mathcal{P}(\mathbb{C}^n), \mathcal{D}(\mathbb{C}^n) \subset Pos(\mathbb{C}^n) \subset \mathcal{S}(\mathbb{C}^n) \subset \mathcal{N}(\mathbb{C}^n) \subset \mathcal{L}(\mathbb{C}^n)$. Normal operators are characterised by the spectral theorem, which states that any normal operator can be entirely expressed as a linear combination of, mutually orthogonal, projection operators [2]. Furthermore, it can be straightforwardly proved that the eigenvalues of self-adjoint operators are real, and that the eigenvalues of positive semi-definite operators are real and non-negative; specifically, an eigenvalue of any projection operator may be either 0 or 1.

2.1.1 Quantum States

A *quantum state* may be most generally regarded to be a mathematical abstraction of a physical state of a quantum system. A quantum state is typically defined as a density operator in $\mathcal{D}(\mathbb{C}^n)$. Accordingly, the general properties of quantum states are, by definition, in correspondence to the mathematical properties of density operators in $\mathcal{D}(\mathbb{C}^n)$. It can be straightforwardly proved that $\mathcal{D}(\mathbb{C}^n)$ is a convex set. Thus, for any subset:

$$\{\rho_k\} \subset \mathcal{D}(\mathbb{C}^n)$$

it holds that any convex sum of its elements is an element of $\mathcal{D}(\mathbb{C}^n)$, that is to say:

$$\sum_k p(k)\rho_k \in \mathcal{D}(\mathbb{C}^n)$$

As any convex sum in $\mathcal{D}(\mathbb{C}^n)$ is by its definition related to a probability distribution, convex sums in $\mathcal{D}(\mathbb{C}^n)$ are called *probabilistic mixtures* of quantum states. Any probabilistic mixture of quantum states may be associated to a function $\eta : \mathbb{N} \rightarrow Pos(\mathbb{C}^n)$, iff $Tr(\eta)$ is a probability distribution;

such a function η is called an *ensemble* of quantum states [2]. Specifically, for an ensemble of quantum states, η , its range, $\{\eta(k)\}$, is associated, through its probability distribution, $Tr(\eta)$, to the probabilistic mixture of quantum states $\sum_k \eta(k)$; thus, any element of the range of η corresponds to a quantum state along with the probability related to it [2]. It is worth noting that the map from ensembles of quantum states to probabilistic mixtures of quantum states is not injective in general; it can be proved that different ensembles of quantum states may be associated to the same probabilistic mixture of quantum states.

Flat, Pure, and Mixed Quantum States

Any projection operator of non-zero rank, Π , may characterise a density operator, ρ , in the sense of the following:

$$\rho = \frac{\Pi}{Tr(\Pi)} \quad (2.6)$$

Quantum states of the above form are called *flat* states [2]. As the trace of a projection operator is equal to its rank, a projection operator is by itself a density operator *iff* its rank is equal to 1, specifically. Any quantum state that is equal to a rank-1 projection operator, is called a *pure* state; any quantum state that is not a pure state is called a *mixed* state. As any density operator is also a normal operator, it may be entirely expressed as a convex linear combination of, mutually orthogonal, projection operators; therefore, any mixed state is equal to a probabilistic mixture. As a reminder, the map from ensembles of quantum states to probabilistic mixtures of quantum states is not injective in general; thus, there is not, in general, a unique ensemble of quantum states associated to a mixed state.

A particularly interesting instance of a mixed state that is also a flat state is the *completely mixed state*, that has a form as in the following:

$$\rho = \frac{I_{\mathbb{C}^n}}{n} \quad (2.7)$$

where $I_{\mathbb{C}^n}$ is the identity operator over $\mathbb{C}^n$. A completely mixed state is equivalent to a uniform probabilistic mixture, so its form may represent a situation of a complete lack of knowledge about the relevant quantum system [2].

2.1.2 Composite Quantum Systems

In the case of a composite quantum system, consisting of any number of quantum subsystems, the possible quantum states evidently constitute the set of density operators over the relevant tensor product complex Euclidean space. For instance, in the case of a composite quantum system, consisting of two quantum subsystems, the relevant complex Euclidean space is $\mathbb{C}^n \otimes \mathbb{C}^m$, so the possible quantum states constitute the set $\mathcal{D}(\mathbb{C}^n \otimes \mathbb{C}^m)$. A special subset of $\mathcal{D}(\mathbb{C}^n \otimes \mathbb{C}^m)$ is the subset of product states, consisting of quantum states that can be expressed as tensor products; this subset is inherently contained in another special subset of $\mathcal{D}(\mathbb{C}^n \otimes \mathbb{C}^m)$, the subset of separable states, consisting of convex sums of product states. Any quantum state that is not a separable state is called an *entangled* state; the concept of entangled states is of great importance in QIT, and is in the core of the concepts that are contained in the subsequent Chapters.

The Partial Trace, Reduction, and Extensions

In the case of a composite quantum system, a characterisation of the quantum state of a subsystem, independently of the remainder of the composite quantum system, is often essential. The mathematical entity to be considered for this purpose is the partial trace. Considering an arbitrary tensor product complex Euclidean space, $\mathbb{C}^n \otimes \mathbb{X}$, the partial trace with respect to the complex Euclidean space $\mathbb{X}$, which is denoted by $Tr_{\mathbb{X}}$, is a linear mapping, that is appropriately defined as in the following:

$$(Tr_{\mathbb{X}} : \mathcal{L}(\mathbb{C}^n \otimes \mathbb{X}) \rightarrow \mathcal{L}(\mathbb{C}^n)) : \forall A \in \mathcal{L}(\mathbb{C}^n), B \in \mathcal{L}(\mathbb{X}) \quad (Tr_{\mathbb{X}}(A \otimes B) = A Tr(B)) \quad (2.8)$$

It is evident that the partial trace, $Tr_{\mathbb{X}}$, is uniquely determined by the above definition, (2.8), due to linearity. In the specific case of a quantum state $\rho \in \mathcal{D}(\mathbb{C}^n \otimes \mathbb{X})$, the partial trace $Tr_{\mathbb{X}}(\rho) \in \mathcal{D}(\mathbb{C}^n)$ is called the *reduced quantum state*, or, simply, the *reduction*, of the quantum state ρ , with respect to the complex Euclidean space $\mathbb{C}^n$; conversely, the quantum state $\rho \in \mathcal{D}(\mathbb{C}^n \otimes \mathbb{X})$ is an *extension* of the quantum state $Tr_{\mathbb{X}}(\rho) \in \mathcal{D}(\mathbb{C}^n)$, with respect to the tensor product complex Euclidean space $\mathbb{C}^n \otimes \mathbb{X}$. It can be straightforwardly proved that, while a reduction of a quantum state with respect to a particular complex Euclidean space is uniquely determined, by the partial trace, any quantum state may have infinite extensions with respect to a particular complex Euclidean space. A specific kind of extensions of a quantum state are extensions to pure states; these extensions are called *purifications*. The concept of purifications of a quantum state is often quite useful in QIT, simplifying various complicated calculations, in virtue of allowing for consideration of pure states instead of mixed states.

2.2 Qubit Systems and States

The qubit (quantum+bit) is the quantum analogue of the classical bit; that is to say, the qubit is the quantum extension and generalisation of the classical bit. Accordingly, a qubit is a specific case of a quantum system, which may be appropriately considered to be associated to the complex Euclidean space $\mathbb{C}^2$; an arbitrary qubit state may then be expressed as a density operator $\rho \in \mathcal{D}(\mathbb{C}^2)$. Denoting an orthonormal basis of $\mathcal{L}(\mathbb{C}^2)$ by E_{ab} , an arbitrary qubit state is expressed as:

$$\rho = \sum_{a,b=1}^2 \rho_{ab} E_{ab} \quad (2.9)$$

with:

$$\rho_{22} = 1 - \rho_{11} \quad (2.10)$$

$$\rho_{21} = \overline{\rho_{12}} \quad (2.11)$$

and:

$$|\rho_{12}|^2 \leq \rho_{11}(1 - \rho_{11}) \quad (2.12)$$

where the equality holds *iff* the state is pure. Obviously, the completely mixed state of a qubit satisfies $\rho_{12} = \rho_{21} = 0$, and thus possesses the eigenvalues $\rho_{11} = \rho_{22} = \frac{1}{2}$. The eigenvalues of a density operator play a central role in QIT; as it will become apparent in the following Chapter, the value of the von Neumann entropy depends exclusively on these eigenvalues. Consequently, the spectral properties of qubit states provide the means of quantifying information in quantum systems.

2.2.1 Composite Qubit Systems

Although arbitrary states of qubits already exhibit uniquely quantum features, such as superposition, which are not considered here, the most distinctive phenomena of QIT happen when several qubits are combined into a composite quantum system, as only the structure of a composite quantum system can amount to quantum entanglement, and, thus, correlations between its subsystems. The canonical examples of such composite qubit systems, for the exhibition of correlations between their subsystems, are 2-qubit systems. Naturally, a 2-qubit system is associated to the complex Euclidean space is $\mathbb{C}^2 \otimes \mathbb{C}^2$, and an arbitrary 2-qubit state may then be expressed as a density operator $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. Given two arbitrary qubit states for the 2 qubits, $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$, the product state, $\rho^{(AB),\Pi} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, may be expressed in a straightforward manner, as:

$$\rho^{(AB),\Pi} = \rho^{(A)} \otimes \rho^{(B)} \quad (2.13)$$

while a convex sum of product states $\rho_n^{(AB),\Pi} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ having the above form, may express a separable state, $\rho^{(AB),\Sigma} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, as:

$$\rho^{(AB),\Sigma} = \sum_n p(n) \rho_n^{(AB),\Pi} \quad (2.14)$$

In the case of an arbitrary product state of a 2-qubit system, $\rho^{(AB),\Pi} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, of the form of the above eq. (2.13), it is evident that its reduced states are simply its factor states $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$. In the case of an arbitrary separable state of a 2-qubit system, $\rho^{(AB),\Sigma} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, of the form of the above eq. (2.14), it is evident that its reduced states, $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$, are the respective probabilistic mixtures of the states $\rho_n^{(A)}, \rho_n^{(B)} \in \mathcal{D}(\mathbb{C}^2)$; this fact generally suggests the existence of classical correlations between the subsystems of a composite quantum system, when its quantum state is a separable state.

A pedagogical example

Consider the pure qubit states:

$$E_{11}, E_{22} \in \mathcal{D}(\mathbb{C}^2)$$

These states determine the product states:

$$\rho_1^{(AB),\Pi} = E_{11} \otimes E_{11}, \quad \rho_2^{(AB),\Pi} = E_{11} \otimes E_{22}, \quad \rho_3^{(AB),\Pi} = E_{22} \otimes E_{11}, \quad \rho_4^{(AB),\Pi} = E_{22} \otimes E_{22}$$

as well as the family of separable states composed by the convex sums of the form:

$$\rho^{(AB),\Sigma} = \sum_{n=1}^4 p_n \rho_n^{(AB),\Pi}$$

The reduced states are, respectively:

$$\rho_1^{(A)} = E_{11}, \quad \rho_1^{(B)} = E_{22}$$

$$\rho_2^{(A)} = E_{11}, \quad \rho_2^{(B)} = E_{22}$$

$$\rho_3^{(A)} = E_{22}, \quad \rho_3^{(B)} = E_{11}$$

$$\rho_4^{(A)} = E_{22}, \quad \rho_4^{(B)} = E_{11}$$

as well as:

$$\rho^{(A)} = \sum_{n=1}^4 p_n \rho_n^{(A)}$$

$$\rho^{(B)} = \sum_{n=1}^4 p_n \rho_n^{(B)}$$

Entangled Quantum States and the Bell States

Most of the states $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ are not separable, thus, they are entangled states. As it has already been mentioned, entangled states play a central role in QIT, and constitute the source of quantum correlations; as it will become apparent in the subsequent Chapters, the von Neumann entropy and mutual information provide powerful means for measuring such correlations. The canonical examples of 2-qubit entangled states are the four Bell states, $\phi^{(AB),\pm}$ and $\psi^{(AB),\pm}$, where:

$$\phi^{(AB),\pm} := \frac{1}{2}(E_{11} \otimes E_{11} \pm E_{11} \otimes E_{22} \pm E_{22} \otimes E_{11} + E_{22} \otimes E_{22}) \quad (2.15)$$

and:

$$\psi^{(AB),\pm} := \frac{1}{2}(E_{12} \otimes E_{12} \pm E_{12} \otimes E_{21} \pm E_{21} \otimes E_{12} + E_{21} \otimes E_{21}) \quad (2.16)$$

Considering that $E_{ab}E_{cd} = \delta_{bc}E_{ad}$, it can be easily proved that the four Bell states are pure states. A remarkable fact regarding the Bell states is that, although they themselves are pure states, the quantum state of any subsystem is a completely mixed state; this fact can be easily verified through the partial trace with respect to the other subsystem, as in the following: Denoting the quantum states of the subsystems as $\rho^{(A),(B)}$, it is the case that: $\rho^{(A),(B)} = \text{Tr}_{B,A}(\rho^{(AB)})$; application to any of the Bell states, $\rho^{(AB)} = \phi^{(AB),\pm}, \psi^{(AB),\pm}$, yields that:

$$\rho^{(A)} = \rho^{(B)} = \frac{1}{2}I_{\mathbb{C}^2} \quad (2.17)$$

The Bell states provide the simplest examples of pure entangled states, exhibiting particular cases of correlations between the subsystems of a 2-qubit system, and serve as the canonical examples of pure, entangled states of a 2-qubit system; for this reason, the Bell states will be used repeatedly in the subsequent Chapters. Moreover, it is evident that, with respect to purity and quantum entanglement, the four Bell states are equivalent; for this reason, in the subsequent Chapters, it will be sufficient to consider, without loss of generality, a single Bell representative, for the exhibition of the various measures of correlations between the subsystems of a 2-qubit system.

Chapter 3

The von Neumann Entropy

The purpose of this Chapter is to introduce the von Neumann entropy, as the quantum extension and generalisation of the Shannon entropy of classical information theory, and to present its essential mathematical properties in quantum states of single qubit systems and of 2-qubit systems.

3.1 Definition of the von Neumann Entropy

As it was mentioned in the previous Chapter, normal operators are characterised by the spectral theorem, which states that any normal operator can be entirely expressed as a linear combination of, mutually orthogonal, projection operators [2]. Any density operator, being a normal operator itself, admits such an expression, which is termed as its *spectral decomposition*. Thus, for any $\rho \in \mathcal{D}(\mathbb{C}^n)$, it holds that:

$$\rho = \sum_k \lambda_k \Pi_k \quad (3.1)$$

where $\Pi_k \in \mathcal{P}(\mathbb{C}^n)$, and:

$$\Pi_k \Pi_l = \delta_{kl} \Pi_k \quad (3.2)$$

As $\rho \in \mathcal{D}(\mathbb{C}^n) \subset \text{Pos}(\mathbb{C}^n)$, it also holds that $\lambda_k \geq 0$, and that:

$$\text{Tr}(\rho) = \sum_k \text{rank}(\Pi_k) \lambda_k = 1 \quad (3.3)$$

Moreover, through consideration of the determinant of ρ , it is evident that the coefficients λ_k are the eigenvalues of ρ , each with an algebraic multiplicity of $m_k = \text{rank}(\Pi_k)$. Consequently, the eigenvalues of ρ , each of them counted according to its multiplicity, constitute a probability distribution. This fact establishes a close connection between quantum states and classical information theory; specifically, it suggests an extension and generalisation of the Shannon entropy of classical information theory, H , for a probability distribution $\{p_k\}$:

$$H(\{p_k\}) := - \sum_k p_k \log(p_k)$$

to its QIT counterpart, S , for the quantum state ρ of eq. (3.1):

$$S(\{\lambda_k\}) := - \sum_k m_k \lambda_k \log(\lambda_k) \quad (3.4)$$

The standard mathematical reflex is to try to express eq. (3.4) in a form that exhibits the quantum state ρ of eq. (3.1) explicitly. To this end, eq. (3.1) may give the following:

$$\log(\rho) = \sum_k \log(\lambda_k) \Pi_k$$

and multiplication of eqs. (3.1) and (3.4) yields:

$$\rho \log(\rho) = \sum_{k,l} \lambda_l \log(\lambda_k) \Pi_k \Pi_l$$

which, due to eq. (3.2), is simplified to the following:

$$\rho \log(\rho) = \sum_k \lambda_k \log(\lambda_k) \Pi_k$$

A straightforward trace on the above expression results in the standard definition of the *von Neumann entropy* of the quantum state ρ :

$$S(\rho) := -\text{Tr}(\rho \log(\rho)) = -\sum_k m_k \lambda_k \log(\lambda_k) \quad (3.5)$$

The above general derivation of the standard definition of the von Neumann entropy of an arbitrary quantum state elucidates its connection to the Shannon entropy of classical information theory, from the naturally justifiable fact that it may depend only on the eigenvalues of the relevant quantum state. It is thus evident that the von Neumann entropy naturally expresses the average information content of quantum states.

3.1.1 The Range of the von Neumann Entropy

It is evident from eq. (3.3) that, for an arbitrary $\rho \in \mathcal{D}(\mathbb{C}^n)$, it holds that:

$$S(\rho) \geq 0 \quad (3.6)$$

The above eq. (3.6) expresses the *positivity* of the von Neumann entropy. The maximum value of the von Neumann entropy of an arbitrary $\rho \in \mathcal{D}(\mathbb{C}^n)$ may be found considering the concavity of the function $f(x) = \log(x)$: Jensen's inequality [2] yields:

$$\sum_k m_k \lambda_k \log\left(\frac{1}{\lambda_k}\right) \leq \log\left(\sum_k m_k \lambda_k \frac{1}{\lambda_k}\right)$$

that is to say:

$$S(\rho) \leq \log(n) \quad (3.7)$$

Concisely, it is thus the case that, for any $\rho \in \mathcal{D}(\mathbb{C}^n)$, the range of the von Neumann entropy is in the following:

$$0 \leq S(\rho) \leq \log(n) \quad (3.8)$$

3.2 The von Neumann Entropy for qubit States

The application of the previous eq. (3.8) in the case of qubit states, $\rho \in \mathcal{D}(\mathbb{C}^2)$, yields:

$$0 \leq S(\rho) \leq 1 \quad (3.9)$$

while in the case of 2-qubit states, $\rho \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, it yields:

$$0 \leq S(\rho) \leq 2 \quad (3.10)$$

For a pure quantum state, it is obvious that the von Neumann entropy is equal to zero, as a pure state is a rank-1 projection operator, while for a completely mixed quantum state, it is again obvious that the von Neumann entropy is equal to its respective maximum value. These facts are in accordance with, and to be anticipated from, the probabilistic interpretations of completely mixed states, as uniform probabilistic mixtures, and of pure states, evidently as the degenerate cases of a probabilistic mixtures [2]. It is thus evident that the von Neumann entropy may also quantify the degree of the mixedness of a quantum state [3].

3.2.1 Product 2-qubit States

A product 2-qubit state, of the form of eq. (2.13), has a von Neumann entropy equal to the sum of the von Neumann entropies of the states of its subsystems; this can be straightforwardly proved considering the following statement, from standard operator theory:

$$\log(\rho^{(A)} \otimes \rho^{(B)}) = \log(\rho^{(A)}) \otimes I_{\mathbb{C}^2} + I_{\mathbb{C}^2} \otimes \log(\rho^{(B)})$$

which yields:

$$\begin{aligned} S(\rho^{(AB),\Pi}) &= -\text{Tr}((\rho^{(A)} \otimes \rho^{(B)})(\log(\rho^{(A)}) \otimes I_{\mathbb{C}^2} + I_{\mathbb{C}^2} \otimes \log(\rho^{(B)}))) \\ &= -\text{Tr}(\rho^{(B)})\text{Tr}(\rho^{(A)} \log(\rho^{(A)})) - \text{Tr}(\rho^{(A)})\text{Tr}(\rho^{(B)} \log(\rho^{(B)})) \end{aligned}$$

Thus:

$$S(\rho^{(AB),\Pi}) = S(\rho^{(A)}) + S(\rho^{(B)}) \quad (3.11)$$

The content of the above eq. (3.11) is simply the fact that, in a product 2-qubit state, the subsystems are independent, as, whenever two subsystems are independent, the average information content of the composite quantum system is equal to the sum of the average information content of each of its subsystems; this fact is in agreement with general intuition.

3.2.2 Separable and Entangled 2-qubit States

The above eq. (3.11), for the case of product 2-qubit states, cannot be straightforwardly generalised for the cases of either separable or entangled states. As the canonical example of 2-qubit entangled states, the specific case of Bell states is particularly illuminating for the precise information-theoretic interpretation of the von Neumann entropy. For a 2-qubit system in any of the four Bell states of Section 2.2.1, the von Neumann entropy is equal to zero, as they are pure states. Remarkably, this is not the case for the states of the its subsystems: Each of these states is a completely mixed state, and as such it has a von Neumann entropy equal to 1. The respective counterpart in classical information theory is impossible. This extraordinary fact suggests that, in general, the von Neumann entropy of the quantum state of a subsystem is not only a measure of the average information content of this quantum state as it is in itself; rather, it is also a measure of the entanglement of the quantum state of the composite quantum system, that is to say, of the quantum correlations between its subsystems [3].

3.3 The Conditional and the Relative Entropy for 2-qubit States

Various derived types of entropy, which are defined through the von Neumann entropy, are measures of the various aspects of the quantum entanglement of a quantum state of a quantum system; they are also central to many proofs of the essential mathematical properties of the von Neumann entropy.

3.3.1 The Conditional Entropy for 2-qubit States

As eq. (3.11) of the previous Section, for the case of product 2-qubit states, generally suggests, the von Neumann entropies of the reduced states may be related, through the von Neumann entropy of the quantum state of the 2-qubit system. Typically, in the context of classical information theory, the information about one random variable, under specific conditional information about another, possibly related, random variable, is quantified by the conditional entropy. The conditional entropy of classical information theory may be extended and generalised by its direct quantum counterpart, which is termed as the von Neumann *conditional entropy*. The conditional entropy is defined here for the reduced qubit states, $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$, of 2-qubit states, $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, as in the following:

$$S(\rho^{(A)}|\rho^{(B)}) := S(\rho^{(AB)}) - S(\rho^{(B)}) \quad (3.12)$$

and similarly, for the permutation of $(A \leftrightarrow B)$.

It is evident that in the case of product 2-qubit states, the conditional entropy for any of the reduced states coincides with its von Neumann entropy; this simply means that the subsystems of a product 2-qubit state are completely independent, in agreement with general intuition. This is not the case either for separable or for entangled 2-qubit states; however, it will be proved in the following Section, that the conditional entropy of a reduced state may serve as an indicator of the entanglement of its respective 2-qubit state. A preliminary illustration of the conditional entropy of a reduced state as an indicator of the entanglement of its respective 2-qubit state, can be given through the example of Bell states. Evidently, the conditional entropy of any reduced state of a Bell state is equal to -1 , demonstrating a fact with no respective counterpart in classical information theory, where the conditional entropy is non-negative. It feels natural, then, to expect that the negativity of the conditional entropy of a reduced state determines the entanglement of at least one of its extensions, namely, its respective 2-qubit state; this will be proved to be the case in the following Section.

3.3.2 The Relative Entropy for 2-qubit States

While the von Neumann entropy naturally expresses the average information content of quantum states, a comparison between two different quantum states is also possible. However, a mathematically adequate comparison would have to consider not only the measure of information contained in the two quantum states, but also the manner in which that information is distributed, which is essentially their statistical structure: Indeed, it is obvious that two distinct quantum states may possess exactly the same von Neumann entropy while having entirely different statistical structures. Thus, a simple difference of the von Neumann entropies of two quantum states is not a mathematically adequate comparison between them. Typically, in the context of classical information theory, a comparison between two probability distributions of the same random variable

is provided by the *Kullback - Leibler divergence* [2]. The Kullback - Leibler divergence of classical information theory may be extended and generalised by its direct quantum counterpart, which is termed as the von Neumann *relative entropy*. The relative entropy is defined here for two arbitrary qubit states, $\rho^{(1)}, \rho^{(2)}$, as in the following:

$$D(\rho^{(1)} || \rho^{(2)}) := S(\rho^{(1)}, \rho^{(2)}) - S(\rho^{(1)}) \quad (3.13)$$

where $S(\rho^{(1)}, \rho^{(2)})$ is called the *cross entropy*, and is defined as in the following:

$$S(\rho^{(1)}, \rho^{(2)}) := -Tr(\rho^{(1)} \log(\rho^{(2)})) \quad (3.14)$$

Similarly, the above eqs. (3.13) and (3.14) define respectively the relevant entropies for $(A \leftrightarrow B)$; it is straightforward to see that, in general:

$$D(\rho^{(1)} || \rho^{(2)}) \neq D(\rho^{(2)} || \rho^{(1)})$$

and:

$$S(\rho^{(1)}, \rho^{(2)}) \neq S(\rho^{(2)}, \rho^{(1)})$$

The relative entropies of two quantum states are equal to zero *iff* the states coincide; this will become evident in the following Section, and it is the essential property of the relative entropy, enabling it to serve as a mathematically adequate comparison between two quantum states. It is worth mentioning that, for the case of commuting density operators, the relative entropy reduces precisely to the Kullback - Leibler divergence; the relative entropy may therefore be regarded as the genuine direct extension and generalisation of the Kullback - Leibler divergence to, typically non-commuting, quantum states [2]. Unlike the von Neumann entropy, which is an intrinsic property of a quantum state, the relative entropy is a relational property of two quantum states. From a mathematical point of view, the relative entropies of two quantum states measure the extent of difference between these states. However, the asymmetry of the relative entropies of two quantum states is sufficient to demonstrate that the relative entropy cannot be interpreted as a distance between two quantum states; rather, it may be more accurately interpreted as the divergence between the quantum states relative to the approximation of one by the other, so that no symmetry is to be anticipated [4].

Logically, the relative entropy occupies a central position in QIT, because many of the essential mathematical properties of the von Neumann entropy follow directly from features of the relative entropy. Furthermore, in the following Chapter, the von Neumann mutual information will be expressed as the relative entropy between a 2-qubit state and the product state of its reduced states, providing directly an interpretation of mutual information as a measure of the total correlations between the subsystems of a composite quantum system.

3.4 Mathematical Properties of the von Neumann Entropy

3.4.1 The Subadditivity Theorems

Among the various relations satisfied by the von Neumann entropy, the Strong Subadditivity Theorem (SST) occupies a distinguished position. It is one of the deepest structural theorems of QIT, and underlies most of the mathematical properties of the von Neumann entropy [5]. The proof of the SST is highly nontrivial, relying on advanced methods from operator theory, and thus lies beyond the scope of the present Thesis; a complete proof of the SST may be found in [Nielsen, 6]. The SST for qubit states is presented below, similarly to its presentation in [5]:

The Strong Subadditivity Theorem (SST)

Consider an arbitrary 3-qubit state $\rho^{(ABC)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$. It holds that:

$$S(\rho^{(ABC)}) + S(\rho^{(B)}) \leq S(\rho^{(AB)}) + S(\rho^{(BC)}) \quad (3.15)$$

and similarly for permutations of (A, B, C) .

In terms of the conditional entropy, the SST states that:

$$S(\rho^{(A)}|\rho^{(BC)}) \leq S(\rho^{(A)}|\rho^{(B)}) \quad (3.16)$$

and similarly for permutations of (A, B, C) . The SST in the form of the above eq. (3.16) is transparent with respect to its interpretation: The content of the SST is simply the fact that any additional conditional information of a reduced state of a quantum system cannot decrease the conditional information content of another reduced state, that is to say, its conditional entropy; this fact is in agreement with general intuition. In other words, additional information about a subsystem of a quantum system can only increase, or, at worst, leave unchanged, the information regarding another subsystem of the quantum system. Although the SST itself will be assumed in the remainder of the Section, several important consequences may follow almost directly from it, the most basic of which is its weaker counterpart, termed as the Weak Subadditivity Theorem (WST):

The Weak Subadditivity Theorem (WST)

Consider an arbitrary 2-qubit state $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. It holds that:

$$S(\rho^{(AB)}) \leq S(\rho^{(A)}) + S(\rho^{(B)}) \quad (3.17)$$

Evidently, the WST is nothing but a special case of the SST, where, appropriately, one of the reduced qubit states is a pure state. The content of the WST is simply the fact that correlations between two subsystems increase the information content of the composite quantum system; this fact is, again, in agreement with general intuition. The equality case of the WST is simply eq. (3.11), which simply expresses the WST in the special case of a product 2-qubit state, where the two subsystems are independent. The WST thus demonstrates that the von Neumann entropy is not typically additive under composition; rather, its behaviour reflects the presence or absence of correlations between the subsystems of the composite quantum system.

3.4.2 Entanglement and the Conditional Entropy

The following theorem can now be proved:

Theorem I

The conditional entropy of the reduced states of an arbitrary separable 2-qubit state is non-negative.

Proof: Consider a set of, mutually orthogonal, rank-1 projection operators, $\{\Pi_n\}$, two subsets $\{\rho_n^{(A)}\}, \{\rho_n^{(B)}\} \subset \mathcal{D}(\mathbb{C}^2)$, and a 3-qubit separable state, $\rho^{(ABC)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)$, of the following form:

$$\rho^{(ABC)} = \sum_n p_n \rho_n^{(A)} \otimes \rho_n^{(B)} \otimes \Pi_n$$

Notice that the reduced 2-qubit state $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is a separable state, being directly expressed as a convex sum of product 2-qubit states, as in the following:

$$\rho^{(AB)} = \sum_n p_n \rho_n^{(A)} \otimes \rho_n^{(B)}$$

Considering the spectral decomposition of each of the qubit states $\rho_n^{(A)} \otimes \rho_n^{(B)} \otimes \Pi_n$:

$$\rho_n^{(A)} \otimes \rho_n^{(B)} \otimes \Pi_n = \sum_k \lambda_k^{(n)} \Pi_k^{(n)}$$

it holds that:

$$S(\rho^{(ABC)}) = - \sum_{n,k} p_n m_k^{(n)} \lambda_k^{(n)} \log(p_n \lambda_k^{(n)})$$

where $m_k^{(n)} := \text{rank}(\Pi_k^{(n)})$. Therefore:

$$\begin{aligned} S(\rho^{(ABC)}) &= - \sum_{n,k} p_n m_k^{(n)} \lambda_k^{(n)} \log(p_n) - \sum_{n,k} p_n m_k^{(n)} \lambda_k^{(n)} \log(\lambda_k^{(n)}) \\ &= - \sum_n p_n \log(p_n) + \sum_n p_n S(\rho_n^{(A)} \otimes \rho_n^{(B)} \otimes \Pi_n) \\ &= - \sum_n p_n \log(p_n) + \sum_n p_n S(\rho_n^{(A)}) + \sum_n p_n S(\rho_n^{(B)}) \end{aligned}$$

Similarly:

$$S(\rho^{(AC)}) = - \sum_n p_n \log(p_n) + \sum_n p_n S(\rho_n^{(A)})$$

and:

$$S(\rho^{(BC)}) = - \sum_n p_n \log(p_n) + \sum_n p_n S(\rho_n^{(B)})$$

Thus, the conditional entropy $S(\rho^{(A)}|\rho^{(BC)})$ satisfies the following:

$$S(\rho^{(A)}|\rho^{(BC)}) = \sum_k p_k S(\rho_k^{(A)}) \geq 0$$

due to the non-negativity of the von Neumann entropies $S(\rho_k^{(A)})$:

$$S(\rho_k^{(A)}) \geq 0$$

and eq. (3.16) of the SST yields straightforwardly the following, for the conditional entropy of the reduced states, of the separable, reduced qubit state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$:

$$S(\rho^{(A)}|\rho^{(B)}) \geq 0 \quad \blacksquare \quad (3.18)$$

Theorem I provides an important distinction between classical and quantum correlations. A separable 2-qubit state contains classical correlations between its qubits, and its reduced states always have a non-negative conditional entropy. As a direct consequence of Theorem I, only entangled 2-qubit states have reduced states of a negative conditional entropy; this means that the conditional entropy of reduced states determines the entanglement of the respective 2-qubit state, that is to say, the existence of quantum correlations between its qubits. Thus, the negativity of the conditional entropy of a reduced state determines the existence of quantum correlations between the respective qubit and the remainder of the qubit system. However, the negativity of the conditional entropy of a reduced state provides only a sufficient criterion for the entanglement of the respective 2-qubit state. The converse statement is not generally true: the negativity of the conditional entropy of a reduced state does not provide a necessary criterion for the entanglement of the respective 2-qubit state, as there exist entangled 2-qubit states with reduced states of non-negative conditional entropy. Consequently, the conditional entropy of a reduced state cannot serve as a complete characterisation of the entanglement of a 2-qubit state; rather, its negativity should be regarded as a particularly strong indicator of quantum correlations between the respective qubit and the remainder of the qubit system.

3.4.3 Distinguishability and the Relative Entropy

The essential property of the relative entropy of two quantum states, enabling it to serve as a mathematically adequate comparison between the two quantum states, can now be proved:

Theorem II

The relative entropy of two arbitrary qubit states is non-negative, and it vanishes *iff* the qubit states coincide.

Proof: Consider the following spectral decompositions of the arbitrary qubit states, $\rho^{(1)}, \rho^{(2)}$:

$$\rho^{(1)} = \sum_n \lambda_n^{(1)} \Pi_n^{(1)}$$

$$\rho^{(2)} = \sum_n \lambda_n^{(2)} \Pi_n^{(2)}$$

The relative entropy $D(\rho^{(1)} || \rho^{(2)})$ is:

$$\begin{aligned} D(\rho^{(1)} || \rho^{(2)}) &= S(\rho^{(1)}, \rho^{(2)}) - S(\rho^{(1)}) = Tr(\rho^{(1)} \log(\rho^{(1)})) - Tr(\rho^{(1)} \log(\rho^{(2)})) \\ &= \sum_n m_n^{(1)} \lambda_n^{(1)} \log(\lambda_n^{(1)}) - \sum_{n,k} Tr(\Pi_n^{(1)} \Pi_k^{(2)}) \lambda_n^{(1)} \log(\lambda_k^{(2)}) \end{aligned}$$

where $m_n^{(1)} := rank(\Pi_n^{(1)})$. Notice that:

$$\sum_k Tr(\Pi_n^{(1)} \Pi_k^{(2)}) = Tr(\Pi_n^{(1)} \sum_k \Pi_k^{(2)}) = Tr(\Pi_n^{(1)}) = m_n^{(1)}$$

Therefore:

$$D(\rho^{(1)}||\rho^{(2)}) = \sum_{n,k} \text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)})\lambda_n^{(1)} \log\left(\frac{\lambda_n^{(1)}}{\lambda_k^{(2)}}\right) = \sum_{n,k} \text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)})\lambda_n^{(1)} \log\left(\frac{\text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)})\lambda_n^{(1)}}{\text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)})\lambda_k^{(2)}}\right)$$

Denoting:

$$\alpha_{nk} := \text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)})\lambda_n^{(1)}$$

and:

$$\beta_{nk} := \text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)})\lambda_k^{(2)}$$

it holds that:

$$D(\rho^{(1)}||\rho^{(2)}) = \sum_{n,k} \alpha_{nk} \log\left(\frac{\alpha_{nk}}{\beta_{nk}}\right)$$

Then, as: $\forall x \in \mathbb{R} \quad (\log(x) \leq x - 1)$, it holds that:

$$D(\rho^{(1)}||\rho^{(2)}) \geq 0 \tag{3.19}$$

whereas $x = 1 \Leftrightarrow \log(x) = x - 1$ yields:

$$D(\rho^{(1)}||\rho^{(2)}) = 0 \Leftrightarrow \alpha_{nk} = \beta_{nk}$$

Moreover, it is the case that:

$$\alpha_{nk} = \beta_{nk} \Leftrightarrow (\lambda_n^{(1)} = \lambda_k^{(2)}) \vee (\text{Tr}(\Pi_n^{(1)}\Pi_k^{(2)}) = 0) \Leftrightarrow (\lambda_n^{(1)} = \lambda_k^{(2)}) \vee (\Pi_n^{(1)}\Pi_k^{(2)} = 0) \Leftrightarrow (\rho^{(1)} = \rho^{(2)})$$

as $\Pi_n^{(1)}, \Pi_k^{(2)}$ are, mutually orthogonal, projection operators. Thus:

$$D(\rho^{(1)}||\rho^{(2)}) = 0 \Leftrightarrow \rho^{(1)} = \rho^{(2)} \tag{3.20}$$

that is to say, the relative entropy of two arbitrary qubit states is non-negative, and it vanishes *iff* the qubit states coincide. ■

Theorem II is commonly attributed to Oskar Klein, and it is often termed as *Klein's Inequality* [5]. Theorem II establishes that the relative entropy of qubit states is always non-negative and vanishes only when the qubit states coincide. Consequently, it may be regarded as a measure of distinguishability, even though it cannot be interpreted as a distance between the qubit states.

3.4.4 Concavity of the von Neumann Entropy

The concavity property of the von Neumann entropy is a consequence of the WST, and it may be proved as in the following:

Theorem III

Every convex sum of arbitrary qubit states, $\sum_n p_n \rho_n$, satisfies the following:

$$S\left(\sum_n p_n \rho_n\right) \geq \sum_n p_n S(\rho_n) \tag{3.21}$$

Proof: Consider a separable qubit state, $\rho^{(AB),\Sigma}$, as in the following:

$$\rho^{(AB),\Sigma} = \sum_n p_n \rho_n^{(A)} \otimes \Pi_n$$

where Π_n are, mutually orthogonal, rank-1 projection operators. Considering the spectral decomposition of each of the qubit states $\rho_n^{(A)} \otimes \Pi_n$:

$$\rho_n^{(A)} \otimes \Pi_n = \sum_k \lambda_k^{(n)} \Pi_k^{(n)}$$

it holds that:

$$S(\rho^{(AB),\Sigma}) = - \sum_{n,k} p_n m_k^{(n)} \lambda_k^{(n)} \log(p_n \lambda_k^{(n)})$$

where $m_k^{(n)} := \text{rank}(\Pi_k^{(n)})$. Therefore:

$$\begin{aligned} S(\rho^{(AB),\Sigma}) &= - \sum_{n,k} p_n m_k^{(n)} \lambda_k^{(n)} \log(p_n) - \sum_{n,k} p_n m_k^{(n)} \lambda_k^{(n)} \log(\lambda_k^{(n)}) \\ &= - \sum_{n,k} p_n \log(p_n) + \sum_n p_n S(\rho_n^{(A)} \otimes \Pi_n) \\ &= - \sum_{n,k} p_n \log(p_n) + \sum_n p_n S(\rho_n^{(A)}) \end{aligned}$$

The reduced qubit states, $\rho^{(A)}$ and $\rho^{(B)}$, of the separable qubit state, $\rho^{(AB),\Sigma}$, are:

$$\rho^{(A)} = \sum_n p_n \rho_n^{(A)}$$

and:

$$\rho^{(B)} = \sum_n p_n \Pi_n$$

exhibiting, respectively, the von Neumann entropies:

$$S(\rho^{(A)}) = S(\sum_n p_n \rho_n^{(A)})$$

and:

$$S(\rho^{(B)}) = S(\sum_n p_n \Pi_n) = - \sum_n p_n \log(p_n)$$

Thus, the WST, for the separable qubit state, $\rho^{(AB),\Sigma}$, yields straightforwardly the following, for the reduced qubit state $\rho^{(A)}$:

$$\sum_n p_n S(\rho_n^{(A)}) \leq S(\sum_n p_n \rho_n^{(A)}) \quad \blacksquare \quad (3.22)$$

Theorem III on the concavity of the von Neumann entropy expresses the fact that a probabilistic mixture cannot have an average information content less than the average information content of its constituent states; that is to say, if a qubit state is prepared according to a probabilistic mixture, then the its average information content is at most as large as the average information content of the constituent qubit states of the probabilistic mixture.

Chapter 4

The von Neumann Mutual Information

The purpose of this Chapter is to introduce the von Neumann mutual information, as the quantum extension and generalisation of the mutual information of classical information theory, and to present its essential mathematical properties in quantum states of single qubit systems and of 2-qubit systems.

4.1 Definition of the von Neumann Mutual Information

In classical information theory, the mutual information between two random variables quantifies the amount of information that one random variable provides about the other. The quantum extension and generalisation of the mutual information of classical information theory is the *von Neumann mutual information*, which is the measure of the total correlations, both classical as well as due to quantum entanglement, between the subsystems of a composite quantum system, in a certain quantum state. Thus, the von Neumann mutual information is a central indicator of the statistical structure and the various statistical properties of quantum states; The von Neumann mutual information also plays a central role in the quantum measurement process [Zurek, Mutual Info, 6], a topic which, however, lies beyond the scope of the present Thesis. In the context of classical information theory, the mutual information between two random variables, X and Y , is defined as in the following:

$$I(X : Y) := \sum_{n,m} p_{nm}^{(XY)} \log\left(\frac{p_{nm}}{p_n^{(X)} p_m^{(Y)}}\right)$$

where:

$$\{p_{nm}^{(XY)}\}$$

is the joint probability distribution of the random variables X and Y , and:

$$p_n^{(X)} := \sum_m p_{nm}, \quad p_m^{(Y)} := \sum_n p_{nm}$$

are the marginal probability distributions of the random variables, X and Y , respectively. Evidently:

$$I(X : Y) = \sum_{n,m} p_{nm}^{(XY)} \log(p_{nm}^{(XY)}) - \sum_n p_n^{(X)} \log(p_n^{(X)}) - \sum_n p_n^{(Y)} \log(p_n^{(Y)})$$

The above form of the mutual information of classical information theory suggests a direct extension and generalisation to its QIT counterpart, the von Neumann mutual information; as it was the case

with the von Neumann entropy in the previous Chapter, the standard mathematical reflex is to try to express the von Neumann mutual information in a form that exhibits quantum states explicitly. To this end, consider the quantum state of a composite quantum system, $\rho^{(AB)} \in \mathcal{D}(\mathbb{X} \otimes \mathbb{Y})$, as in the following:

$$\rho^{(AB)} = \sum_{k,l=1}^{\dim(\mathbb{X})} \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{klmn}^{(AB)} E_{kl}^{(\mathbb{X})} \otimes E_{mn}^{(\mathbb{Y})}$$

where $E_{kl}^{(\mathbb{X})}$ and $E_{mn}^{(\mathbb{Y})}$ denote orthonormal bases of $\mathcal{L}(\mathbb{X})$ and $\mathcal{L}(\mathbb{Y})$, respectively. The reduced states, $\rho^{(A)} \in \mathcal{D}(\mathbb{X})$, and, $\rho^{(B)} \in \mathcal{D}(\mathbb{Y})$, are, respectively, the following:

$$\rho^{(A)} = \sum_{k,l=1}^{\dim(\mathbb{X})} P_{kl}^{(A)} E_{kl}^{(\mathbb{X})}$$

and:

$$\rho^{(B)} = \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{mn}^{(B)} E_{mn}^{(\mathbb{Y})}$$

where:

$$P_{kl}^{(A)} = \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{klmn}^{(AB)}$$

and:

$$P_{mn}^{(B)} = \sum_{k,l=1}^{\dim(\mathbb{X})} P_{klmn}^{(AB)}$$

The von Neumann mutual information defined by the probability distributions $\{P_{klmn}^{(AB)}\}$, $\{P_{kl}^{(A)}\}$, and $\{P_{mn}^{(B)}\}$ related, respectively, to the quantum state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{X} \otimes \mathbb{Y})$, and the reduced states $\rho^{(A)} \in \mathcal{D}(\mathbb{X})$ and $\rho^{(B)} \in \mathcal{D}(\mathbb{Y})$, is the following:

$$I(A : B) = \sum_{k,l=1}^{\dim(\mathbb{X})} \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{klmn}^{(AB)} \log(P_{klmn}^{(AB)}) - \sum_{k,l=1}^{\dim(\mathbb{X})} P_{kl}^{(A)} \log(P_{kl}^{(A)}) - \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{mn}^{(B)} \log(P_{mn}^{(B)})$$

It is evident that, the von Neumann entropies of the quantum state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{X} \otimes \mathbb{Y})$, and the reduced states $\rho^{(A)} \in \mathcal{D}(\mathbb{X})$ and $\rho^{(B)} \in \mathcal{D}(\mathbb{Y})$, are, respectively, the following:

$$S(\rho^{(AB)}) = - \sum_{k,l=1}^{\dim(\mathbb{X})} \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{klmn}^{(AB)} \log(P_{klmn}^{(AB)})$$

while:

$$S(\rho^{(A)}) = - \sum_{k,l=1}^{\dim(\mathbb{X})} P_{kl}^{(A)} \log(P_{kl}^{(A)})$$

and:

$$S(\rho^{(B)}) = - \sum_{m,n=1}^{\dim(\mathbb{Y})} P_{mn}^{(B)} \log(P_{mn}^{(B)})$$

Thus, the von Neumann mutual information of the reduced states $\rho^{(A)} \in \mathcal{D}(\mathbb{X})$ and $\rho^{(B)} \in \mathcal{D}(\mathbb{Y})$ of the quantum state $\rho^{(AB)} \in \mathcal{D}(\mathbb{X} \otimes \mathbb{Y})$, may be expressed as in the following:

$$I(\rho^{(A)} : \rho^{(B)}) = S(\rho^{(A)}) + S(\rho^{(B)}) - S(\rho^{(AB)}) \quad (4.1)$$

It is clear, from the difference in the above eq. (4.1), that the von Neumann mutual information quantifies the amount of information shared between the subsystems of a composite quantum system, in a certain quantum state, hence its characterisation as the mutual information. An alternative interpretation follows immediately from the relation of the mutual information to the conditional entropy. It is evident that:

$$I(\rho^{(A)} : \rho^{(B)}) = S(\rho^{(A)}) - S(\rho^{(A)}|\rho^{(B)}) = S(\rho^{(B)}) - S(\rho^{(B)}|\rho^{(A)}) \quad (4.2)$$

The difference in the above eq. (4.2) demonstrates clearly that the mutual information quantifies the increase in the information about a subsystem, that may result from conditional information about the remainder of the composite quantum system.

4.1.1 The Sign of the von Neumann Mutual Information

The interpretation of the mutual information demonstrated by eq. (4.2) anticipates that the mutual information is non-negative; this fact can be easily proved, considering the WST and eq. (4.1). Thus, obviously, for the reduced states, $\rho^{(A)} \in \mathcal{D}(\mathbb{X})$, and, $\rho^{(B)} \in \mathcal{D}(\mathbb{Y})$, of an arbitrary quantum state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{X} \otimes \mathbb{Y})$, it is the case that:

$$I(\rho^{(A)} : \rho^{(B)}) \geq 0 \quad (4.3)$$

It is evident that if the quantum state $\rho^{(AB)} \in \mathcal{D}(\mathbb{X} \otimes \mathbb{Y})$ is a product state of its reduced states, $\rho^{(A)} \in \mathcal{D}(\mathbb{X})$, and, $\rho^{(B)} \in \mathcal{D}(\mathbb{Y})$, the mutual information vanishes; in the following section, it will be proved that the converse is also true.

4.2 Mathematical Properties of the von Neumann Mutual Information

4.2.1 The Symmetry of the von Neumann Mutual Information

The mutual information is symmetric under the permutation of $(A \leftrightarrow B)$:

$$I(\rho^{(A)} : \rho^{(B)}) = I(\rho^{(B)} : \rho^{(A)}) \quad (4.4)$$

as it is evident, from both eqs. (4.1) and (4.2).

4.2.2 The Relation between the von Neumann Mutual Information and the von Neumann Relative Entropy

The relation between the mutual information and the relative entropy is particularly interesting in that it provides an interpretation of the mutual information of two reduced states as a measure of the total correlations, both classical as well as due to quantum entanglement, between the respective subsystems of a composite quantum system, in a certain quantum state. Accordingly, the following theorem can be proved:

Theorem IV

For an arbitrary 2-qubit state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, it is the case that:

$$I(\rho^{(A)} : \rho^{(B)}) = D(\rho^{(AB)} || \rho^{(A)} \otimes \rho^{(B)}) \quad (4.5)$$

Proof: From the definitions of the relative entropy and the cross entropy, of eqs. (3.13) and (3.14), respectively, it holds that:

$$\begin{aligned} D(\rho^{(AB)} || \rho^{(A)} \otimes \rho^{(B)}) &= S(\rho^{(AB)}, \rho^{(A)} \otimes \rho^{(B)}) - S(\rho^{(AB)}) \\ &= -Tr(\rho^{(AB)} \log(\rho^{(A)} \otimes \rho^{(B)})) + Tr(\rho^{(AB)} \log(\rho^{(AB)})) \end{aligned}$$

Considering the spectral decompositions of $\rho^{(A)}$ and $\rho^{(B)}$ directly yields the following:

$$\log(\rho^{(A)} \otimes \rho^{(B)}) = \log(\rho^{(A)}) \otimes I_{\mathbb{C}^2} + I_{\mathbb{C}^2} \otimes \log(\rho^{(B)})$$

Therefore:

$$\begin{aligned} D(\rho^{(AB)} || \rho^{(A)} \otimes \rho^{(B)}) &= -Tr(\rho^{(AB)} (\log(\rho^{(A)}) \otimes I_{\mathbb{C}^2} + I_{\mathbb{C}^2} \otimes \log(\rho^{(B)}))) + Tr(\rho^{(AB)} \log(\rho^{(AB)})) \\ &= -Tr(\rho^{(AB)} (\log(\rho^{(A)}) \otimes I_{\mathbb{C}^2})) - Tr(\rho^{(AB)} (I_{\mathbb{C}^2} \otimes \log(\rho^{(B)}))) + Tr(\rho^{(AB)} \log(\rho^{(AB)})) \\ &= -Tr(\rho^{(A)} \log(\rho^{(A)})) - Tr(\rho^{(B)} \log(\rho^{(B)})) + Tr(\rho^{(AB)} \log(\rho^{(AB)})) \\ &= S(\rho^{(A)}) + S(\rho^{(B)}) - S(\rho^{(AB)}) \end{aligned}$$

Thus, from the definition of the mutual information, of eq. (4.1), it holds that:

$$D(\rho^{(AB)} || \rho^{(A)} \otimes \rho^{(B)}) = I(\rho^{(A)} : \rho^{(B)}) \quad \blacksquare \quad (4.6)$$

Theorem IV demonstrates that, as the relative entropy measures the distinguishability between two quantum states, the mutual information of two reduced states is a measure of difference between the quantum state of the composite quantum system and the product state of these reduced states; since, in a product state, the respective subsystems are independent, this difference is precisely the total correlations, both classical as well as due to quantum entanglement, between the respective subsystems of the composite quantum system, in that certain quantum state. Therefore, as the mutual information of two reduced states vanishes only in the case of total absence of correlations between the respective subsystems of a composite quantum system, in a certain quantum state, Theorem IV essentially anticipates the fact that the mutual information of two reduced states vanishes *iff* the quantum state of the composite quantum system is a product state of these reduced states, that is to say, if the respective subsystems are independent, so that there is a total absence of correlations between the respective subsystems of the composite quantum system, in that certain quantum state. Thus, the below Corollary naturally follows from Theorem IV:

Corollary

The von Neumann mutual information of the two reduced qubit states, $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$, of an arbitrary 2-qubit state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, vanishes *iff* $\rho^{(AB)} = \rho^{(A)} \otimes \rho^{(B)}$.

Proof: Theorem IV along with Theorem II directly yield the above Corollary. ■

It has been established, then, that the mutual information of two reduced states is always non-negative and vanishes precisely when the respective subsystems are independent. Additionally, the above Corollary, along with the definition of the mutual information, of eq. (4.1), straightforwardly expand the WST, as in the following:

The Expanded Weak Subadditivity Theorem (EWST)

Consider an arbitrary 2-qubit state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. It holds that:

$$S(\rho^{(AB)}) \leq S(\rho^{(A)}) + S(\rho^{(B)}) \quad (4.7)$$

while it is also the case that:

$$S(\rho^{(AB)}) = S(\rho^{(A)}) + S(\rho^{(B)}) \Leftrightarrow \rho^{(AB)} = \rho^{(A)} \otimes \rho^{(B)} \quad (4.8)$$

4.3 The von Neumann Mutual Information for typical qubit States

While the essential mathematical properties of the mutual information have been established, the identification of the mutual information as a measure of the total correlations in a quantum state, due to the fact that correlations arise precisely by deviations from statistical independence, motivates the calculation of the mutual information for representative classes of qubit states.

4.3.1 Product 2-qubit states

In a product 2-qubit state, the subsystems are independent; it has been established, in the previous Section, that the mutual information of two reduced states is always non-negative and vanishes precisely when the respective subsystems are independent.

4.3.2 Separable 2-qubit States

A distinctive example of a separable 2-qubit state, $\rho^{(AB),\Sigma} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is the following:

$$\rho^{(AB),\Sigma} = \frac{1}{2}(E_{11} \otimes E_{11} + E_{22} \otimes E_{22})$$

which, evidently, exhibits *perfect* classical correlations between its qubits, as it is a uniform probabilistic mixture of the two product states, $E_{11} \otimes E_{11}, E_{22} \otimes E_{22} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. The von Neumann entropy of the separable 2-qubit state, $\rho^{(AB),\Sigma} \in \mathcal{D}(\mathbb{C}^2)$, is:

$$S(\rho^{(AB)}) = -2 \frac{1}{2} \log\left(\frac{1}{2}\right) = \log(2) = 1$$

The reduced qubit states, $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$, of the separable 2-qubit state, $\rho^{(AB),\Sigma} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, are the following:

$$\rho^{(A)} = \rho^{(B)} = \frac{1}{2}(E_{11} + E_{22})$$

and their von Neumann entropies are:

$$S(\rho^{(A)}) = S(\rho^{(B)}) = -2\frac{1}{2}\log\left(\frac{1}{2}\right) = \log(2) = 1$$

Thus, the mutual information of the reduced states, $\rho^{(A)}, \rho^{(B)} \in \mathcal{D}(\mathbb{C}^2)$, of the separable 2-qubit state, $\rho^{(AB),\Sigma} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, is the following:

$$I(\rho^{(A)} : \rho^{(B)}) = S(\rho^{(A)}) + S(\rho^{(B)}) - S(\rho^{(AB)}) = 1 + 1 - 1 = 1$$

It is obvious, from the above, that the mutual information of the reduced qubit states is positive, despite the absence of entanglement in the 2-qubit state; this fact is consistent with the provided interpretation of the mutual information as a measure of the total correlations in a quantum state.

4.3.3 Entangled 2-qubit States: The canonical example of the Bell States

The canonical example of entangled 2-qubit states, that is to say, the Bell states, illustrates the importance of the mutual information, as the mutual information is a measure of the total correlations in a quantum state. Consider, without loss of generality, the following Bell state, from eq. (2.15):

$$\phi^{(AB),+} = \frac{1}{2}(E_{11} \otimes E_{11} + E_{11} \otimes E_{22} + E_{22} \otimes E_{11} + E_{22} \otimes E_{22})$$

Since the Bell state $\phi^{(AB),+}$ is a pure state, its von Neumann entropy vanishes, that is to say:

$$S(\phi^{(AB),+}) = 0$$

However, the reduced states, $\phi^{(A),+}$ and $\phi^{(B),+}$, of the Bell state, $\phi^{(AB),+}$, are the following completely mixed states:

$$\phi^{(A),+} = \phi^{(B),+} = \frac{1}{2}I_{\mathbb{C}^2}$$

with von Neumann entropies:

$$S(\phi^{(A),+}) = S(\phi^{(B),+}) = -\log\left(\frac{1}{2}\right) = \log(2) = 1$$

Thus, the mutual information of the reduced states, $\phi^{(A),+}$ and $\phi^{(B),+}$, of the Bell state $\phi^{(AB),+}$, is the following:

$$I(\phi^{(A),+} : \phi^{(B),+}) = S(\phi^{(A),+}) + S(\phi^{(B),+}) - S(\phi^{(AB),+}) = 1 + 1 - 0 = 2$$

It can be straightforwardly proved that the mutual information of the reduced states of any of the Bell states is the same.

A comparison between a separable 2-qubit state and the Bell state reveals that, in both cases, the reduced states possess a positive mutual information; however, the origin of the correlations

between their respective subsystems is fundamentally different: In the former case, the correlations are entirely classical, while, in the latter case, the correlations are due to quantum entanglement as well. Evidently, since the mutual information of the reduced states is positive in both cases, these examples demonstrate that it is a measure of the total correlations in a quantum state, without distinguishing between classical and quantum correlations.

It is worth noting that, the mutual information of the reduced qubit states of a 2-qubit system, while always being non-negative, also possesses an upper bound: the definition of the mutual information, of eq. (4.1), combined with the eqs. (3.9) and (3.10), for the range of the von Neumann entropy in single qubit systems, and 2-qubit systems, respectively, exhibit that the mutual information of the reduced qubit states of a 2-qubit system is never greater than 2; this seems a fact worthy of its own Theorem:

Theorem V

For an arbitrary 2-qubit state, $\rho^{(AB)} \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, it is the case that:

$$0 \leq I(\rho^{(A)} : \rho^{(B)}) \leq 2 \quad (4.9)$$

Proof: Eq. (4.3), along with the definition of the mutual information, of eq. (4.1), combined with eqs. (3.9) and (3.10), directly yield the above Theorem V. ■

Theorem V highlights the particularity of the Bell states, as the canonical example of entangled 2-qubit states: The mutual information of the reduced states of any of the Bell states is the maximum possible mutual information related to a 2-qubit system; consequently, the Bell states are regarded as specific cases of *maximally correlated* or *maximally entangled states*. While the reduced states of any of the Bell states saturate the upper bound of eq. (4.9), of Theorem V, the reduced states of any product 2-qubit state saturate the lower bound of eq. (4.9), as per the Corollary of Section 4.2; consequently, and in accordance with general wisdom, product 2-qubit states exhibit no correlations between their qubits.

Chapter 5

Conclusions and Future Perspectives

The main purpose of this Thesis has been to provide a clear, concise, and relatively independent, presentation of the von Neumann entropy and mutual information in qubit systems. Beginning from the mathematical framework of QIT, the presentation has developed progressively towards the von Neumann mutual information, which provides a quantitative description of the total correlations between the subsystems of a composite quantum system. The mathematical framework of QIT, that was introduced in Chapter 2, established the concepts required throughout the remainder of the Thesis. The language of density operators was presented as the general language of quantum states, accommodating both pure and mixed states within a common mathematical formalism; restricting consideration to qubit systems allowed for the rigorous development of the mathematical framework, while avoiding technical complications, favouring conceptual clarity over computational prowess. Chapter 3 introduced the principal entropic quantities of QIT: The von Neumann entropy was motivated as the natural extension and generalisation of the Shannon entropy of classical information theory to quantum states through their spectral decompositions; its essential mathematical properties, including subadditivity and concavity, were proved, illuminating the behaviour of quantum information in quantum systems. The subsequent study of the conditional entropy and the relative entropy provided a strong indicator of quantum entanglement, and a quantitative measure of the distinguishability between quantum states, respectively. The developments of Chapter 3 naturally led to the introduction of the von Neumann mutual information, in Chapter 4. Expressed equivalently in terms of the von Neumann entropy, the conditional entropy, and the relative entropy, the mutual information was presented as the unifying aspect it is indeed, relating the entropic quantities considered throughout the Thesis; its interpretation as the relative entropy of a quantum state and the product state of its reduced states, demonstrated that the mutual information provides a measure of the total correlations between two quantum subsystems of a quantum system, encompassing both classical correlations as well as correlations due to quantum entanglement. The examples examined in the Chapter 4 further highlighted that the mutual information may determine qualitatively different classes of quantum states, with respect to the correlations they exhibit.

Future Perspectives

Although the present Thesis has focused primarily on the mathematical development of essential concepts of QIT, these concepts constitute the foundation of several important areas of contemporary research in QIT. Specifically, the von Neumann mutual information has central role in modern approaches to the quantum theory of measurement. In general, QIT-approaches to the quantum

theory of measurement describe quantum measurement as the establishment and evolution of correlations between a quantum system and a measuring apparatus of quantum origins; within these approaches to the quantum theory of measurement, the mutual information provides a quantitative measure of the information transferred during the measurement interaction. In particular, a largely influential development along the lines of QIT-approaches to the quantum theory of measurement is the formulation of quantum measurement developed by W. H. Zurek [6, 7, 8, 9]; in this approach, the mutual information becomes the fundamental quantity describing how information about a quantum system is distributed between the quantum system, the measuring apparatus, and, subsequently, the surrounding environment. Zurek's perspective naturally evolves the basis of decoherence theory to quantum Darwinism, in which the emergence of effectively classical behaviour is understood through the proliferation of stable, and redundantly accessible, correlations [8, 9]. Although these topics lie beyond the scope of the present Thesis, the mathematical framework developed in this Thesis provides essential prerequisites for their rigorous study.

As a conclusion, the progression of the QIT concepts contained in this Thesis highlights the internal coherence of QIT, as well as the central role played by information in the mathematical description of quantum systems. It is the hope of the author that the present exposition will provide part of a useful foundation for further study of QIT, and its applications to the quantum theory of measurement, and to the broader field of the foundations of quantum theory.

References

- [1] Niiniluoto, I. (1999), *Critical Scientific Realism*, Oxford University Press.
- [2] Watrous, J. (2018), *The Theory of Quantum Information*, Cambridge University Press.
- [3] Holevo, A. S. (2001), *Statistical Structure of Quantum Theory*, Springer - Verlag.
- [4] Kullback, S.; Leibler, R.A. (1951), 'On information and sufficiency', *Annals of Mathematical Statistics*, vol. 22, no. 1, pp. 7986.
- [5] Palazuelos, C. (2013), *Introduction to Quantum Information Theory*, ICMAT.
- [6] Zurek, W. H. (1981), 'Pointer basis of quantum apparatus: Into what mixture does the wave packet collapse?', *Physical Review D*, vol. 24, no. 6, pp. 1516 - 1525.
- [7] Zurek, W. H. (1982), 'Environment-induced superselection rules', *Physical Review D*, vol. 26, no. 8, pp. 1862.
- [8] Zurek, W. H. (2003), 'Decoherence, einselection, and the quantum origins of the classical', *Reviews of Modern Physics*, vol. 75, no. 3, pp. 715 - 775.
- [9] Zurek, W. H. (2009), 'Quantum Darwinism', *Nature Physics*, vol. 5, pp. 181 - 188.