On the Relation between Quantum Discord and Purified Entanglement

by

Eric Webster

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Applied Mathematics - Quantum Information

Waterloo, Ontario, Canada, 2013

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis, I study bipartite discord between A and B in terms of the structure formed by the bipartite and tripartite entanglement found in the purified system ABC. I find that discord manifests itself only when there is both tripartite and bipartite entanglement present in the purification. This allows one to understand the asymmetry of quantum discord, $D(A|B) \neq D(B|A)$ in terms of entanglement monogamy. For the cases where AB has rank two and for two-mode Gaussian states, I find that discord also necessarily appears whenever there is tripartite and bipartite entanglement in ABC. As a result of this, some light is shed on a counter-intuitive property of Gaussian states: the presence of classical correlations necessarily requires the presence of quantum discord. Finally, these results are found to be closely linked to the protocol for remote activation of entanglement by a third party.

Acknowledgements

First of all, I want to thank my supervisor Prof. Achim Kempf for taking me into his great group of students and for answering all of my silly questions. Also, I would like to thank him for being so good at conjuring up ideas, which would motivate me to sit down and try to work them out. I would like to thank my collaborators Eric Brown and Eduardo Martín-Martínez for their hard work. I want to thank those with whom I shared the Kempf lab with, and the rest of the friends I've made over here in Waterloo.

Table of Contents

List of Figures

Chapter 1

Introduction

Quantum information science has as its final goal the successful creation of a *quantum computer*. Ever since the discovery of an algorithm by Shor [7] which would factorize numbers efficiently on a quantum computer, there have been spectacular advances in building such a computer. The resource which Shor's algorithm depends on is the so-called *quantum entanglement*. This is the resource believed by most to allow such quantum speedups and advantages. This can be seen through the fact that unentangled pure states require only a polynomial (in the number of subsystems) amount of parameters to completely describe them while an entangled state requires an exponential number of parameters. Therefore, a quantum computer can do things a classical computer would find hard to simulate.

Building a quantum computer using pure states is difficult. There are already many successful implementations of pure state algorithms such as Shor's in the laboratory. These are limited however by their lack of scalability. As the quantum computer grows, there are more ways for it to couple to the environment, thus losing the purity of the states. This is called *decoherence* [2].

Another approach to quantum computing would be to use *mixed states*. The first mixed-state scheme for quantum computation was proposed by E. Knill and R. Laflamme in 1998 and is called $DQC1$ [25], which is short for Deterministic Quantum Computation with 1 pure qubit. This model has been shown to contain very little, if any, entanglement and instead contains *quantum discord*. In addition to playing a role in mixed state computation, discord has been found to be useful in a range of applications, discussed in Chapter 3. We wish here to gain an understanding of discord in terms of entanglement. This is motivated by the fact

that discord is equivalent to entanglement in the case of pure states. It is natural then to wonder how the two are related in the case of mixed states. We make use of the fact that every mixed state can be *purified* into a pure state of a larger system and propose to view discord as a manifestation of entanglement inside this purification.

This thesis is organized as follows. In Section 1.1 we provide a quick review of some important concepts in quantum information such as *projective measurements*, *POVMs* and general *quantum operations*. All of the material presented here may be found in more detail in the wonderful introductory book by Michael Nielsen and Isaac Chuang [1]. In Section 1.2 we define the notion of a qubit and what a *quantum gate* is along with other important quantum computing terms. We show how a qubit may be represented as a point in or on a sphere, depending on the *purity* of the qubit. Chapter 2 is devoted to quantum correlations based on non-locality such as ones defined through the *Bell inequalities* and, as the title of this section suggests, quantum entanglement. In Section 2.4, we give an axiomatic definition of quantum entanglement which arises out of the concept of *LOCC operations*, defined in Section 2.3. In Chapter 3 we introduce the quantum discord between two systems through ideas originally conceived in classical information theory (Section 3.1) and adapted to the quantum formalism. Section 3.3 discusses the uses which have been found for quantum discord recently. In there we show how the model for mixed state quantum computation $DQC1$ seems to make use of quantum discord, instead of entanglement, to provide a quantum advantage. Finally, in Chapter 4 we discuss relating discord and entanglement. Section 4.1 it is shown that, in the case of pure states, discord is exactly the same as entanglement. Discord in mixed states is not well understood except for some specific classes of states. Section 4.2 discusses the class of *Bell-state mixtures*. In Section 4.3 is where our work begins. We relate discord between two unentangled subsystems A and B to the different entanglements found in the purification ABC. First, we explore this in the case where A, B and C are qubits, then move on to the more general case where the AB system is simply rank two. We find that the results for rank two systems AB do not exactly carry over to the completely general case which is explored in Section 4.4. Following this, some applications of our results are discussed.

1.1 Quantum framework

In classical mechanics, the state of a system is always be well-defined in the sense that we can associate a set of numbers which completely describe it (or as much as we care for) at any moment in time. For example, a wheel falling from the top of a building could be described by the speed it is falling, how fast it is spinning and its diameter. When we deal with small *quantum* objects, this description is no longer valid. We find that, to completely describe a quantum system, we must allow that it may be in a *superposition* of possible states at any moment in time. Formally, a quantum mechanical state is given by

$$|\psi\rangle = \sum_k \alpha_k |\psi_k\rangle$$

where α_k are complex numbers which represents the *probability amplitude* with which the system is in the basis state $|\psi_k\rangle$. For example, these could be the energy levels of an atom or the spin of a photon. When we make a measurement on the system, however, the state *collapses* to one of its basis states $|\psi_k\rangle$ with probability $|\alpha_k|^2$ and will remain in that state if left undisturbed. The amplitudes must satisfy

$$\sum_k |\alpha_k|^2 = 1$$

for the probability distribution upon measurement to make sense. We say the state is *normalized*. These states can equivalently be represented in a column vector form as

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ . \end{bmatrix}$$

The set of all vectors $|\psi\rangle$ along with the inner product between them form what we call a *Hilbert space*, which we denote by $\mathcal{H}$. Only the vectors which are normalized correspond to physical states. Usually we choose basis states $|\psi_k\rangle$ which are *orthonormal*, which means they are *orthogonal* in addition to being normalized. The normalization condition can then be written more succinctly as

$$\langle\psi|\psi\rangle = 1$$

where $\langle x|y\rangle$ is the *inner product* between $|x\rangle$ and $|y\rangle$. It is also possible to take the *tensor product* between two states of systems A and B: $|\psi_A\rangle \otimes |\psi_B\rangle$. This represents looking at the state of the combined system AB as a whole inside the enlarged Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

1.1.1 Unitary evolution

Whenever a system is *closed*, its state evolves via a linear function U on its state vector. Mathematically this means that, after evolution by U, it will be in the state

$$|\psi'\rangle = U\,|\psi\rangle$$

The normalization condition requires that $\langle\psi'|\psi'\rangle = 1$ so that we have

$$\langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = 1 \implies U^\dagger U = I$$

The function U is therefore *unitary* and we say that a closed system undergoes unitary evolution. Since a unitary has an inverse, $U^{-1} = U^\dagger$, the evolution of a closed system is reversible.

1.1.2 Open systems

In general, our quantum system may not be closed (and is instead *open*) and therefore we may not have complete knowledge about it at any point in time. This also means a system undergoes an evolution which is not unitary. We can, however, always enlarge our system's Hilbert space to include its environment, the total of the two being a closed system and thus evolving unitarily. The *density operator* or *density matrix* associated with the initial state of the system plus environment can be written as, without loss of generality, the Kronecker product composition of the density operator for the system with that for the environment

$$\rho \otimes \rho_{env}$$

and acts on the enlarged Hilbert space $\mathcal{H} \otimes \mathcal{H}_{env}$. The density matrix can be used as an alternative to the vector representation of the state. It captures all relevant information about the state of the system and is also used to describe

open systems where vectors fail. Any density matrix ρ may be written as a *convex combination* of orthogonal, *pure* density matrices

$$\rho = \sum_k p_k \left|\psi_k\right\rangle \left\langle\psi_k\right|$$

where $\sum_k p_k = Tr(\rho) \equiv \sum_k \left\langle\psi_k\right| \rho \left|\psi_k\right\rangle = 1$. Each $\left|\psi_k\right\rangle \left\langle\psi_k\right|$ is also called a rank-one *projection operator*, due to the fact that it projects a vector $|\phi\rangle$ onto the subspace spanned by $|\psi_k\rangle$. The density matrix can be viewed as a *mixture*, containing a fraction p_k of the pure state $|\psi_k\rangle$. If all but one of the p_k are 0 then ρ is pure and we have complete information about the system it describes, otherwise is it said to be *mixed* and we lack information about the system. Our original state can be written by taking the *partial trace* over the environment $\mathcal{H}_{env}$

$$Tr_{env}(\rho \otimes \rho_{env}) = \rho \otimes Tr(\rho_{env}) = \rho.$$

With this we can describe the evolution of the state ρ of an open system

$$\rho' = Tr_{env}(U(\rho \otimes \rho_{env})U^\dagger)$$

where U is a unitary operator acting on $\mathcal{H} \otimes \mathcal{H}_{env}$.

1.1.3 Projective measurements

The Hilbert space in quantum mechanics is analogous to the phase space in classical mechanics. In both cases, the state of a system is completely described by a vector in that space. What differs are the physical quantities we want to measure, the observables, which are described by quantum mechanics as operators acting on the Hilbert space $\mathcal{H}$. Every state can be written as a sum of rank-one projection operators which are orthogonal to one another

$$\rho = \sum_k p_k \left|\psi_k\right\rangle \left\langle\psi_k\right|,$$

i.e. it has an *eigendecomposition*, and, similarly, so can an observable

$$A = \sum_m a_m \left|a_m\right\rangle \left\langle a_m\right|$$

where the a_m are the eigenvalues of the operator A and represent the values of the outcomes of a measurement: the result of a *projective measurement* of an

observable A for a system in state ρ will be one of the eigenvalues a_m of A and will be obtained with probability

$$p_m = \langle a_m | \rho | a_m \rangle = Tr(|a_m\rangle \langle a_m| \rho).$$

After the measurement, the system will collapse to the state of the projection operator $|a_m\rangle \langle a_m|$ associated with the outcome a_m and therefore, if the system is left undisturbed, returns the same outcome when performing the measurement again. This is called the von Neumann *projection postulate*. The *expectation* or average value of a projective measurement is given by

$$\langle A \rangle = \sum_m a_m p_m = Tr\left(\sum_m a_m |a_m\rangle \langle a_m| \rho\right) = Tr\left(A\rho\right) \tag{1.1}$$

To shorten notation, a projective measurement is usually denoted by $\{\Pi_m\}$, where the Π_m are rank-one projection operators. It is also possible to perform a projective measurement $\{\Pi_A^m\}$ on only a subsystem A of a larger system AB. The probability of the outcome m is then given by

$$p_m = Tr[(\Pi_A^m \otimes I_B)\rho_{AB}].$$

The state of A after measuring outcome m is Π_A^m and the state on B is given by the partial trace over the subsystem being measured

$$\rho_{B|A=m} = Tr_A[(\Pi_A^m \otimes I_B)\rho_{AB}]/p_m.$$

The factor of $\frac{1}{p_m}$ is there to normalize the right hand side.

The result of a projective measurement is always a pure state. That means after we perform a projective measurement on a subsystem A of a larger system AB which is in a pure state, the B system will be left in a pure state as well. This can be seen by arguing that, through the process of measuring A, we certainly don't lose any information and so we must still have perfect information about AB.

1.1.4 Positive Operator Valued Measurements

Projective measurements do not cover all the measurements we might be able to do. For example, we might let the system evolve unitarily before making our

measurement, or even non-unitarily as an open system. To capture this, we say a measurement consists of a set of operators $\{M_m\}$ acting on $\mathcal{H}$. The probability of measuring outcome m on state ρ is given by

$$p_m = Tr(M_m \rho M_m^\dagger)$$

and after the measurement the state collapses to

$$M_m \rho M_m^\dagger / p_m$$

The measurement operators must satisfy the completeness relation in order for the probabilities p_m to sum to 1

$$\sum_m M_m^\dagger M_m = I.$$

If $\langle M \rangle$ represents the expectation value of the measurement $\{M_m\}$, then

$$\langle M \rangle = \sum_m m p_m = Tr\left(\sum_m m M_m M_m^\dagger \rho\right) = Tr\left(M\rho\right) \tag{1.2}$$

where we have simply set $M = \sum_m m M_m M_m^\dagger$ which is the observable associated with the measurement $\{M_m\}$. This sum becomes an integral when our set of measurements is not discrete, for example measuring the momentum of a particle. In the case of such a general measurement, the von Neumann projection postulate no longer necessarily holds.

In a lot of the cases dealt with in physics, only the probabilities of the outcomes are necessary to know and not the final state of the system. So to make notation more compact we define something called a *positive operator-valued measurement* (POVM) which is simply defined as a set $\{E_m\}$ of POVM elements where $\sum_m E_m = I$. What *positive operator* means is that the eigenvalues of the operator are non-negative numbers. A positive operator O_p also has the property that

$$\langle \psi | O_p | \psi \rangle \geq 0. \tag{1.3}$$

for all vectors $|\psi\rangle$ in the Hilbert space. This simply guarantees that the probabilities associated with the outcomes m, $p_m = Tr(E_m \rho)$, are also non-negative numbers.

In general it is always possible to factorize a POVM element as $E_m = M_m^\dagger M_m$, which might lead one to believe that we can determine the state of the system after measuring outcome m via $M_m \rho M_m^\dagger / p_m$, but their factorization is not unique so this is not possible. It is, however, possible to rule out certain final states $M_m \rho M_m^\dagger / p_m$ by checking if $E_m \neq M_m^\dagger M_m$. The expected value of a POVM $\{E_m\}$ is given by $Tr(E\rho)$ where $E = \sum_m m E_m$. It is always possible to view a POVM on $\mathcal{H}$ as a projective measurement of an observable $A = \sum_m a_m |a_m\rangle \langle a_m|$ in a larger Hilbert space $\mathcal{H} \otimes \mathcal{H}_{env}$ so that $p_m = Tr(E_m \rho) = Tr(|a_m\rangle \langle a_m| \rho \otimes \rho_{env})$, this is called the *Stinespring dilation*. Each E_m can be diagonalized and the number of non-zero eigenvalues gives the *rank* of the POVM element. Rank-one POVMs are of special interest and are defined as POVMs with only rank-one elements. These elements are proportional to rank-one projection operators and are not necessarily orthogonal to one another.

1.1.5 Quantum operations

We can go even further than measurements and define what a quantum operation is in general. Here we take the axiomatic approach:

Definition A quantum operation is any physical process that takes a state ρ of a system on $\mathcal{H}_1$ to a state ρ' on $\mathcal{H}_2$. This process is described by a map $\mathcal{E} : \mathcal{H}_1 \to \mathcal{H}_2$

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

The process is said to be physical if it satisfies the following three axioms [1]

1. $Tr(\mathcal{E}(\rho))$ is the probability that the process represented by $\mathcal{E}$ occurs. Therefore, $0 \leq Tr(\mathcal{E}(\rho)) \leq 1$ for any state ρ.

2. $\mathcal{E}$ is a *convex-linear map* on the set of density operators

$$\mathcal{E}\left(\sum_k p_k \rho_k\right) = \sum_k p_k \mathcal{E}(\rho_k)$$

   for probabilities $\{p_k\}$.

3. $\mathcal{E}$ is a *completely positive map*. This means $\mathcal{E}(A)$ must be a positive operator over $\mathcal{H}_2$ for any positive operator A over $\mathcal{H}_1$. Furthermore, $(I_R \otimes \mathcal{E})(A)$

must be positive for any positive operator A on any combined Hilbert space $\mathcal{H}_R \otimes \mathcal{H}_1$. I_R is the identity operation over $\mathcal{H}_R$.

There are a lot of words in those axioms, but the physical intuition might not be clear. The first axiom is pretty clear, since a physical process $\mathcal{E}_k$ out of a set of possible processes $\{\mathcal{E}_i\}$ should take a state to a multiple of another

$$\mathcal{E}_k(\rho) = p_k \rho_k$$

where p_k represents the probability of obtaining state ρ_k starting with ρ. The second says if we have a machine which produces a particle in the state ρ_k with probability p_k, then whether $\mathcal{E}$ occurs on the particle while it is inside the machine or after it is received should not change the outcome of the overall state we see. And finally the third mentions positive operators, which just means the operator in question has only non-negative eigenvalues, a property density operators have since their eigenvalues are probabilities. It must be completely positive since we should be able to view a physical process on a subsystem as one on any system which includes the subsystem.

The unitary evolution of a closed system, the evolution of an open system $\mathcal{E}(\rho) = Tr_{env}(U(\rho \otimes \rho_{env})U^\dagger)$ and quantum measurements are all examples of valid quantum operations under the previous three axioms. Any quantum operation has an *operator sum* representation which means $\mathcal{E}$ can be expressed as

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger$$

where K_k are called *Kraus operators* and have the property $\sum_i K_i^\dagger K_i \leq I$. An example of this could be a measurement $\{M_m\}$. In this case, the Kraus representation of the process which consists of measuring outcome m would be $\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$ and so there is just one Kraus operator which is equal to M_m.

1.2 Quantum computing basics

In this section we go through some of the quantum computing basics, which are not required to understand most of this thesis, but are of interest nonetheless. We do, however, later make use of the notion of a *qubit* which is defined here. For a much more detailed discussion, see [1].

1.2.1 Quantum bits

In a classical computer, the fundamental unit of information is the *bit* which is simply either a 0 or a 1. Everything you see on the computer screen has been encoded in terms of bits and then interpreted somehow by the computer to create something we can understand. For example, the number of combinations of 2 bits is 4: 00, 01, 10 and 11, and in general the number of combinations of n bits is 2^n. There are 26 letters in the alphabet, meaning we would require $n > \log_2 26 \approx 4.7$ bits to encode a single letter of the alphabet. For a letter, we therefore need at least 5 bits to encode it, i.e. 5 bits allow us to encode $2^5 = 32$ objects. The computer is also able to perform operations on the bits to give new sets of bits which can then be interpreted and displayed to us. In a *quantum computer*, the fundamental unit of information is a *quantum bit* or *qubit*. Just like a classical bit, which has a state of either 0 or 1, a qubit also has a state. Instead of being either in the 0 or the 1 state though, a qubit may be in a superposition of the 0 and 1 state:

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$$

where c_0 and c_1 and complex numbers satisfying $|c_0|^2 + |c_1|^2 = 1$. These can be physically realized with a system which can be in any of two definite states, such as the spin of an electron (spin up or spin down). A qubit represents a regular quantum system; it just lives in a Hilbert space with dimension 2. It can therefore be in a mixed state, have quantum operations be performed on it, measurements and so on.

1.2.2 Bloch sphere representation

In general, a complex number c may be written as $c = |c|e^{i\gamma}$ where θ is a real number and $i = \sqrt{-1}$. This means our qubit can we written as

$$|\psi\rangle = |c_0|e^{i\gamma_0} |0\rangle + |c_1|e^{i\gamma_1} |1\rangle .$$

Now, the normalization condition implies $|c_0|^2 + |c_1|^2 = 1$ so we can set $|c_0| = \cos(\theta/2)$ and $|c_1| = \sin(\theta/2)$. Since global phases are of no interest to us, we can factor one out from our qubit and drop it

$$\begin{aligned} |\psi\rangle &= e^{i\gamma_0} \left(\cos(\theta/2) |0\rangle + \sin(\theta/2) e^{i(\gamma_1 - \gamma_0)} |1\rangle\right) \\ \rightarrow |\psi\rangle &= \cos(\theta/2) |0\rangle + \sin(\theta/2) e^{i\phi} |1\rangle \end{aligned}$$

This equation provides a useful means to visualize a single qubit on the surface of a sphere; the parameters θ and ψ specify a point $\vec{a} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$. This sphere is commonly called the *Bloch sphere*. Many of the operations on single qubits are neatly described by paths along the Bloch sphere. There is, however, no simple generalization of the Bloch sphere known for multiple qubits. For mixed

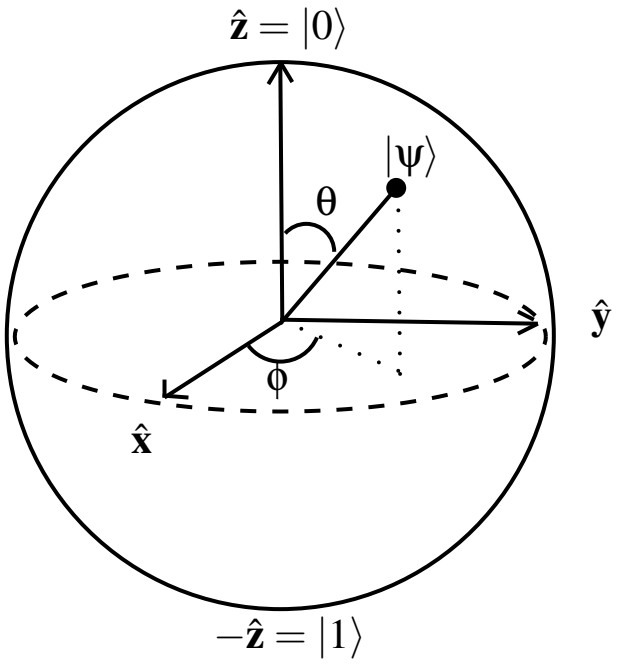


Figure 1.1: Bloch sphere representation of a qubit.

states, any single qubit density matrix ρ can be expanded using the identity and the *Pauli matrices* $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ where $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ as

$$\rho = \frac{1}{2}(I + \vec{a} \cdot \vec{\sigma}).$$

One way to check whether a state is mixed or not, is by evaluating the trace of its square

$$purity = Tr(\rho^2)$$

which is 1 for pure states and $1/d$, where d is the dimension of the system, for a *maximally mixed* state (one with highest entropy, $\rho = I/d$). Therefore, in order for

a point on the Bloch sphere to correspond to a pure state, we must have

$$Tr(\rho^2) = \frac{1}{2}(1 + |\vec{a}|^2) = 1 \Leftrightarrow |\vec{a}| = 1,$$

i.e., a point on the surface corresponds to a pure state while a point within the sphere corresponds to a mixed state.

1.2.3 Quantum logic gates

Classical computers, as was mentioned, perform operations on their bits. When these operations are performed in a computing setting we call them *logic gates*. Consider a single classical bit and the possible operations we can perform on it. The only non-trivial operation consists of changing a 0 to a 1 and vice-versa, this is called a *NOT* gate. For single qubits, however, there are more. The analogue to a *NOT* gate for qubits is given by the X gate which in matrix form is (in the *computational basis*, i.e., $\{|0\rangle, |1\rangle\}$)

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

i.e. the Pauli matrix σ_x. Applying it to the qubit state $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$ yields

$$X |\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_0 \end{bmatrix}$$

and we see that $|0\rangle$ has been *flipped* to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. The other non-trivial quantum gates consist of all other unitary operations U. A couple more important ones are the Z gate:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

which leaves $|0\rangle$ unchanged, and flips the sign of $|1\rangle$ to give $-|1\rangle$, and the *Hadamard* gate,

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

which sends $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$.

On the Bloch sphere, the X gate simply reflects a state with respect to the xy plane, the Z gate does a 180 degree rotation about the z axis and H is a 90 degree rotation about the y axis.

There are also gates which act on multiple qubits, such as the *controlled not* or $CNOT$ gate, which takes a *control* qubit and a *target* qubit as input. The target qubit is flipped whenever the control qubit is $|1\rangle$ and remains the same otherwise. The $CNOT$ gate in matrix form is

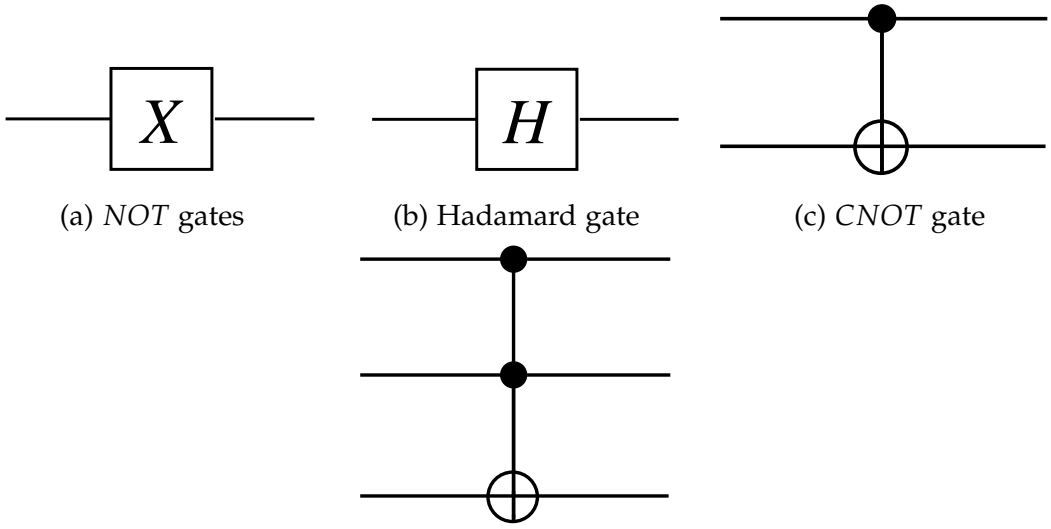
$$CNOT \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix}$$

for the case where the first qubit is the control. Another important controlled gate is the three-qubit *Toffoli* gate, also called a $CCNOT$ gate, which is the same as a $CNOT$ except an extra control qubit is added. Its matrix form is

$$CCNOT \equiv \begin{bmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & X \end{bmatrix}$$

1.2.4 Quantum circuits

A *quantum circuit* is an acyclic network of quantum gates connected by wires. At each end of the circuit are the input and output qubits which are connected by the wires which pass through the gates. At any point within this network, we may also perform measurements. Gates are represented by a number of different symbols across the wires which they affect. In Fig. 1.2 we list the gates previously discussed and their symbols. An example of one inside a circuit is given in Fig. 1.3, where the circuit performs a $CNOT$ gate on the input state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$ and then measures the value of the first qubit, i.e., performs a projective measurement in the *computational basis* $\{|0\rangle, |1\rangle\}$.



(a) *NOT* gates (b) Hadamard gate (c) *CNOT* gate

(d) Toffoli gate

Figure 1.2: Symbols for some important quantum gates. The solid black dots are used to represent the control qubits in a controlled gate. We challenge the reader to figure out what the symbol for a Z gate looks like.

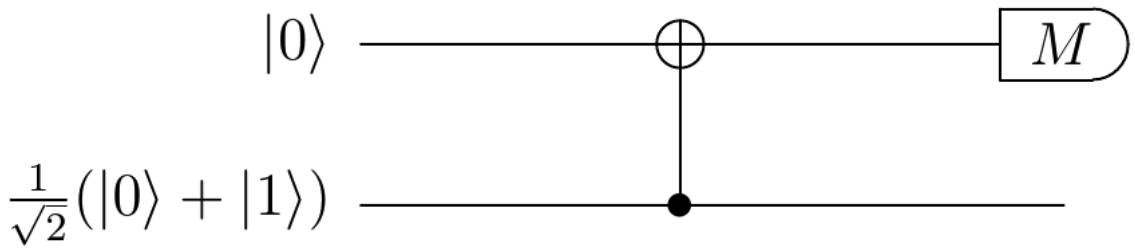


Figure 1.3: Example of a quantum circuit containing a *CNOT* gate.

Chapter 2

Quantum entanglement

2.1 Classical correlations

Consider a composite system $\rho = \rho_A \otimes \rho_B$ on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. This state is uncorrelated and it can be seen that the expected value for any joint observables $O_A \otimes O_B$ on the respective subsystems (O_A acts on $\mathcal{H}_A$, O_B acts on $\mathcal{H}_B$) always factorizes

$$\begin{aligned}\langle O_A \otimes O_B \rangle &= Tr[(O_A \otimes O_B)(\rho_A \otimes \rho_B)] \\ &= Tr(O_A\rho_A \otimes O_B\rho_B) \\ &= Tr(O_A\rho_A)Tr(O_B\rho_B) \\ &= \langle O_A \rangle \langle O_B \rangle .\end{aligned}$$

If a state cannot be factorized in such a way, then the system is said to be correlated. But correlated how? Do these correlations exhibit non-classical behaviour? In this chapter, we introduce a couple distinct notions of *quantum correlations*, one of them being the famed *quantum entanglement*. In Chapter 3, we define yet another notion of quantum correlations called quantum *discord*.

2.2 Local-realistic world view

This comes from the famous 1935 EPR paradox where Einstein, Podolsky and Rosen [3] had major objections to quantum mechanics and intended to show that it was an incomplete theory. It concerns two spacially separated particles who are

perfectly correlated in positions and momenta as predicted possible by quantum mechanics. What this means is that measurement of one particle's position yields perfect knowledge of the other's position in an instantaneous way, without the need to look at the other particle! They said that in order for a theory to be complete it would have to have an element of physical reality to it which they claimed to be *local realism* [4] which in short means

- ⊙ *locality* - There is no action at a distance;
- ⊙ *realism* - If, without disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.

Consider, for example, the two qubit mixed state

$$\rho = \frac{1}{2}\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|\right) \tag{2.1}$$

which has exactly the same statistics in the computational basis as the two qubit pure state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right). \tag{2.2}$$

That is, either outcome has a 50% chance on each qubit, but once the value of one of the qubits is known the other is also known. However, we can rewrite the first qubit of ρ in terms of the $\{|\pm\rangle\}$ basis, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, as

$$\begin{aligned}\rho =& \frac{1}{4}(|+\rangle + |-\rangle)(\langle +| + \langle -|) \otimes |0\rangle\langle 0| + \frac{1}{4}(|+\rangle - |-\rangle)(\langle +| - \langle -|) \otimes |1\rangle\langle 1| \\ =& \frac{1}{2}\left(|+\rangle\langle +| + |-\rangle\langle -|\right) \otimes \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) \\ &+ \frac{1}{2}\left(|+\rangle\langle -| + |-\rangle\langle +|\right) \otimes \frac{1}{2}\left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)\end{aligned}$$

From this we see that measuring the first qubit in the $\{|\pm\rangle\}$ basis will yield either outcome with 50% probability, but once we know the outcome, this does not tell us anything about the second qubit. The state ρ is considered to be classically correlated since there is clearly nothing *nonlocal* about this state. This is not so for $|\psi\rangle$. Whatever basis we decide to measure in will always yield perfect correlation

between both subsystems. Using the $\{|\pm\rangle\}$ basis as an example, we get

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \otimes \frac{1}{\sqrt{2}}|1\rangle \\ &= \frac{1}{\sqrt{2}}|+\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}|-\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}|+\rangle \otimes |+\rangle + \frac{1}{\sqrt{2}}|-\rangle \otimes |-\rangle\end{aligned}$$

which shows both qubits are perfectly correlated in the $\{|\pm\rangle\}$ basis as well. This clearly violates the element of locality EPR has argued must hold, since the outcome of any measurement on one subsystem is perfectly correlated with the other.

EPR argued that states such as $|\psi\rangle$ violate fundamental truths about reality and therefore quantum mechanics must be incomplete. But in comes Bell and his *Bell inequalities* [1] which provide experimental tests to end the debate between EPR and quantum mechanics. These inequalities tell us whether we have a state like ρ in Eq. 2.1 or one like $|\psi\rangle$ in Eq. 2.2. The first one which was discovered (there are multiple such inequalities) is the CHSH inequality: Suppose Alice and Bob live in an EPR world and each have some particle in their possession along with two measurement apparatuses which measure the observables Q and R for Alice, and S and T for Bob. Suppose also, for simplicity, that these observables have the outcomes $+1$ or -1. Then the CHSH inequality is

$$\langle Q \otimes S\rangle + \langle R \otimes S\rangle + \langle R \otimes T\rangle - \langle Q \otimes T\rangle \leq 2. \tag{2.3}$$

This allows one to set up an experiment to verify whether this inequality holds. If one can prepare a system which violates this Bell inequality, then we must certainly live in a quantum world where non locality exists and the local realism brought forth by EPR must not be valid.

We can also use this inequality to define a notion of classical correlations: States which do not violate the Bell inequalities are considered to be classical and quantum otherwise. For example, a product state $\rho_A \otimes \rho_B$ is easily shown to satisfy the CHSH inequality by using the fact that observables factorize:

$$\begin{aligned}&\langle Q \otimes S\rangle + \langle R \otimes S\rangle + \langle R \otimes T\rangle - \langle Q \otimes T\rangle \\ &= (\langle Q\rangle + \langle R\rangle)\langle S\rangle + (\langle R\rangle - \langle Q\rangle)\langle T\rangle \\ &\leq 2\langle R\rangle \\ &\leq 2\end{aligned}$$

where we have assumed, without loss of generality, that $\langle R\rangle \geq \langle Q\rangle$, and since all expectations are at most 1. As another example, consider the previous state ρ (Eq. 2.1). The expectation of the joint observable $Q \otimes S$ on this state is

$$\begin{aligned}\langle Q \otimes S\rangle &= \frac{1}{2}Tr[(Q \otimes S)(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)] \\ &= \frac{1}{2}Tr[Q|0\rangle\langle 0| \otimes S|0\rangle\langle 0|] + \frac{1}{2}Tr[Q|1\rangle\langle 1| \otimes S|1\rangle\langle 1|)] \\ &= \frac{1}{2}\left[Tr(Q|0\rangle\langle 0|)Tr(S|0\rangle\langle 0|) + Tr(Q|1\rangle\langle 1|)Tr(S|1\rangle\langle 1|)\right]\end{aligned}$$

and since $Tr(Q) = 0$, we have $Tr(Q|0\rangle\langle 0|) = -Tr(Q|1\rangle\langle 1|)$ (similarly for S) and so

$$\langle Q \otimes S\rangle = Tr(Q|0\rangle\langle 0|)Tr(S|0\rangle\langle 0|).$$

Doing this for each of the other joint observables and applying the argument for product states shows that the state ρ satisfies the CHSH inequality as well and is thus deemed classical. As a final example, we test the state $|\psi\rangle$ (Eq. 2.2): Consider the observables

$$\begin{array}{cc} Q = \sigma_z & R = \sigma_x \\ S = (\sigma_x + \sigma_z)/\sqrt{2} & T = (\sigma_x - \sigma_z)/\sqrt{2}\end{array}$$

Recall that σ_z flips only the sign of $|1\rangle$ and σ_x flips the qubit. We can readily calculate the expectations for the joint observables given by these, the first one is

$$\begin{aligned}\langle Q \otimes S\rangle &= \frac{1}{\sqrt{2}}\langle \sigma_z \otimes \sigma_z\rangle + \frac{1}{\sqrt{2}}\langle \sigma_z \otimes \sigma_x\rangle \\ &= \frac{1}{\sqrt{2}}Tr(|\psi\rangle\langle\psi|) + \frac{1}{\sqrt{2}}Tr\left(\frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)\langle\psi|\right) \\ &= \frac{1}{\sqrt{2}} + 0\end{aligned}$$

and the rest are

$$\langle R \otimes S\rangle = \frac{1}{\sqrt{2}};\ \langle R \otimes T\rangle = \frac{1}{\sqrt{2}};\ \langle Q \otimes T\rangle = -\frac{1}{\sqrt{2}}. \tag{2.4}$$

Thus,

$$\langle Q \otimes S\rangle + \langle R \otimes S\rangle + \langle R \otimes T\rangle - \langle Q \otimes T\rangle = 2\sqrt{2} \tag{2.5}$$

which violates the CHSH inequality! The state $|\psi\rangle$ is therefore deemed to have quantum correlations.

2.3 Local operations and classical communication

Local operations and classical communication (LOCC) is a particular restriction on the set of operations between two systems which means exactly what its title suggests. If observers Alice and Bob start with the uncorrelated states ρ_A and ρ_B respectively and sets of quantum operations $\{\mathcal{A}_i\}$ and $\{\mathcal{B}_i\}$ on each respective state in their possession, then an LOCC operation could be the following: Alice performs a measurement on her state and finds the outcome described by the quantum operation $\mathcal{A}_k$, she then phones Bob (a regular phone is a classical device) telling him exactly what she found. Bob can now decide what he would like to do with his state based on Alice's phone call. This process can then continue for as long as Alice and Bob wish. Mathematically, the first part described looks like

$$\rho'_{AB} = \frac{(\mathcal{A}_k \otimes I_B)(\rho_A \otimes \rho_B)}{Tr((\mathcal{A}_k \otimes I_B)(\rho_A \otimes \rho_B))} \rightarrow \text{ ring ring "Hi, Bob? Its Alice..."}$$

after some discussion, they might decide it would be best for Bob to perform a certain measurement, for which he receives the outcome described by $\mathcal{B}_j$:

$$\rho''_{AB} = \frac{(I_A \otimes \mathcal{B}_j)(\rho'_{AB})}{Tr((I_A \otimes \mathcal{B}_j)(\rho'_{AB}))}$$

and so on... One can verify that such a protocol is indeed a quantum operation

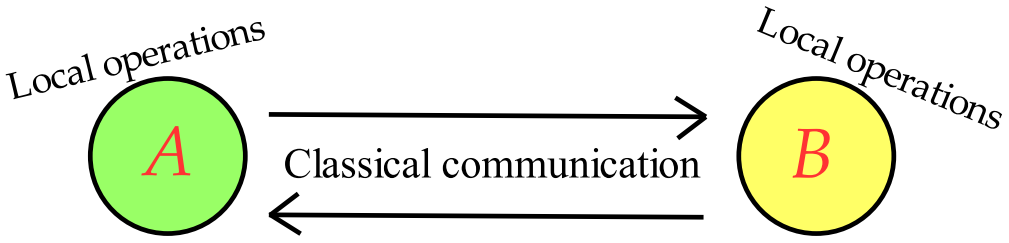


Figure 2.1: LOCC allows for operations on each system separately and sending of classical bits back and forth between systems.

under the axioms defined in Chapter 1.

Allowing classical communication give these operations quite a complicated structure. Alice and Bob may communicate after any round of local operations and decide on the next operation based on previous outcomes of measurements.

Because of this complexity, a general operation Λ_{LOCC} has no known simple characterization [9]. We can, however, write down any local operation as

$$\mathcal{E}_{local}(\rho_{AB}) = \sum_k (K_A^k \otimes K_B^k)\rho_{AB}(K_A^k \otimes K_B^k)^\dagger \tag{2.6}$$

where K_A^k and K_A^k are Kraus operators with

$$\sum_k (K_A^k \otimes K_B^k)^\dagger (K_A^k \otimes K_B^k) = \sum_k K_A^{k\dagger} K_A^k \otimes K_B^{k\dagger} K_B^k \leq I_A \otimes I_B.$$

The ability to send classical information in general does not allow one to write Λ_{LOCC} in such way. It can be shown that any state which can be prepared via LOCC, e.g. Alice and Bob share a product state $\rho_A \otimes \rho_B$ initially and use LOCC to end up with some ρ_{AB}, has the following form

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \tag{2.7}$$

and is said to be a separable state. All other states are defined as entangled. Eq. 2.7 says that a separable state is a mixture of product states or, since we can write ρ_A^i and ρ_B^i as convex mixtures of pure states, a mixture of separable pure states. The LOCC protocol therefore provides a precise definition of classicality: all separable states are deemed classical.

It is known that every separable state satisfies the Bell inequalities and, in the past, it was believed that all entangled states violate Bell's inequalities, thus making LOCC and Bell's inequalities equivalent notions of classicality. It was pointed out, however, by Werner in 1989 [5] that there exist certain mixed quantum states which are entangled but do not violate any of the Bell inequalities. Therefore under a local-hidden-variable theory, what is considered a classical state can have entanglement.

2.4 Quantum entanglement

We have defined an entangled state as one which is not separable, i.e. cannot be written in the form $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$. This entanglement turns out to be necessary for certain quantum algorithms which we discuss in Subsection 2.4.1. Quantum entanglement is thus a quantum resource which is used to perform

computations efficiently where a classical computer could not. This is where *entanglement measures* come into play. They attempt to put a number on the usefulness of an entangled state. We go into more detail about entanglement measures in Section 2.5.

2.4.1 Quantum computing and entanglement

Quantum entanglement has been studied extensively and there are a wide range of applications for it. An example is the well known *quantum teleportation* protocol [6], which is a process by which a qubit is transmitted exactly from one location to another, without the qubit being transmitted through the intervening space. To get an idea of how this works, suppose two observers Alice and Bob share two maximally entangled qubits, i.e., one of the four *Bell basis states*

$$\begin{aligned}
|\Phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \\
|\Phi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \\
|\Psi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \\
|\Psi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)
\end{aligned} \tag{2.8}$$

Alice take the A qubit and Bob takes the B qubit. In the following we assume Alice and Bob share the $|\Phi^+\rangle_{AB}$ state. Alice also starts with another qubit $|\psi\rangle_C$: the qubit she wishes to send to Bob. The total system is thus given by

$$|\Phi^+\rangle_{AB} \otimes |\psi\rangle_C = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \otimes (c_0 |0\rangle_C + c_1 |1\rangle_C)$$

We can rewrite this through a change of basis using the easily verifiable identities

$$
\begin{aligned}
|0\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) \\
|0\rangle \otimes |1\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \\
|1\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \\
|1\rangle \otimes |1\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)
\end{aligned}
$$

as

$$
\begin{aligned}
|\Phi^+\rangle_{AB} \otimes |\psi\rangle_C = &\frac{1}{2} |\Phi^+\rangle_{AC} \otimes (c_0 |0\rangle_B + c_1 |1\rangle_B) \\
&+\frac{1}{2} |\Phi^-\rangle_{AC} \otimes (c_0 |0\rangle_B - c_1 |1\rangle_B) \\
&+\frac{1}{2} |\Psi^+\rangle_{AC} \otimes (c_1 |0\rangle_B + c_0 |1\rangle_B) \\
&+\frac{1}{2} |\Psi^-\rangle_{AC} \otimes (c_1 |0\rangle_B - c_0 |1\rangle_B)
\end{aligned}
$$

It can easily be seen that by performing a projective measurement in the Bell basis, that, given the outcome of the measurement, Alice can inform Bob on the telephone that he must perform one of four operations on his qubit:

- ⊙ If Alice measures $|\Phi^+\rangle_{AC}$, then Bob leaves his qubit alone.
- ⊙ If Alice measures $|\Phi^-\rangle_{AC}$, then Bob performs $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ on his qubit.
- ⊙ If Alice measures $|\Psi^+\rangle_{AC}$, then Bob performs $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ on his qubit.
- ⊙ If Alice measures $|\Psi^-\rangle_{AC}$, then Bob performs $\sigma_x\sigma_z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = -i\sigma_y$ on his qubit.

Now Bob has the exact qubit which Alice previously had in her possession. Notice that Alice has communicated her state to Bob using only 2 bits of classical information (she tells Bob to perform one of four unitaries), while the state

$|\psi\rangle_C = c_0 |0\rangle_C + c_1 |1\rangle_C$ requires 3 real parameters to describe it (including its global phase). It is the quantum nature of the maximally entangled qubit they share at the beginning which allows this advantage.

Although it is not certain whether entanglement is the only resource which provides a quantum speedup, it is required for algorithms such as quantum teleportation, *Shor's algorithm* for finding the prime factorization of numbers and computing the *discrete logarithm* [7]. The last two algorithms involve the *quantum Fourier transform* [8], which makes use of entanglement.

2.5 Entanglement measures

If quantum entanglement is a resource which can be used to make faster computers, then we should be able to quantify just how much of this resource is at hand. This is where the concept of entanglement measure comes into play. The theory behind entanglement measures is very well understood for pure states. For pure states we have what is called the *Schmidt decomposition* which is stated in the following theorem [1]

Theorem (Schmidt decomposition)**.** For a bipartite pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, there exists a basis of $\mathcal{H}_A$: $\{|\alpha_k\rangle\}_{k=1}^{\dim \mathcal{H}_A}$, a basis of $\mathcal{H}_B$: $\{|\beta_k\rangle\}_{k=1}^{\dim \mathcal{H}_B}$, and probabilities $\{p_k\}_{k=1}^{\min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}}$ such that $|\psi\rangle$ can be written down as

$$|\psi\rangle = \sum_{k=1}^{\min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}} \sqrt{p_k}\, |\alpha_k\rangle \otimes |\beta_k\rangle \tag{2.9}$$

A pure bipartite state is then separable if and only if the probabilities p_k, which are called *Schmidt coefficients* are all 0 except for one, i.e its Schmidt decomposition has only one term in it. These coefficients are unique and are precisely the features of the state which do not change under local unitary transformations, thus they tell you everything about the separability of a state and therefore its entanglement. The *Schmidt rank* is simply the number of non-zero Schmidt coefficients in the expansion and serves to give an idea of how entangled a state is, i.e., a pure state is entangled if and only if its Schmidt rank is one. The goal of an entanglement measure is to try and capture what the Schmidt coefficients tell us about entanglement in a single number and, it turns out, entanglement measures

satisfying a certain set of requirements reduce to the *entropy of entanglement* for pure states.

For mixed states, it isn't so simple. We can, however, define properties that a good entanglement measure should have. The idea is that, since entanglement cannot be created by an LOCC operation Λ_{LOCC}, a state $\sigma_{AB} = \Lambda_{LOCC}(\rho_{AB})$ is a weaker resource than ρ_{AB} since whatever can be done with σ_{AB} and LOCC can also be done with ρ_{AB} and LOCC. So we say $E : \rho_{AB} \to E(\rho_{AB}) \in \mathbb{R}$ is an *entanglement monotone* if [10]

$$E(\Lambda_{LOCC}(\rho_{AB})) \leq E(\rho_{AB}) \tag{2.10}$$

for all bipartite states ρ_{AB} and all LOCC operations. Since any separable state can be created via LOCC, we know that $\rho_{sep} = \Lambda_{LOCC}(\sigma_{sep})$ and $\sigma_{sep} = \Lambda'_{LOCC}(\rho_{sep})$. This tells us that $E(\rho_{sep}) = E(\Lambda_{LOCC}(\sigma_{sep})) \leq E(\sigma_{sep})$ and $E(\sigma_{sep}) = E(\Lambda'_{LOCC}(\rho_{sep})) \leq E(\rho_{sep})$, therefore $E(\rho_{sep}) = E(\sigma_{sep})$. This means we may ask the monotone to take on a particular value for separable states, lets take 0, and if we also ask that $E(\rho_{AB}) \geq 0$ for all ρ_{AB} then E becomes an *entanglement measure*. Throughout the rest of this thesis, the word *entanglement* is used to mean the value of an entanglement measure. The following are some properties of entanglement [9]:

⊙ Entanglement does not change under local unitary operations

This follows easily from the fact that LOCC does not increase entanglement. Since an LOCC consisting of a local unitary operation can be inverted, it certainly cannot decrease entanglement otherwise its inverse would increase it. Therefore the entanglement before and after the local unitary must be the same.

⊙ There are maximally entangled states.

It turns out that any state consisting of two d-dimensional systems can be prepared through LOCC with a state of the form

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d} |\alpha_k\rangle \otimes |\beta_k\rangle \,. \tag{2.11}$$

Such a state and all of its unitary equivalents therefore have maximal entanglement.

⊙ The only correlations in a pure state are due to entanglement.

A separable pure state is also a product state and therefore has no correlations, classical or quantum.

⊙ The two subsystems of a maximally entangled states are maximally mixed.

This can be seen through the expression for a maximally entangled state: by tracing out either subsystem we get $\rho = Tr_A(|\psi\rangle\langle\psi|) = Tr_B(|\psi\rangle\langle\psi|) = I/d$.

We say that E is *faithful* if it only maps separable states to 0 (i.e. $E(\rho_{AB}) > 0$ for entangled states). There are also many other optional properties that an entanglement measure may satisfy [9, 10]:

⊙ Instead of entanglement monotones, we might consider measures which are *monotone on average*, which means

$$E(\rho^{in}) \geq \sum_k p_k^{out} E(\rho_k^{out}) \tag{2.12}$$

where ρ_k^{out} are states which can be obtained with probabilities p_k^{out} starting with ρ^{in} through LOCC. Every entanglement monotone is also monotone on average since $E(\rho^{in}) \geq E(\rho_k^{out})$ for all k.

⊙ A measure is *convex* if

$$E\left(\sum_k p_k \rho_k\right) \leq \sum_k p_k E(\rho_k) \tag{2.13}$$

for all density matrices ρ_k and probability distributions p_k.

⊙ A measure is *additive* with respect to independent systems if

$$E(\rho_{AB} \otimes \sigma_{A'B'}) = E(\rho_{AB}) + E(\sigma_{A'B'}) \tag{2.14}$$

where the entanglement is measured between AA' and BB' on the left hand side.

2.5.1 Entanglement entropy

Using the Schmidt decomposition, we can write down expressions for the state of each subsystem in a bipartite pure state $|\psi_{AB}\rangle = \sum_{k=1}^{d} \sqrt{p_k}\,|\alpha_k\rangle \otimes |\beta_k\rangle$

$$\rho_A = Tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|) = \sum_{k=1}^{d} p_k\,|\alpha_k\rangle\langle\alpha_k| \tag{2.15}$$

and similarly

$$\rho_B = Tr_A(|\psi_{AB}\rangle \langle\psi_{AB}|) = \sum_{k=1}^{d} p_k |\beta_k\rangle \langle\beta_k| \tag{2.16}$$

where d is just shorthand for $\min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$. From this we see that the Schmidt coefficients p_k are just the eigenvalues of the density matrices of either subsystem! Now we make use of the very useful quantity called the *von Neumann entropy* $S(\rho)$ which is defined as

$$S(\rho) \equiv -Tr(\rho \log \rho). \tag{2.17}$$

If ρ is written in terms of its eigendecomposition as $\rho = \sum_k p_k |\psi_k\rangle \langle\psi_k|$, then the von Neumann entropy becomes

$$S(\rho) = -\sum_k p_k \log p_k \tag{2.18}$$

Some properties of the von Neumann entropy are [1]:

- $S(\rho)$ is non-negative.
- $S(\rho) = 0$ if and only if ρ is a pure state.

  This is simply due to the fact that $S(\rho) = -\sum_j p_j \log p_j = 0$ if and only if $p_k = 1$ for some k which means $\rho = |\psi_k\rangle \langle\psi_k|$.
- $S(\rho) = \log d$, where d is the dimension of the Hilbert space of ρ, if and only if ρ is maximally mixed.
- $S(\rho)$ is invariant under unitary transformations of ρ.

  This is obvious since a unitary transformation does not change the eigenvalues of ρ.
- $S(\rho)$ is *concave*:

  $$S\left(\sum_k \lambda_k \rho_k\right) \geq \sum_k \lambda_k S(\rho_k) \tag{2.19}$$

  where the λ_k are positive numbers such that $\sum_k \lambda_k = 1$.
- $S(\rho)$ is additive:

  $$S(\rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B) \tag{2.20}$$

- $|S(\rho_A) - S(\rho_B)| \leq S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$, where the right hand inequality is known as *subadditivity*.

If system AB is in a pure state, then its subsystems A and B are separable if and only if they are in a product state. This means $S(\rho_A) = S(\rho_B) = 0$ for separable pure states and $S(\rho_A) > 0$ (and $S(\rho_B) > 0$, since $S(\rho_A) = S(\rho_B)$) for entangled states. The entanglement entropy is defined as

$$E_E(|\psi_{AB}\rangle) \equiv S(\rho_A) = S(\rho_B) \tag{2.21}$$

and is an entanglement monotone. It is additive due to the additivity of von Neumann entropy.

2.5.2 Mixed state entanglement

In the case of mixed states, the answer is not so simple. In 1996, Peres [11] had shown a necessary condition for a separable state:

Theorem (Peres criterion)**.** *If ρ is separable, then the operator $(T \otimes I)(\rho)$ is positive.*

The map T is a transpose map on one of the subsystems of ρ and $(T \otimes I)$ is called the *partial transpose* of ρ. In Appendix C we show how the Peres criterion can be used to find a simple sufficient condition for entanglement. Soon after, was shown by the Horodecki family, a necessary and sufficient condition for separability in the following theorem [12]:

Theorem. *Let ρ act on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. Then ρ is separable if and only if for any positive map $\Lambda : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$, the operator $(I \otimes \Lambda)(\rho)$ is positive.*

The symbol $\mathcal{L}(\mathcal{H})$ denotes the space of all linear operators on the Hilbert space $\mathcal{H}$. This theorem cannot usually be applied to determine the separability of concrete states, but it was also shown in the same paper [12] that for 2×2 and 2×3 dimensional quantum systems the partial transpose criterion provided by Peres is necessary and sufficient. There exists an entanglement monotone for mixed states called the *negativity* [13] which makes use of the Peres criterion. It is defined as follows:

$$\mathcal{N}(\rho_{AB}) \equiv \frac{\|(T_A \otimes I_B)(\rho_{AB})\|_1 - 1}{2} \tag{2.22}$$

where $\|X\|_1 = Tr(|X|) = Tr\left(\sqrt{X^\dagger X}\right)$ is the *trace norm* of the operator X, which is just the sum of the absolute value of each eigenvalue. Since the partial transpose is a trace preserving map, it is clear this is zero if and only if the eigenvalues of $(T_A \otimes I_B)(\rho_{AB})$ are all positive, i.e. the partial transpose of ρ_{AB} is a density matrix. This is therefore a faithful entanglement measure for 2×2 and 2×3 systems. The negativity is not additive, and so is an example of an entanglement measure which does not reduce to the entropy of entanglement for pure states [9].

Another measure for mixed state entanglement which extends the definition of entanglement entropy is the *entanglement of formation* [14]. It is defined as

$$E_f(\rho_{AB}) \equiv \min \sum_k p_k E_E(|\psi^k_{AB}\rangle) \tag{2.23}$$

where the minimization is taken over all ensembles of pairs $\{(p_k, |\psi^k_{AB}\rangle)\}$ such that

$$\rho_{AB} = \sum_k p_k \, |\psi^k_{AB}\rangle \, \langle\psi^k_{AB}| \tag{2.24}$$

This process of minimizing the average pure state entanglement over sets of pure states is called a *convex roof* construction and it is guaranteed that such a construction is an entanglement monotone [9]. It is clearly a faithful measure of entanglement for mixed states since if $E_f(\rho_{AB}) = 0$, then each $|\psi^k_{AB}\rangle$ in the minimization is separable and therefore ρ_{AB} in Eq. 2.24 is written as a convex sum of product states, i.e. is separable. This measure trivially reduces to the entanglement entropy for pure states.

2.5.3 Entanglement monogamy

Consider sharing a secret with a friend via some classical means such as email. There is absolutely nothing stopping your secret from being shared, apart from your friend's loyalty, with as many other people who care to hear about it. One of the distinct properties of entanglement is that it cannot be freely shared in such a way. If Alice and Bob both share a maximally entangled state, then it is impossible for anyone else to share entanglement with them. This is known as *monogamy of entanglement* [15]. This is also true of states which are not maximally entangled: systems cannot freely share entanglement between each other.

For a pure three qubit system ABC, the negativity obeys the following *monogamy inequality* [16]

$$\mathcal{N}_{AC}^2 + \mathcal{N}_{BC}^2 \leq \mathcal{N}_{(AB)C}^2 \tag{2.25}$$

where $\mathcal{N}_{XY}$ is the negativity between systems X and Y. This exactly means that, the more system A is entangled with C, the less system B is entangled with C. The entanglement A and C each separately share with C is also bounded by the entanglement shared by the combined system AB and C.

It turns out this inequality does not hold for all entanglement measures. For example, it does not hold in general for the entanglement of formation [14, 17].

2.5.4 Multipartite entanglement

So far we have only talked about *bipartite* entanglement, that is, entanglement between any two systems A and B. What about entanglement between multiple systems? It is possible for a system A to be separable from system B and from system C, but entangled with the combined system BC. So how do we define *multipartite* entanglement? First, we define the notion of k-separability [18]:

Definition A state ρ composed of n systems is called k-separable if the length of the longest separable chain of subsystems is k:

$$\rho = \sum_i p_i \rho_i^1 \otimes \rho_i^2 \otimes (...) \otimes \rho_i^k \tag{2.26}$$

where each ρ_i^j may contain an arbitrary positive number of subsystems and p_i is a probability distribution.

In such an n-partite system, if $k = n$ then the state is fully separable. If $k = 1$ then the state is fully entangled. For pure states, k is easily found by calculating the entanglement entropy between any two bipartitions and checking its nullity. For example, given a state $|\psi\rangle$, we find that one of its bipartitions is separable

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \,. \tag{2.27}$$

We may continue this process on each of the states $|\psi_1\rangle$ and $|\psi_2\rangle$ until we can't go further. If $k > 1$, then at least one of the bipartitions must be separable and we do not have truly multipartite entanglement. The significance of entanglement for

pure state computations can be seen here. For separable n-qubit pure states $|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes ... \otimes |\psi_n\rangle$, we see that only a polynomial amount of parameters are required to describe this state, i.e. both coefficients in each $|\psi_i\rangle$. In an entangled n-qubit state, however, we do not have such a factorization and so we require an exponential (2^n, if the state is fully entangled) number of parameters to describe such a state. This is where entanglement in pure state computations is believed to draw its power from.

The question now is, how do we quantify multipartite entanglement? We can use all of the axioms defined in the bipartite setting to define a measure, additionally, we add the following requirements:

$$E(\rho_{k-sep}) > 0 \text{ if } k < n$$
$$E(\rho_{k-sep}) = 0 \text{ if } k = n \text{ , i.e. is fully separable}$$

Notice that, with these axioms in place, an entanglement measure cannot differentiate between truly multipartite entanglement ($k = 1$) and others. An easy way to overcome this is by simply changing the previous axioms to

$$E(\rho_{k-sep}) > 0 \text{ if } k = 1$$
$$E(\rho_{k-sep}) = 0 \text{ otherwise.}$$

Truly multipartite entanglement is what we are concerned with in the next sections, more specifically tripartite entanglement. We use a measure valid for three qubit mixed states called the *pi-tangle* [16] which is defined for a system ABC as the average of the three quantities

$$\pi_A = \mathcal{N}^2_{A(BC)} - \mathcal{N}^2_{AB} - \mathcal{N}^2_{AC}$$
$$\pi_B = \mathcal{N}^2_{B(AC)} - \mathcal{N}^2_{BA} - \mathcal{N}^2_{BC}$$
$$\pi_C = \mathcal{N}^2_{C(AB)} - \mathcal{N}^2_{CA} - \mathcal{N}^2_{CB}.$$

where $\mathcal{N}_{XY}$ denotes the negativity between subsystems X and Y. In symbols, the pi-tangle is defined as

$$\pi_{ABC} \equiv \frac{\pi_A + \pi_B + \pi_C}{3} \tag{2.28}$$

This is a good measure of truly tripartite entanglement. Since negativity is itself an entanglement monotone, we know the pi-tangle must also be. It is positive

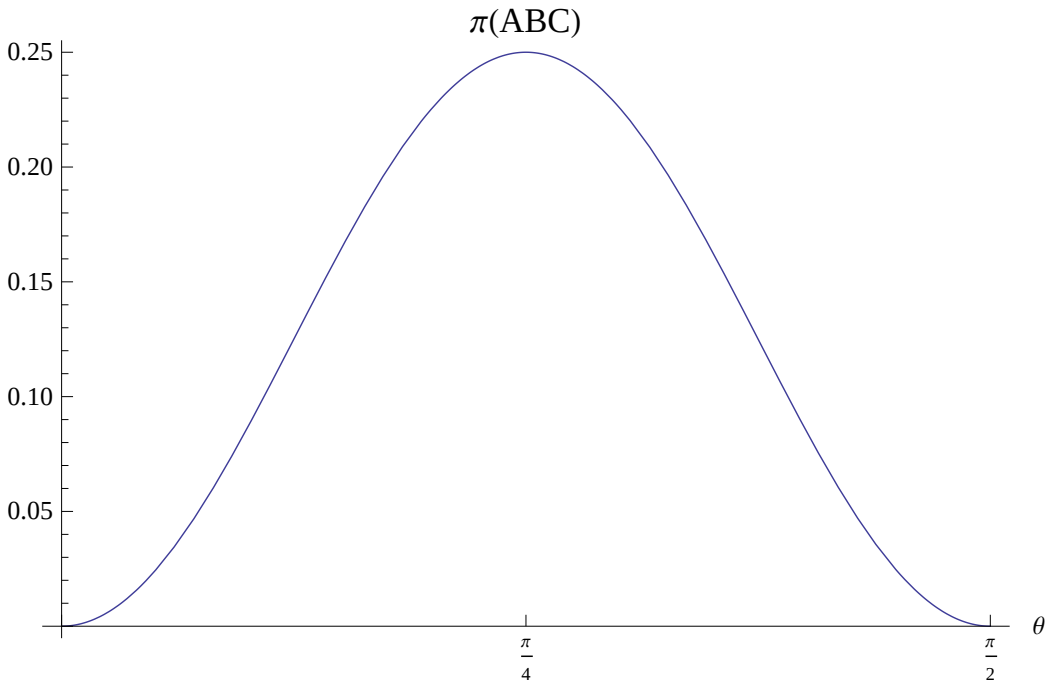


Figure 2.2: Pi-tangle for the three qubit GHZ type state $|\psi\rangle = \cos\theta\,|000\rangle + \sin\theta\,|111\rangle$.

and zero when tripartite entanglement does not exist, i.e. when at least one of the bipartitions of ABC is separable, due to the monogamy inequality for negativity (Eq. 2.25). In Figures [2.2,2.3,2.4] we show plots of the pi-tangle for two classes of states: the W and GHZ states. We see that, for these states, the pi-tangle is a faithful measure of tripartite entanglement.

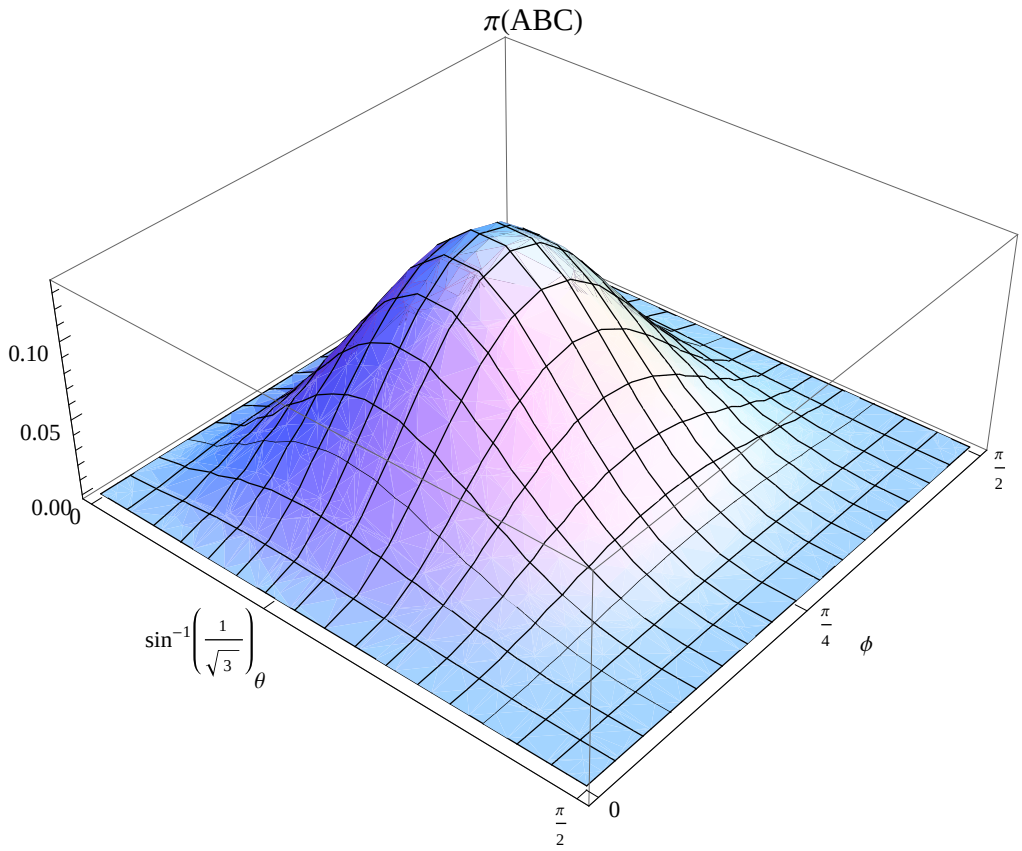


Figure 2.3: Pi-tangle for the three qubit W type state $|\psi\rangle = \cos\theta\cos\phi\,|001\rangle + \cos\theta\sin\phi\,|010\rangle + \sin\theta\,|100\rangle$.

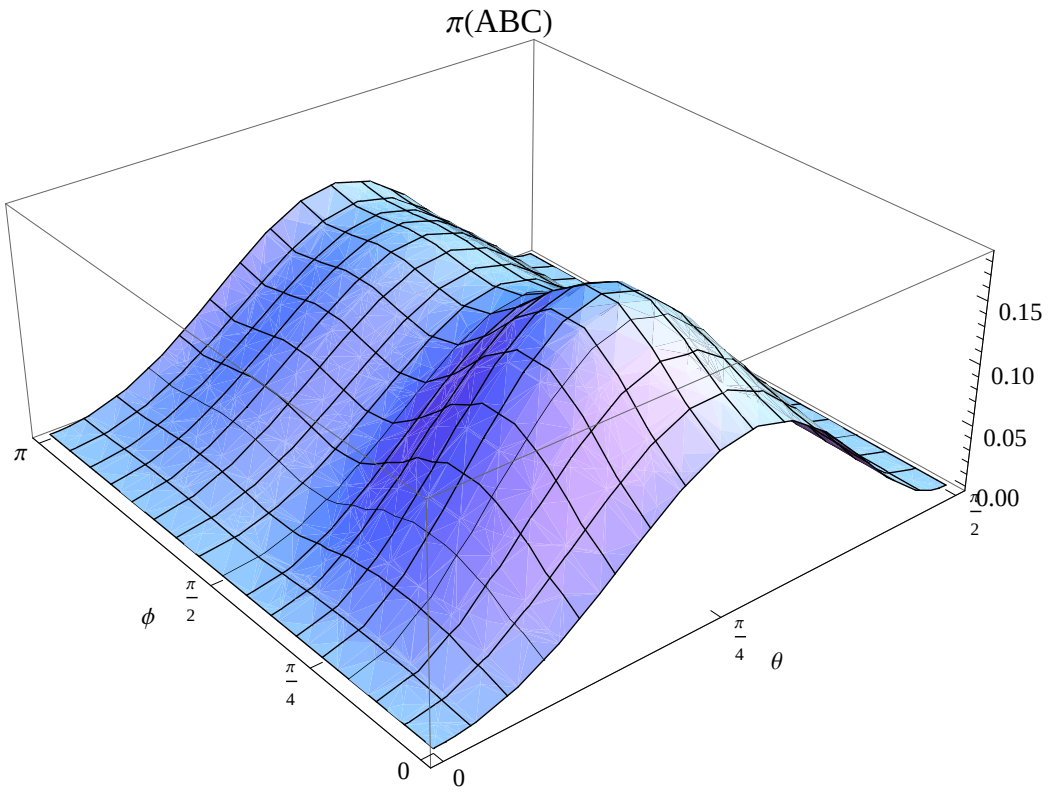


Figure 2.4: Pi-tangle for a combination of GHZ and W type states $|\psi\rangle = (\cos\theta\,|000\rangle + \sin\theta\,|111\rangle + \cos\theta\cos\phi\,|001\rangle + \cos\theta\sin\phi\,|010\rangle + \sin\theta\,|100\rangle)/\sqrt{2}$.

Chapter 3

Quantum discord

Here we introduce the measure of quantum correlations called *quantum discord*. I was initially proposed in [19] using ideas from classical information theory and adapting them to the quantum formalism. A more thorough review can be found in [20].

3.1 Information theory

We wish to quantify how much two systems are correlated. One way to look at this is to calculate the redundant information between two systems A and B. This quantity is called the *mutual information* between systems A and B [19]

$$I(A:B) \equiv H(A) + H(B) - H(AB). \tag{3.1}$$

$H(X)$ is the Shannon entropy $H(X) = -\sum_x p_x \log p_x$ where X is a classical variable with values x occurring with probability p_x (usually the logarithm is taken to be base two).

One could also get a sense of the correlations between two systems A and B by calculating how much information is gained about B through knowledge of A. For classical systems A and B, this is equal the mutual information

$$I(A:B) = H(B) - H(B|A) \tag{3.2}$$

where the *conditional entropy* $H(B|A) = \sum_a p_a H(B|A=a)$ is the average of entropies $H(B|A=a)$. The entropies $H(B|A=a)$ denote the amount of information

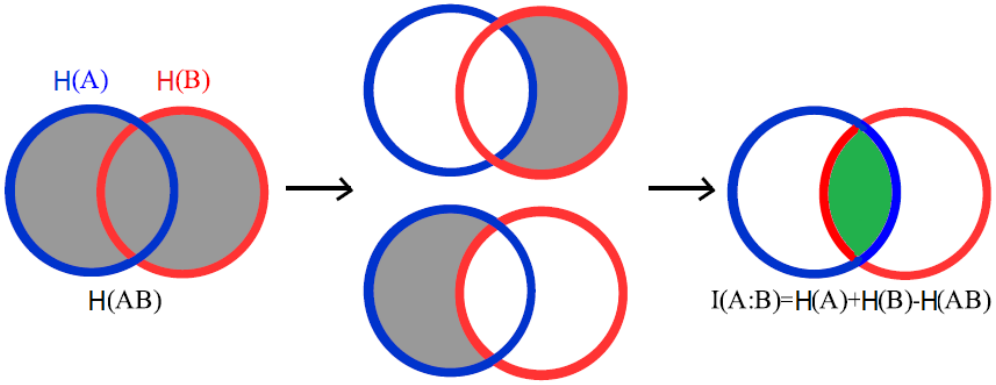


Figure 3.1: The mutual information $I(A:B)$ is equal to the redundant information after discovering both A and B separately.

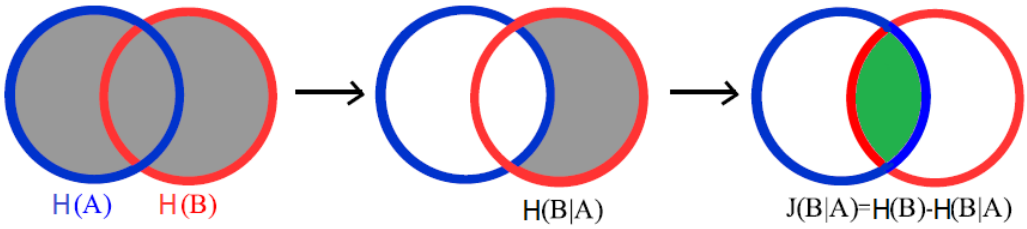


Figure 3.2: $H(B|A)$ is the amount of information remaining in B after discovering everything about A. What has been discovered about B through A, i.e. $H(B) - H(B|A)$, is equal to $I(A:B)$ in classical information theory.

in B given that A is in the state a which, for classical variables A and B, can be written as

$$H(B|A=a) = -\sum_b p_{b|a} \log p_{b|a} \tag{3.3}$$

where $p_{b|a} = p_{ba}/p_a$ is the conditional probability as defined by *Bayes' rule*.

This relationship between the conditional entropy and mutual information does not, in general, hold for quantum states. The outcomes a discussed are now dependent upon the measurement made on the system. If $\{E_a\}$ denotes a POVM on the system A, then outcome a will be observed with probability $p_a = Tr(E_a \rho_{AB})$ and B has the conditional state $\rho_{B|A=a} = Tr_A(E_a \rho_{AB})/p_a$. Therefore, the classical-quantum analogue to the conditional entropy can be defined as

$$S(B|\{E_a\}) \equiv \sum_a p_a S(\rho_{B|A=a}) \tag{3.4}$$

for the measurement $\{E_a\}$, where $S(X)$ is the von Neumann entropy $S(X) = -Tr(\rho_X \log \rho_X)$. We can define the classical-quantum mutual information, for a particular measurement, as

$$J(B|\{E_a\}) \equiv S(B) - S(B|\{E_a\}) \tag{3.5}$$

In order to quantify the amount of classical-quantum information contained between A and B, it is natural to maximize this quantity over all possible measurements we could perform on A

$$J(B|A) \equiv \max_{\{E_a\}} J(B|\{E_a\}) \tag{3.6}$$

This equation tells us exactly how much information it is possible to gain about B through measurements performed on A only.

3.2 Quantum discord

We have rewritten the definition of conditional entropy using the language of quantum mechanics: instead of classical random variables A and B we have used the density matrix formalism where $\rho_A = Tr_B(\rho_{AB})$ and $\rho_B = Tr_A(\rho_{AB})$, and, instead of restricting ourselves to classical measurements (questions about the value of a classical random variable) we have the more general POVMs.

It turns out, however, that only rank-one POVMs are required in order to maximize $J(B|\{E_a\})$. This can be seen through the following argument [24]: In order to maximize $J(B|\{E_a\}) = S(B) - S(B|\{E_a\})$, we must minimize $S(B|\{E_a\})$. First, notice that any POVM element E_a may be reduced to a combination of rank-one POVM elements through E_a's spectral decomposition

$$E_a = \sum_k E_{ak}. \tag{3.7}$$

We have

$$\rho_{B|A=a} = Tr_A(E_a \rho_{AB})/p_a = \sum_k Tr_A(E_{ak}\rho_{AB})/p_a = \sum_k \frac{p_{ak}}{p_a}\rho_{B|A=ak} \tag{3.8}$$

and so by the concavity of entropy (Eq. 2.19)

$$S(\rho_{B|A=a}) \geq \sum_k \frac{p_{ak}}{p_a} S(\rho_{B|A=ak}) \rightarrow S(B|\{E_a\}) \geq S(B|\{E_{ak}\}) \tag{3.9}$$

In classical theory these correspond to questions about the value of a classical random variable, so our quantum version of $J(B|A)$ is equivalent to the classical conditional entropy whenever A and B are classical. It is natural then to define a state to be classical whenever

$$I(A:B) = J(B|A), \tag{3.10}$$

where $I(A:B) = S(A) + S(B) - S(AB)$ is the quantum version of the mutual information, and quantum whenever

$$D(B|A) \equiv I(A:B) - J(B|A) > 0 \tag{3.11}$$

where $D(B|A)$ is called quantum *discord*. The quantity $J(B|A)$ can be shown to be always less than or equal the mutual information and so quantum discord is a non-negative quantity [20]. It has also been shown [23, 24] that a state has the form

$$\rho_{AB} = \sum_k p_k \Pi_A^k \otimes \rho_B^k, \tag{3.12}$$

where $\Pi_A^k = |\alpha_k\rangle \langle\alpha_k|$ are orthogonal rank-one projection operators, if and only if $D(B|A) = 0$. Similarly, $\rho_{AB} = \sum_k p_k \rho_A^k \otimes \Pi_B^k$ if and only if $D(A|B) = 0$. It follows from this that zero discord states are also separable. It is not, however, true that all

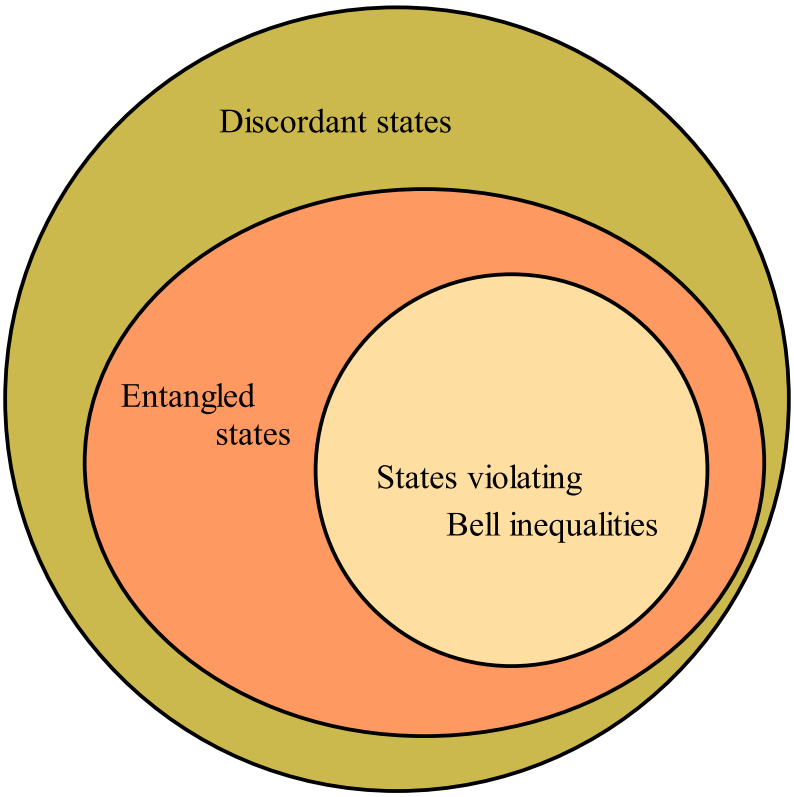


Figure 3.3: The set of discordant states includes all entangled states, which in turn includes all states which violate the Bell inequalities.

separable states have zero discord and so the set of *discordant* (non-zero discord) states is larger than the set of entangled states, the latter of which is larger than the set of states which violate the Bell inequalities. Discord is also not symmetric, i.e., in general $D(B|A) \neq D(A|B)$ which is due to the fact that conditional entropy is not a symmetric quantity. An example of this is the following two qubit state, which has $D(B|A) = 0$ but $D(A|B) > 0$:

$$\rho = \frac{1}{2}(|0\rangle\langle 0| \otimes |-\rangle\langle -| + |1\rangle\langle 1| \otimes |0\rangle\langle 0|)$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Local unitary transformations $(U_A \otimes U_B)\rho_{AB}(U_A \otimes U_B)^\dagger$ do not change discord because such a transformation does not alter the entropies of each subsystem and the value obtained for $S(B|\{E_a\})$ can be obtained via the measurement $\{U_A E_a U_A^\dagger\}$. Non-unitary local operations on A (but not on B) can, however, increase discord $D(B|A)$ [21]. This is not overly surprising since A is the system over which classicality is being tested through measurement [20].

3.3 Quantum computing and discord

Recent results have shown that not only entanglement is a resource capable of allowing a quantum advantage, but that mere discord could also provide a quantum advantage in some cases. This could be of practical significance because discord is more easily produced and maintained than entanglement [37]. Here we provide an example where quantum discord has been found to be useful in the context of quantum computing through the computational model DQC1 [25], and we also present results from [26] which give an operational interpretation of discord.

3.3.1 Discord in DQC1

A computational model was proposed by Knill and Laflamme [25], called DQC1, in which the initial input to any circuit consists of a single pure qubit, along with n qubits in the maximally mixed state $I^{\otimes n}/2^n$. Although it has been proven that this model is less powerful than a regular, pure state quantum computer [27], it can still perform tasks efficiently where there are no known polynomial time classical algorithms. In the following, we show how a DQC1 circuit can be used to approximate the *normalized trace* of an arbitrary n qubit unitary U_n, $Tr(U_n)/2^n$, in a efficient manner [25, 28]. The only known classical algorithms for calculating such a trace are exponential in the number of qubits, n. Figure 3.4 contains a generalization of the DQC1 circuit which performs the trace. Notice that this circuit takes as input n maximally mixed qubits along with the qubit $\frac{1}{2}(I + \alpha\sigma_z)$ which is pure when $\alpha = 1$ and mixed otherwise, with $\alpha = 0$ giving the maximally mixed state of a single qubit. We expect this circuit to perform at its best when $\alpha = 1$ and not work at all when $\alpha = 0$ since all our inputs are maximally mixed states. The overall initial state is

$$\begin{aligned}\rho_i &= \frac{1}{2^{n+1}}(I + \alpha\sigma_z) \otimes I^{\otimes n} \\ &= \frac{1}{2^{n+1}}\left[(\alpha+1)\left|0\right\rangle\left\langle 0\right| \otimes I^{\otimes n} + (1-\alpha)\left|1\right\rangle\left\langle 1\right| \otimes I^{\otimes n}\right] \end{aligned} \tag{3.13}$$

The first qubit passes through a Hadamard gate which maps $|0\rangle$ to $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ to $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

$$\rho_i \to \frac{1}{2^{n+1}}\left[|0\rangle\langle 0| \otimes I^{\otimes n} + |1\rangle\langle 1| \otimes I^{\otimes n} + \alpha\,|0\rangle\langle 1| \otimes I^{\otimes n} + \alpha\,|1\rangle\langle 0| \otimes I^{\otimes n}\right],$$

then the others undergo the controlled unitary U_n. The state right before the measurement is performed thus becomes

$$\begin{aligned}\rho_f &= \frac{1}{2^{n+1}}\left[|0\rangle\langle 0| \otimes I^{\otimes n} + |1\rangle\langle 1| \otimes I^{\otimes n} + \alpha\,|0\rangle\langle 1| \otimes U_n^\dagger + \alpha\,|1\rangle\langle 0| \otimes U_n\right] \\ &= \frac{1}{2^{n+1}}\begin{pmatrix} I^{\otimes n} & \alpha U_n^\dagger \\ \alpha U_n & I^{\otimes n}\end{pmatrix}\end{aligned} \tag{3.14}$$

Consider now the observables σ_x and σ_y. Recall from Chapter 1 the expression for the expected value of an observable. This tells us that

$$\langle\sigma_x\rangle = Tr(\rho_f\sigma_x) = \frac{\alpha}{2^n}\mathrm{Re}\left[Tr(U_n)\right] \tag{3.15}$$

and

$$\langle\sigma_y\rangle = Tr(\rho_f\sigma_y) = -\frac{\alpha}{2^n}\mathrm{Im}\left[Tr(U_n)\right] \tag{3.16}$$

Obviously, the accuracy of this calculation depends on the number of runs the circuit must perform. The number of runs required to estimate the trace to within an accuracy of ϵ is approximately $1/\alpha^2\epsilon^2$ [28]. This number is independent of the size of the unitary U_n and it is in that sense that this algorithm is deemed efficient. It is also easily shown that the first qubit remains separable from the other n qubits during the entire run through the circuit. Clearly, it cannot be entangled after the Hadamard operation since it is local. If the eigendecomposition for the unitary U_n is

$$U_n = \sum_j e^{i\phi_j}\,|e_j\rangle\langle e_j|, \tag{3.17}$$

then we can write $I^{\otimes n} = \sum_j |e_j\rangle\langle e_j|$ and plug this all into the expression for ρ_f to give

$$\rho_f = \frac{1}{2^{n+1}}\sum_j\left[|0\rangle\langle 0| + |1\rangle\langle 1| + \alpha e^{i\phi_j}\,|0\rangle\langle 1| + \alpha e^{-i\phi_j}\,|1\rangle\langle 0|\right] \otimes |e_j\rangle\langle e_j| \tag{3.18}$$

thus showing it is indeed always separable. What then, could possibly account for the speedup over classical algorithms? The answer is quantum discord. Clearly

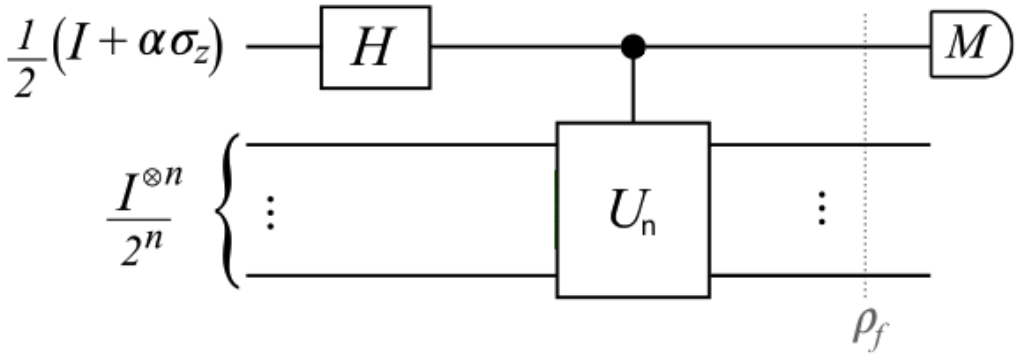


Figure 3.4: Circuit to measure the normalized trace of an arbitrary n qubit unitary U_n. The measurement M belongs either to the observable σ_x or σ_y, depending on wether we want to measure the real or the imaginary part of the normalized trace.

there is no initial discord between the first qubit and the rest, but there is after the controlled unitary. If A represents the first qubit and B the other n qubits, then $D(A|B) = 0$. However, it can be shown [29] that for large n and small $Tr(U_n)/2^n$, the discord $D(B|A)$ is given by

$$D(B|A) = 2 + \frac{1-\alpha}{2}\log\left(\frac{1-\alpha}{2}\right) + \frac{1+\alpha}{2}\log\left(\frac{1+\alpha}{2}\right) - \log\left(1+\sqrt{1-\alpha^2}\right) - \left(1-\sqrt{1-\alpha^2}\right)\log e \tag{3.19}$$

where the logarithm is taken base 2. Figure 3.5 plots this as a function of α.

There are some doubts about whether discord is truly the resource being utilized in this case [23]. But there has since been additional evidence that discord provides a quantum advantage in computation and/or communication. This includes, for example, the activation of *distillable entanglement* [38], bounds on distributed entanglement [39], quantum communication [40] and certification of entangling gates [41].

3.3.2 Coherent interactions and discord

Discord has been related [26] to the advantage of *coherent interactions* over single local measurements. An observer Alice encodes information within the subsystem A of the bipartite system AB and Bob is tasked with retrieving the encoded

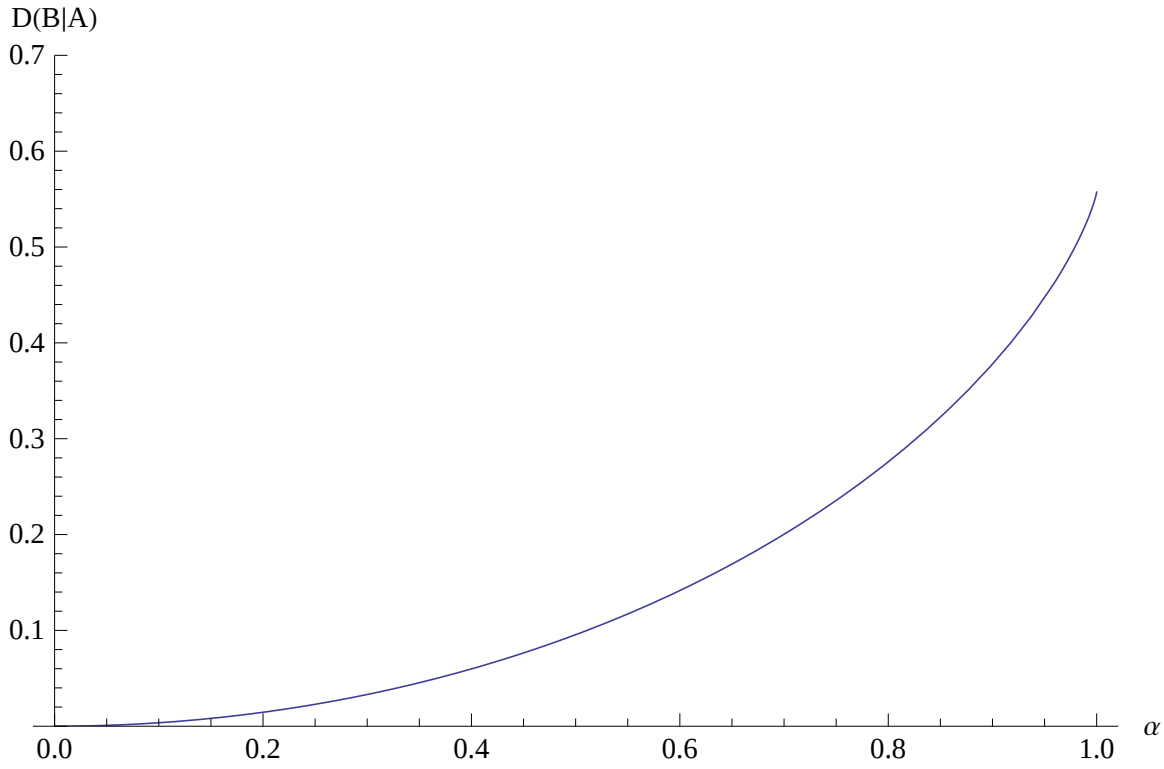


Figure 3.5: Approximate discord between the first qubit and the rest of the n qubits before measurement in the circuit depicted in Figure 3.4 as a function of the parameter α.

data. Bob's optimal performance when he is restricted to a single local measurement on each subsystem (in whichever order) is compared to the case where Bob may also coherently interact with the subsystems, which means he is allowed to implement arbitrary quantum operations between A and B. It was shown in [26] that these coherent interactions give Bob an advantage if and only if AB contains discord and that the amount of discord used by Alice during the encoding exactly bounds this advantage. This gives an operationally significant use for discord, as a resource which can be used to give coherent interactions this advantage.

More concretely, let ρ_{AB} represent the state of the system AB. Assume, also, that this state has been prepared in such a way so that $D(A|B) \leq D(B|A)$. Alice wants to encode the random variable K with the probability distribution $P(K = k) = p_k$ by applying a corresponding unitary U_k to her subsystem A with probability p_k. Bob is aware of the encoding scheme but since Bob does not know for sure which unitary Alice applies, the state he sees is

$$\rho'_{AB} = \sum_k p_k (U_k \otimes I)\rho_{AB}(U_k^\dagger \otimes I) \tag{3.20}$$

which has discord $D'(A|B)$. Bob is now tasked with estimating, as best as he can, the variable K. If his best attempt yields the classical variable K_0, then his estimate's quality is determined by the mutual information $I(K : K_0) = H(K_0) - H(K_0|K)$ between K and K_0. If I_c represents the quality of Bob's estimate when restricted to single local measurements on A and B and I_q the quality with additional coherent interactions, then $\Delta I = I_q - I_c$ represents the advantage coherent interactions allow. In [26] it is proven that

$$\Delta D(A|B) - J'(A|B) \leq \Delta I \leq \Delta D(A|B) \tag{3.21}$$

where $\Delta D(A|B) = D(A|B) - D'(A|B)$ is the discord consumed by Alice during the encoding process and $J'(A|B)$ is the classical-quantum information after encoding. This says that the advantage Bob has through coherent interactions is at most the discord consumed by Alice throughout her encoding process and so discord is required in order to have an advantage. As it turns out, it is also possible for Alice to use up all of the discord initially present so that $D'(A|B) = J'(A|B) = 0$ and

$$\Delta I = \Delta D(A|B) = D(A|B). \tag{3.22}$$

In this case, the advantage of coherent interactions is exactly the discord initially present between A and B.

Chapter 4

Discord and entanglement

In this chapter we briefly discuss known closed form expressions for discord in mixed states and then we show work which has been done by us [31] in relating discord to entanglement.

4.1 Discord in pure states

For pure states $|\psi_{AB}\rangle$ the relation between discord and entanglement is simple: they are the same. This can be seen by looking at the Schmidt decomposition of $|\psi_{AB}\rangle$

$$|\psi_{AB}\rangle = \sum_i \sqrt{p_i}\,|\alpha_i\rangle \otimes |\beta_i\rangle\,. \tag{4.1}$$

If we choose the projective measurement $\{|\alpha_k\rangle\langle\alpha_k|\}$ we get

$$\rho_{B|A=k} = \frac{Tr_A(|\alpha_k\rangle\langle\alpha_k|\,|\psi_{AB}\rangle\langle\psi_{AB}|)}{Tr(|\alpha_k\rangle\langle\alpha_k|\,|\psi_{AB}\rangle\langle\psi_{AB}|)} = |\beta_k\rangle\langle\beta_k|\,. \tag{4.2}$$

This means that $S(B|A) = \min_{\{E_a\}} \sum_a p_a S(\rho_{B|A=a})$ must be zero and

$$J(B|A) = S(B) - S(B|A) = S(B) \tag{4.3}$$

and the discord $D(B|A) = I(A:B) - J(B|A) = S(A) + S(B) - S(AB) - S(B) = S(A)$ which is the entropy of entanglement for the pure state $|\psi_{AB}\rangle$. Similarly, $D(A|B) = S(B) = S(A) = D(B|A)$.

4.2 Discord in mixed states

The story for mixed states is more complicated. For example, there exist mixed states which do not have entanglement but discord is present, such as the single qubit state

$$\rho = \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |-\rangle\langle -| \otimes |+\rangle\langle +|) \tag{4.4}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. This clearly has both discord $D(A|B)$ and $D(B|A)$ present but is separable.

Discord is a challenging quantity to calculate due to the optimization involved. Many studies of discord rely on numerical optimization to determine which measurement minimizes $S(B|\{E_a\})$. There is no known analytic expression for the discord in a general mixed state, but a few have been obtained for specific classes of states. For example, an analytic result is known for the class of *Bell-diagonal* states, which are arbitrary mixtures of Bell states (Eqs. 2.8):

$$\rho_{BD} = p_1 |\Psi^+\rangle\langle\Psi^+| + p_2 |\Psi^-\rangle\langle\Psi^-| + p_3 |\Phi^+\rangle\langle\Phi^+| + p_4 |\Phi^-\rangle\langle\Phi^-|. \tag{4.5}$$

Through local unitary transformations, which do not alter correlations, the Bell-diagonal states can be rewritten in the general form [20]

$$\rho_{BD} = (I \otimes I + c_x\sigma_x \otimes \sigma_x + c_y\sigma_y \otimes \sigma_y + c_z\sigma_z \otimes \sigma_z)/4. \tag{4.6}$$

where each of the p_k can be written in terms of c_x, c_y and c_z [22]:

$$\begin{aligned} p_1 &= (1 + c_x + c_y - c_z)/4 \\ p_2 &= (1 - c_x - c_y - c_z)/4 \\ p_3 &= (1 + c_x - c_y + c_z)/4 \\ p_4 &= (1 - c_x + c_y + c_z)/4 \end{aligned}$$

It turns out [22] that the optimization over POVMs reduces to calculating $c = \max\{|c_x|, |c_y|, |c_z|\}$ which gives

$$J_{BD}(B|A) = [(1-c)/2]\log(1-c) + [(1+c)/2]\log(1+c). \tag{4.7}$$

The reduced density matrices for ρ_{BD} are both $I/2$, which can easily be seen from Eq. 4.6. Thus, $S(A) = S(B) = 1$ and $S(AB) = -\sum_{k=1}^{4} p_k \log p_k$, giving a mutual information of

$$I(A:B) = 2 + \sum_{k=1}^{4} p_k \log p_k. \tag{4.8}$$

Discord is thus given by

$$D_{BD}(B|A) = 2 + \sum_{k=1}^{4} p_k \log p_k - [(1-c)/2]\log(1-c) - [(1+c)/2]\log(1+c) \tag{4.9}$$

The discord in this case is symmetric, which is clear from the general form in Eq. 4.6. The entanglement of formation is also known for this class of states [30]

$$E_f(\rho_{BD}) = 1 - [(1-x)/2]\log(1-x) - [(1+x)/2]\log(1+x) \tag{4.10}$$

where $x = 2\sqrt{p_{max}(1-p_{max})}$ if $p_{max} = \max_k p_k > 1/2$, otherwise $E_f(\rho_{BD}) = 0$.

Although this is a nice simple equation for discord, it is restricted to a narrow class of states. Not much is known about mixed state discord, we have a better understanding of entanglement and of its applications. For this reason, we would like to somehow link discord to entanglement.

Notice that it is always possible to view a mixed state on $\mathcal{H}_A$ as part of a larger Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. More specifically, given a ρ_A over $\mathcal{H}_A$, there exists a $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that

$$Tr_B(|\psi_{AB}\rangle\langle\psi_{AB}|) = \rho_A$$

for any ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$. This is called state *purification*. A simple purification which works for any mixed state $\rho_A = \sum_k p_k |\psi_A^k\rangle\langle\psi_A^k|$ is

$$|\psi_{AB}\rangle = \sum_k \sqrt{p_k}\,|\psi_A^k\rangle \otimes |\psi_B^k\rangle \tag{4.11}$$

where $\{|\psi_B^k\rangle\}$ is an orthonormal basis for $\mathcal{H}_B$. The purification is not unique, e.g. you can always append some other pure state to $|\psi_{AB}\rangle$: $|\psi_{AB}\rangle \otimes |\psi_C\rangle$. It should thus be possible to view discord in a mixed state as arising from the entanglement present in its purification. We use this in the next sections to get an idea of how discord in a bipartite mixed state relates to the entanglement structure in its purification.

4.3 Entanglement structure

Here I report on a collaboration [31] which is focused on relating discord to the various entanglements found in a pure tripartite system. In particular, I wrote

code to look at the behaviour of discord and entanglement numerically in different scenarios. I also add here a calculation for the entanglement structure in an arbitrary rank-two state which was not included in the paper which concerns this thesis.

4.3.1 Three-qubit pure states

To get an idea of how bipartite discord is related to the bipartite and tripartite entanglements inside a tripartite pure state, we start by looking at a simple case: a pure three-qubit state $|\psi_{ABC}\rangle$. If we require that the AB system be separable, then we expect that, since discord is equivalent to entanglement entropy for pure states, the presence of discord in the AB system arises because of entanglement in its purification $|\psi_{ABC}\rangle$. It can easily be shown, through the Schmidt decomposition, that the reduction $\rho_{AB} = Tr_C(|\psi_{ABC}\rangle \langle\psi_{ABC}|)$ must have at most two eigenvalues, i.e. a rank-two operator. This fact allows us to write out a simple expression for the most general (up to local unitary transformations) two-qubit, rank-two, separable state

$$\rho_{AB} = |c_1|^2 |0\rangle \langle 0| \otimes |0\rangle \langle 0| + |c_2|^2 |\alpha\rangle \langle\alpha| \otimes |\beta\rangle \langle\beta| \tag{4.12}$$

where $|c_1|^2 + |c_2|^2 = 1$ and $|\alpha\rangle$ and $|\beta\rangle$ are arbitrary qubits. Ignoring the trivial cases where $c_1 = 0$ or $c_2 = 0$, we now ask under what circumstances ρ_{AB} contains discord or not. Recall that discord $D(B|A)$ is zero if and only if

$$\rho_{AB} = \sum_k p_k \Pi_A^k \otimes \rho_B^k$$

where the Π_A^k are rank-one orthogonal projectors on $\mathcal{H}_A$. Comparing this with our expression for our two-qubit ρ_{AB} we see that

$$D(B|A) = 0 \text{ iff } \{|\alpha\rangle \propto |1\rangle \text{ or } |\alpha\rangle \propto |0\rangle \text{ or } |\beta\rangle \propto |0\rangle\} \tag{4.13}$$

and similarly for discord $D(A|B)$ to be zero we require

$$\rho_{AB} = \sum_k p_k \rho_A^k \otimes \Pi_B^k$$

so for our two-qubit ρ_{AB}

$$D(A|B) = 0 \text{ iff } \{|\beta\rangle \propto |1\rangle \text{ or } |\alpha\rangle \propto |0\rangle \text{ or } |\beta\rangle \propto |0\rangle\}. \tag{4.14}$$

We now want to determine the entanglement structure found within the purification of ρ_{AB} by comparing where AC, BC and ABC are separable with where we have found discord to be zero. The purification $|\psi_{ABC}\rangle$ is given by

$$|\psi_{ABC}\rangle = c_1 |0\rangle \otimes |0\rangle \otimes |0\rangle + c_2 |\alpha\rangle \otimes |\beta\rangle \otimes |1\rangle . \tag{4.15}$$

Now tracing out the B system to get the state on AC yields

$$\begin{aligned} \rho_{AC} &= Tr_B(|\psi_{ABC}\rangle \langle\psi_{ABC}|) \\ &= |c_1|^2 |0\rangle \langle 0| \otimes |0\rangle \langle 0| + |c_2|^2 |\alpha\rangle \langle\alpha| \otimes |1\rangle \langle 1| + (\chi + \chi^\dagger) \end{aligned} \tag{4.16}$$

where we have set $\chi = c_1 c_2^* \langle 0|\beta\rangle |\alpha\rangle \langle 0| \otimes |1\rangle \langle 0|$. We can rewrite χ by using the fact that $|\alpha\rangle = \langle 0|\alpha\rangle |0\rangle + \langle 1|\alpha\rangle |1\rangle$ to get

$$\chi = c_1 c_2^* \langle 0|\beta\rangle [\langle 0|\alpha\rangle |0\rangle \langle 0| \otimes |1\rangle \langle 0| + \langle 1|\alpha\rangle |1\rangle \langle 0| \otimes |1\rangle \langle 0|] \tag{4.17}$$

$$= \gamma + \zeta \tag{4.18}$$

where

$$\gamma \equiv c_1 c_2^* \langle 0|\beta\rangle \langle 0|\alpha\rangle |0\rangle \langle 0| \otimes |1\rangle \langle 0| \tag{4.19}$$

$$\zeta \equiv c_1 c_2^* \langle 0|\beta\rangle \langle 1|\alpha\rangle |1\rangle \langle 0| \otimes |1\rangle \langle 0| . \tag{4.20}$$

Combining the $|0\rangle \langle 0|$ terms together in ρ_{AC} yields

$$\rho_{AC} = |c_1|^2 |0\rangle \langle 0| \otimes \rho_0 + |c_2|^2 |\alpha\rangle \langle\alpha| \otimes |1\rangle \langle 1| + (\zeta + \zeta^\dagger) \tag{4.21}$$

and from this we see that ρ_{AC} is separable if and only if $\zeta = 0$ (see Appendix B for proof), i.e.

$$\rho_{AC} \text{ is separable iff } \{|\beta\rangle \propto |1\rangle \text{ or } |\alpha\rangle \propto |0\rangle\} \tag{4.22}$$

similarly, we find when ρ_{BC} is separable

$$\rho_{BC} \text{ is separable iff } \{|\alpha\rangle \propto |1\rangle \text{ or } |\beta\rangle \propto |0\rangle\}. \tag{4.23}$$

Now we must figure out when $|\psi_{ABC}\rangle$ has no tripartite entanglement. A state is said to have no tripartite entanglement if any one of its bipartitions $A(BC)$, $(AB)C$ or $(AC)B$ is separable. Since $|\psi_{ABC}\rangle$ is a pure state, this happens if and only if one of the subsystems A, B or C is in a pure state. We can find out when this is

so by simply looking at our expression for ρ_{AB}: we want either ρ_{AB}, $Tr_A(\rho_{AB})$, or $Tr_B(\rho_{AB})$ to be pure. This happens when and only when $|\alpha\rangle \propto |0\rangle$ or $|\beta\rangle \propto |0\rangle$:

$$|\psi_{ABC}\rangle \text{ has no tripartite entanglement iff } \{|\alpha\rangle \propto |0\rangle \text{ or } |\beta\rangle \propto |0\rangle\}. \quad (4.24)$$

The main result of this section is found by comparing these statements about zero entanglement with the one we had for zero discord, yielding

$$D(B|A) = 0 \text{ iff } \{BC \text{ is separable or } ABC \text{ has no tripartite entanglement } \} \quad (4.25)$$

and of course, similarly we have

$$D(A|B) = 0 \text{ iff } \{AC \text{ is separable or } ABC \text{ has no tripartite entanglement}\}. \quad (4.26)$$

A summary of these statements can be found in Fig. 4.1.

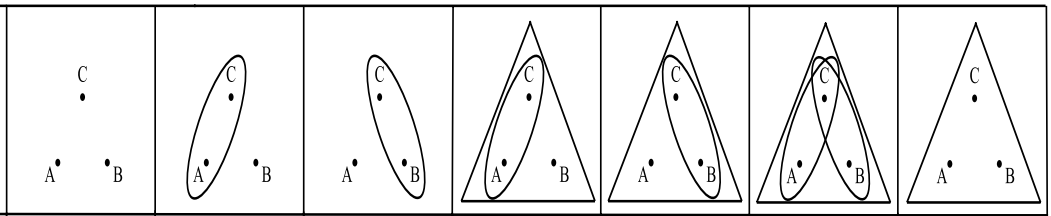
Entanglement structure							
D(A|B)	0	0	0	>0	0	>0	0
D(B|A)	0	0	0	0	>0	>0	0

Figure 4.1: Entanglement structure in pure three qubit system with A and B separable. Systems which are grouped together by either an ellipse or a triangle share bipartite or tripartite entanglement respectively.

4.3.2 Testing the relation numerically

The structure seen in Fig. 4.1 would seem to suggest that an increase in $D(B|A)$ should be accompanied by an either an increase in the entanglement BC or ABC, or both. Similarly $D(A|B)$ seems it should increase with increasing entanglement AC or ABC, or both. To test these relations, we first set $|\alpha\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle$ and $|\beta\rangle = \cos\beta\,|0\rangle + \sin\beta\,|1\rangle$ and calculate the discord for such a two qubit state, along with the bipartite and tripartite entanglements via the negativity (Eq. 2.22), denoted by $\mathcal{N}$, and pi-tangle (Eq. 2.28), denoted by π, respectively. We then

consider two trajectories through the (α, β) plane characterizing our state. One of these is a path of constant $\pi(ABC)$ and the other is a path of constant $\mathcal{N}(AC)$. We then plot the remaining quantities as functions of an arbitrary parameter φ that parameterizes these paths. This will let us, for example deduce how $D(A|B)$ changes as entanglement AC changes but while entanglement ABC is kept at a constant, nonzero value. These plots are displayed in Fig. 4.2, where we keep constant $\pi(ABC) = 0.2$, and in Fig. 4.3 where we keep constant $\mathcal{N}(AC) = 0.1$. In Fig. 4.2 we observe the behaviour that was expected, namely $D(A|B)$ is perfectly monotonic with $\mathcal{N}(AC)$ and $D(B|A)$ is perfectly monotonic with $\mathcal{N}(BC)$. In Fig. 4.3, however, we find something rather different, namely we find that neither $D(A|B)$ nor $D(B|A)$ is always monotonic with with $\pi(ABC)$. This is not surprising in the case of $D(B|A)$ because, as we see, the negativity $\mathcal{N}(BC)$ drops to zero. It is surprising, however, that we also see a decrease in $D(A|B)$ during this period, despite $\mathcal{N}(AC)$ remaining constant and $\pi(ABC)$ increasing. Evidently, while $\mathcal{N}(BC)$ does not play a role in the nullity of $D(A|B)$, is does generally contribute to its value.

There is another interesting observation that can be made from Fig. 4.2: For a fixed value of $\pi(ABC)$, since $D(A|B)$ increases with $\mathcal{N}(AC)$ and $D(B|A)$ increases with $\mathcal{N}(BC)$, we notice that the asymmetry between $D(A|B)$ and $D(B|A)$ stems from the fact that entanglement AC and BC are anticorrelated (entanglement monogamy, see Section 2.5.3).

4.3.3 Separable rank-two states

These statements hold for any separable rank-two state on AB (does not have to be two qubits) since the argument can be carried out again but without assuming $|\alpha\rangle$ and $|\beta\rangle$ are qubits. The if and only if statement about zero discord in Eq. 4.14, without assuming $|\alpha\rangle$ and $|\beta\rangle$ are qubits, becomes

$$D(A|B) = 0 \text{ iff } \{\langle 0|\beta\rangle = 0 \text{ or } |\alpha\rangle \propto |0\rangle \text{ or } |\beta\rangle \propto |0\rangle\}, \tag{4.27}$$

i.e., the $|\beta\rangle\langle\beta|$ projector must be orthogonal to the first projector $|0\rangle\langle 0|$, or AB be in a product state. We can purify the state of AB using a single qubit and, by tracing over the B system, we see that ρ_{AC} has the same form as Eq. 4.21 except

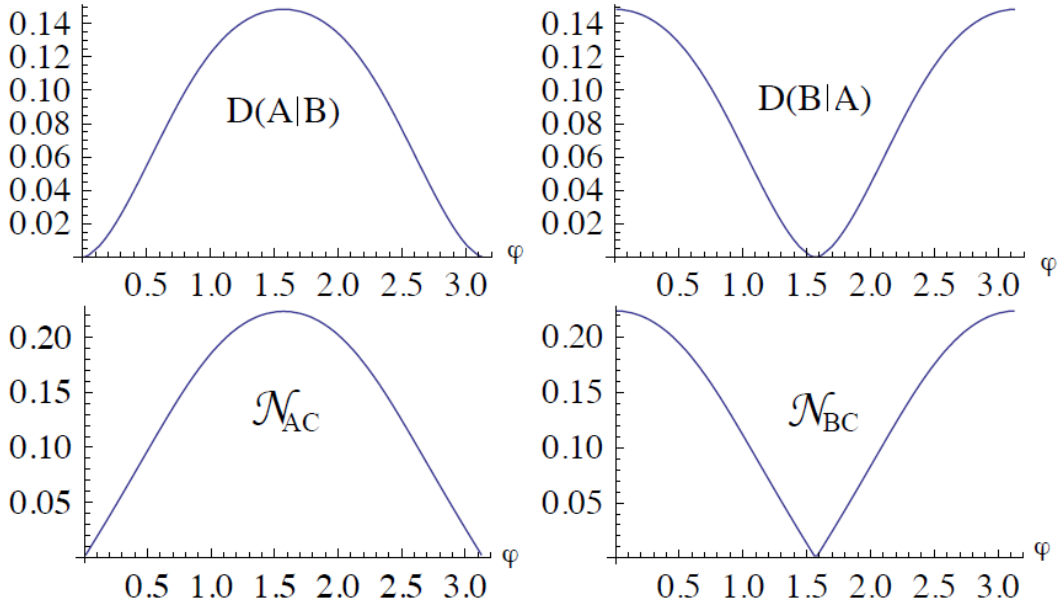


Figure 4.2: The behavior of discord and bipartite negativity as we move in the (α, β) plane along a trajectory of constant tripartite entanglement $\pi_{ABC} = 0.2$. $\varphi \in [0, 2\pi)$ is a variable used to parameterize the trajectory through (α, β) space.

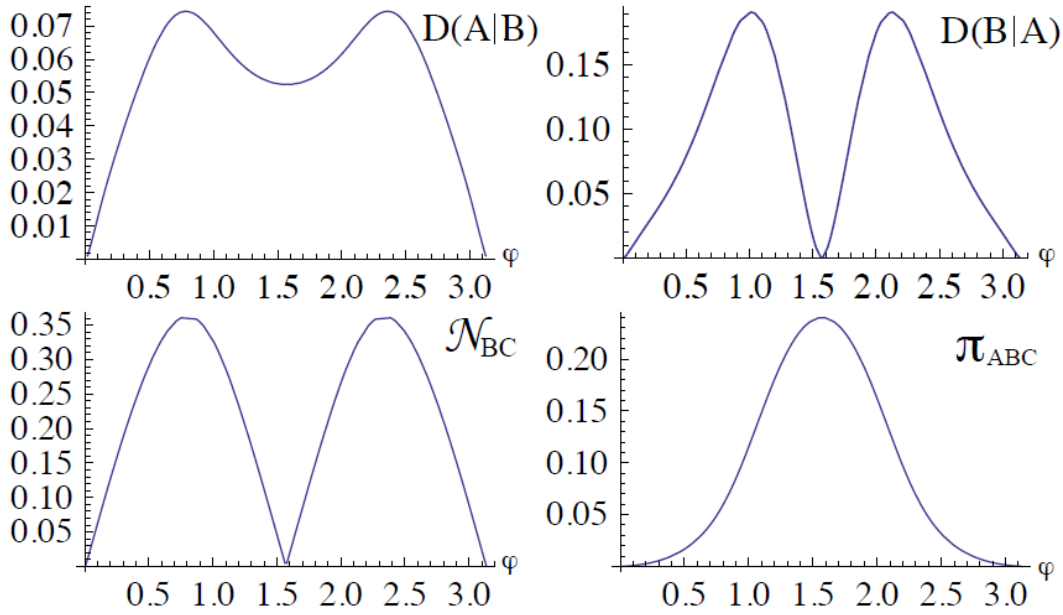


Figure 4.3: The behavior of discord, negativity, and π-tangle as we move in the (α, β) plane along a trajectory of constant bipartite entanglement $\mathcal{N}_{AC} = 0.1$. $\varphi \in [0, 2\pi)$ is a variable used to parameterize the trajectory through (α, β) space.

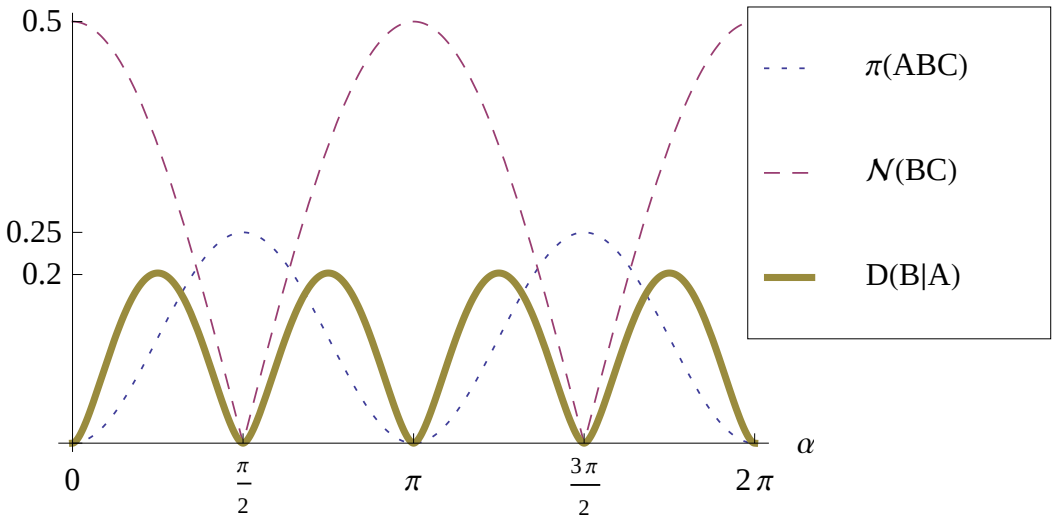


Figure 4.4: Graphs showing discord and entanglements in pure 3-qubit state with $c_1 = c_2 = \frac{1}{\sqrt{2}}$ and $|\beta\rangle = |1\rangle$. $\pi(ABC)$ represents the tripartite entanglement as measured by the pi-tangle and $\mathcal{N}(BC)$ is the entanglement between BC as measured by the negativity.

the value for ζ (Eq. 4.19) becomes

$$\zeta = c_1 c_2^* \langle 0|\beta\rangle \left(\sum_{k=1}^{d} \langle k|\alpha\rangle |k\rangle \langle 0| \right) \otimes |1\rangle \langle 0| \tag{4.28}$$

where d is the dimension of $|\alpha\rangle$. Therefore, the if and only if statement about AC separability becomes (see Appendix B for proof)

$$\rho_{AC} \text{ is separable iff } \{\langle 0|\beta\rangle = 0 \text{ or } |\alpha\rangle \propto |0\rangle\}. \tag{4.29}$$

The exact same statement (Eq. 4.24) about tripartite entanglement holds.

It turns out these if and only if statements about zero discord are not true in general for higher rank states. Consider, for example, the rank-three state

$$\rho_{AB} = |c_1|^2 |0\rangle \langle 0| \otimes |0\rangle \langle 0| + |c_2|^2 |0\rangle \langle 0| \otimes |1\rangle \langle 1| + |c_3|^2 |1\rangle \langle 1| \otimes |1\rangle \langle 1|$$

which has zero discord. Its purification with a 3 dimensional system

$$|\psi_{ABC}\rangle = c_1 |0\rangle \otimes |0\rangle \otimes |0\rangle + c_2 |0\rangle \otimes |1\rangle \otimes |1\rangle + c_3 |1\rangle \otimes |1\rangle \otimes |2\rangle$$

clearly is not separable on any of its bipartitions. The state on AC is

$$\rho_{AC} = |c_1|^2 |0\rangle \langle 0| \otimes |0\rangle \langle 0| + |c_2|^2 |0\rangle \langle 0| \otimes |1\rangle \langle 1| + |c_3|^2 |1\rangle \langle 1| \otimes |2\rangle \langle 2| + \chi + \chi^\dagger$$

where

$$\chi = c_2 c_3^* |0\rangle \langle 1| \otimes |1\rangle \langle 2|$$

which is clearly not separable (for a more rigorous argument, see Appendix C). Therefore, zero discord does not imply AC separable or zero tripartite entanglement in this case.

4.4 Generalizing the results

We make use of the following theorem, originally proven in [32]

Theorem. *If a system ABC is in a pure state $|\psi_{ABC}\rangle$, then the following equality holds*

$$D(B|A) = S(A) - S(C) + E(BC) \tag{4.30}$$

where S is the von Neumann entropy and E is the entanglement of formation.

Proof This can be proven quite easily by choosing a set $\{(p_i, |\psi^i_{BC}\rangle)\}$ such that $\rho_{BC} = \sum_i p_i |\psi^i_{BC}\rangle \langle\psi^i_{BC}|$ for which $E(BC) = \sum_i p_i S(Tr_C(|\psi^i_{BC}\rangle \langle\psi^i_{BC}|))$ and noticing that there must exist a measurement on A, $\{E^a_A\}$, which leaves the BC system in the state $|\psi^a_{BC}\rangle \langle\psi^a_{BC}|$ with probability p_a and hence leave the B system in state $\rho_{B|A=a} = Tr_C(|\psi^a_{BC}\rangle \langle\psi^a_{BC}|)$. From the definition of discord we have

$$\begin{aligned} D(B|A) = I(A:B) - J(B|A) &= S(A) - S(AB) + S(B|A) \\ &\leq S(A) - S(C) + \sum_a p_a S(\rho_{B|A=a}) \\ &= S(A) - S(C) + E(BC). \end{aligned}$$

The entropy $S(AB)$ is equal to $S(C)$ since ABC is in a pure state. On the other hand, choose the measurement $\{E^a_A\}$ on A which minimizes $S(B|\{E^a_A\})$. Since the ABC system is in a pure state and the E^a_A must all be proportional to rank-one projectors, we know that outcome a will leave system BC in a pure state $|\psi^a_{BC}\rangle$ and happen with probability p_a. Therefore we have a set $\{(p_a, |\psi^a_{BC}\rangle)\}$ such that $\rho_{BC} = \sum_a p_a |\psi^a_{BC}\rangle \langle\psi^a_{BC}|$. The state of the B system after the measurement on A is $\rho_{B|A=a} = Tr_C(|\psi^a_{BC}\rangle \langle\psi^a_{BC}|)$

$$\begin{aligned} E(BC) &\leq \sum_a p_a S(\rho_{B|A=a}) \\ &= S(B|A) \\ &= D(B|A) - S(A) + S(C). \end{aligned}$$

Putting these two inequalities together proves the theorem. ∎

Since there is nothing which distinguishes A, B or C we can also write down equations for the other discords in the system. For example, by simply interchanging letters we get

$$D(B|C) = S(C) - S(A) + E(AB) \tag{4.31}$$

and

$$D(C|A) = S(A) - S(B) + E(BC) \tag{4.32}$$

which gives us two new equalities, which are discussed in more detail in [33]

$$D(B|A) + D(B|C) = E(AB) + E(BC) \tag{4.33}$$

and

$$D(B|A) - D(C|A) = S(B) - S(C). \tag{4.34}$$

The first can be interpreted as the following: "Given an arbitrary tripartite pure system, the sum of all possible bipartite entanglement shared with a particular subsystem, as given by the entanglement of formation, cannot be increased without increasing, by the same amount, the sum of all discord shared with this same subsystem.". In our case, AB is separable so $E(AB) = 0$. This means that if BC is separable, Eq. 4.33 tells us that $D(B|A) = D(B|C) = 0$ since discord is non-negative. If tripartite entanglement is zero, then at least one of the subsystems A, B or C must be in a pure state. If A is in a pure state then $|\psi_{ABC}\rangle = |\psi_A\rangle \otimes |\psi_{BC}\rangle$ and so

$$\rho_{AB} = Tr_C(|\psi_{ABC}\rangle \langle\psi_{ABC}|) = |\psi_A\rangle \langle\psi_A| \otimes \rho_B \tag{4.35}$$

which is a product state so $D(B|A) = 0$. A similar argument for B can be made, and if C is pure then so is AB and its discord is therefore equal its entanglement which is zero. Therefore, for arbitrary separable systems AB, we have

$$D(B|A) = 0 \text{ if } \{BC \text{ is separable or } ABC \text{ has no tripartite entanglement}\} \tag{4.36}$$

The *only if* direction is not true in general, as was shown in Section 4.3.3. Another simple example where this fails is any product state in which both A and B are mixed: $\rho_{AB} = \rho_A \otimes \rho_B$. Clearly this state has neither classical nor quantum correlations. Purifying this state may be achieved by purifying ρ_A and ρ_B individually to end up with the state $|\psi_{AC}\rangle \otimes |\psi_{BD}\rangle$. If we consider the CD system as the third system, then this state clearly contains both bipartite and tripartite entanglement.

Even though the two-way implication for zero discord fails in general, the one direction which is true tells us something about the nature of correlations in a separable state: in order for such a state to have any correlations, classical or quantum, its purification must contain tripartite entanglement. Furthermore, if one wishes those correlations to have any quantum nature, this requires the purification to have bipartite entanglement AC and/or BC.

4.4.1 Gaussian states

Pure states exhibit the property that they have classical correlations, only when they have quantum correlations. That is, their classical correlations are equal to

their entanglement or, equivalently, their discord since they are pure states. This is because a pure state $|\psi_{AB}\rangle$ is separable only when it is also a product state $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$. Another set of states which also exhibit a similar property are the so-called *two-mode Gaussian* states. They have zero discord if and only if the two modes are in a product state. This property was first suggested in [34] and later proven in [35]. This is somewhat surprising since Gaussian states are often considered to be the "most classical" of the quantum states, and yet it is impossible for them to contain correlations which are only classical, in the sense of quantum discord.

Consider a pure three-mode Gaussian system ABC where the AB system is in a separable, mixed state. There is no point in considering AB pure since the property just discussed is trivially true. The following statement will be proven later, but first, we discuss its implications:

$$AB \text{ is in a product state} \iff ABC \text{ has no tripartite entanglement} \tag{4.37}$$

From this result, we can make two immediate observations. First, the property proven in [35] says that, for a two-mode Gaussian state ρ_{AB},

$$D(A|B) = 0 \iff \rho_{AB} = \rho_A \otimes \rho_B \iff D(B|A) = 0$$

which means the result in Section 4.4 has a two-way implication for Gaussian states. Namely, $D(A|B) = 0$ if and only if AC separable or no tripartite entanglement. Second, this gives a clear picture as to why zero discord in a Gaussian state implies that it is in a product state. Recall from Section 4.4 that tripartite entanglement in the purification is required for any correlations to be present in AB, classical or quantum, and the further addition of bipartite entanglement in the purification is what allows these correlations to have a quantum nature. But in this case, it is impossible to have tripartite entanglement without automatically having bipartite entanglement:

$$\begin{aligned} AC \text{ separable} \implies D(A|B) = 0 &\implies \rho_{AB} = \rho_A \otimes \rho_B \\ &\implies \text{no tripartite entanglement} \end{aligned} \tag{4.38}$$

with a similar statement for BC separable. Therefore, having tripartite entanglement implies both AC and BC are entangled! It is now clear why any correlations between A and B must be quantum.

In the following, we will not go into any detail about Gaussian states. Everything we use to prove Eq. 4.37 can be found in [36] in more detail. Consider the covariance matrix of a pure three-mode Gaussian state in standard form:

$$\sigma_{ABC} = \begin{bmatrix} \sigma_A & \gamma_{AB} & \gamma_{AC} \\ \gamma_{AB}^T & \sigma_B & \gamma_{BC} \\ \gamma_{AC}^T & \gamma_{BC}^T & \sigma_C \end{bmatrix} \tag{4.39}$$

where

$$\gamma_{ij} = \begin{bmatrix} e_{ij}^+ & 0 \\ 0 & e_{ij}^- \end{bmatrix} \tag{4.40}$$

$$\sigma_i = \begin{bmatrix} \nu_i & 0 \\ 0 & \nu_i \end{bmatrix}. \tag{4.41}$$

The σ_is are 2×2 covariance matrices for the ith mode of the three-mode Gaussian state and, in their standard form, are written in terms of $\nu_i = \sqrt{\det\sigma_i}$. These ν_i are all greater or equal 1 with equality if and only if system i is in a pure state. The 2×2 matrices γ_{ij} encode the information about the correlations between system i and system j. These can be written in terms of the covariance matrices $\{\sigma_k\}$

$$e_{ij}^{\pm} \equiv \frac{1}{4\sqrt{\nu_i \nu_j}} \left(S_{ij}^- \pm S_{ij}^+ \right) \tag{4.42}$$

where

$$S_{ij}^{\pm} = \sqrt{[(\nu_i \pm \nu_j)^2 - (\nu_k - 1)^2][(\nu_i \pm \nu_j)^2 - (\nu_k + 1)^2]}\,, \; k \neq i, j. \tag{4.43}$$

With this information at hand, we can prove our statement. Note that one of the directions is trivial: no tripartite entanglement $\implies$ $A(BC)$ or $(AC)B$ separable $\implies$ AB is in a product state. To prove the other direction, we use the fact that the AB system is in a product state if and only if $\gamma_{AB} = 0$ which is equivalent to $e_{AB}^{\pm} = 0$, and so

$$e_{AB}^{\pm} = 0 \implies S_{AB}^{\pm} = 0 \implies \nu_A = 1 \text{ or } \nu_B = 1. \tag{4.44}$$

The statement $\nu_A = 1$ or $\nu_B = 1$ means either system A or B is in a pure state, which means exactly that either $A(BC)$ or $(AC)B$ is separable $\implies$ no tripartite entanglement.

4.4.2 Remote activation of entanglement

These results are directly related to the protocol of remote entanglement activation. This protocol enables a system C to locally activate bipartite entanglement between two systems A and B if ABC has tripartite entanglement. For example, consider the three qubit GHZ state, which possesses tripartite but no bipartite entanglement:

$$|\psi_{ABC}\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$$

It is possible to perform an operation on the third qubit C so that the first two qubits A and B are entangled. This can be seen through our results in the following way: Recall that discord $D(A|C)$ can be increased by local non-unitary operations on C. In particular, if we apply the map $|0\rangle \to |0\rangle$ and $|1\rangle \to (|0\rangle + |1\rangle)/\sqrt{2}$ on C, then the AC system will have discord, i.e. $D(A|C) > 0$. Thus we can immediately conclude that, since $D(A|C) > 0$, AB must have entanglement. Since the tripartite entanglement is reduced through this process, an attractive interpretation of this is that the tripartite entanglement present in the system has been redistributed away from ABC and injected into AB. Notice that this description is true for arbitrary systems ABC, not just qubits. The result in Section 4.4 says that if $D(A|C)$ is non-zero (and AC separable), then entanglement AB must be non-zero. $D(A|C)$ can always be made non-zero through local non-unitary operations (see Section 3.2).

The ability to remotely activate entanglement is a useful tool, and our criteria presented above can easily be used in general to determine when such an action is possible.

Chapter 5

Conclusion

In this thesis, we found a relationship between the quantum discord in a separable, mixed state and the entanglement structure in its purification. We found that, for certain classes of states such as rank-two and two-mode gaussian states, a state being discordant is equivalent to its purification having both tripartite and bipartite entanglement. The discord $D(A|B)$ in the case of a rank-two pair of qubits is perfectly monotonic with the entanglement AC. This allows us to understand the asymmetry of quantum discord in terms of entanglement monogamy: as the entanglement AC increases, the entanglement BC decreases, and the associated discords are monotonic with these. We find that, even though the entanglement in the BC system does not affect the nullity of discord $D(A|B)$, it does play a role as we explore the dependence of discord on tripartite entanglement. We expect the same behavior for general rank-two states and this should be possible to verify.

We also find a sufficient condition for zero discord in a general separable state based on the nullity of tripartite and bipartite entanglement in its purification. This result can be applied to the protocol for remote entanglement activation by noticing that discord may be increased via local non-unitary operations, thus increasing an initially null discord implies we have increased entanglement somewhere else in the purification. It turns out that the lack of tripartite entanglement implies that the state on AB contains no correlations at all. The absence of bipartite entanglement means there is no discord, i.e. quantum correlations. This tells us that tripartite entanglement is required to have correlations of any type, while bipartite entanglement is required for these correlations to have a quantum nature. This provides a nice explanation as to why Gaussian states have the prop-

erty that they have no discord only when they are in a product state. We show that Gaussian states have the property that they are without tripartite entanglement if bipartite entanglement is zero. This means that any correlations between A and B must have a quantum nature.

There may exist natural and potentially useful notions of n-partite discord for $n > 2$, which in turn can be expressed in terms of n and $n+1$ partite entanglements of a larger system. This may even help disentangle the structure of multipartite entanglement in general. We leave this as possible future work. Also, it should be possible and very interesting, also for practical purposes, to investigate the Hamiltonians, i.e. the types of interactions, which give rise to the structures of discord and entanglement.

Bibliography

[1] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, 9th Edition, 2007

[2] W. H. Zurek, *Decoherence and the transition from quantum to classical*, arXiv:quant-ph/0306072

[3] A. Einstein, B. Podolsky, N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777-780 (1935).

[4] L. C. Céleri, J. Maziero, R. M. Serra, *Theoretical and experimental aspects of quantum discord and related measures*, arXiv:1107.3428 [quant-ph]

[5] R. F. Werner, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A **40**, 4277 (1989).

[6] C. Bennett, *et. al.*, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. 70, 1895 (1993).

[7] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, arXiv:quant-ph/9508027

[8] R. Cleve, J. Watrous, *Fast parallel circuits for the quantum Fourier transform*, arXiv:quant-ph/0006004

[9] M. B. Plenio, S. Virmani, *An introduction to entanglement measures*, arXiv:quant-ph/0504163

[10] M. Horodecki, *Entanglement measures*, Quantum Information and Computation, Vol. 1, No. 1 (2001) 3-26

[11] A. Peres, *Separability Criterion for Density Matrices*, Phys. Rev. Lett. **77**, 1413 (1996)

[12] M. Horodecki, P. Horodecki and R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Phys. Lett. A. **223**, 1 (1996)

[13] G. Vidal and R.F. Werner, *A computable measure of entanglement*, arXiv:quant-ph/0102117

[14] W. K. Wootters, *Entanglement of Formation of an Arbitrary State of Two Qubits*, Phys. Rev. Lett. **80**, 2245 (1998).

[15] B. M. Terhal, *Is Entanglement Monogamous?*, arXiv:quant-ph/0307120

[16] Y. Ou and H. Fan, *Monogamy inequality in terms of negativity for three-qubit states*, Phys. Rev. A. **75**, 062308 (2007)

[17] F. F. Fanchini, M. C. de Oliveira, L. K. Castelano, M. F. Cornelio, *Why the Entanglement of Formation is not generally monogamic*, arXiv:1110.1054 [quant-ph]

[18] R. Horodecki, P. Horodecki, M.Horodecki and K. Horodecki, *Quantum entanglement*, arXiv:quant-ph/0702225

[19] H. Ollivier & W. H. Zurek, *Quantum Discord: A Measure of the Quantumness of Correlations*, Phys. Rev. Lett. **88**, 017901 (2001).

[20] K. Modi *et. al.*, *The classical-quantum boundary for correlations: Discord and related measures*, arXiv:1112.6238 [quant-ph]

[21] M. Piani, *The problem with the geometric discord*, arXiv:1206.0231 [quant-ph]

[22] S. Luo, *Quantum discord for two-qubit systems*, Phys. Rev. A **77**, 042303 (2008)

[23] B. Dakic, V. Vedral and C. Brukner, *Necessary and Sufficient Condition for Nonzero Quantum Discord*, Phys. Rev. Lett. **105**, 190502 (2010)

[24] A. Datta, *Studies on the Role of Entanglement in Mixed-state Quantum Computation*, arXiv:0807.4490v1 [quant-ph]

[25] E. Knill & R. Laflamme, *Power of One Bit of Quantum Information*, Phys. Rev. Lett. **81**, 5672-5675 (1998).

[26] M. Gu *et. al.*, *Observing the operational significance of discord consumption*, Nature Physics, **8**, 671 (2012)

[27] A. Ambainis, L. J. Schulman, and U. V. Vazirani, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (ACM Press, New York, 2000), p. 697.

[28] A. Datta, S. T. Flammia, and C. M. Caves, *Entanglement and the power of one qubit*, Phys. Rev. A 72, 042316 (2005).

[29] A. Datta, A. Shaji, and C. M. Caves, *Quantum Discord and the Power of One Qubit*, Phys. Rev. Lett. 100, 050502 (2008).

[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, *Mixed State Entanglement and Quantum Error Correction*, arXiv:quant-ph/9604024

[31] E. G. Brown, E. J. Webster, E. M.-Martinez, A. Kempf, *Purified discord and multipartite entanglement*, arXiv:1212.3275 [quant-ph]

[32] M. Koashi and A. Winter, *Monogamy of quantum entanglement and other correlations*, Phys. Rev. A 69, 022309 (2004).

[33] Felipe F. Fanchini, *et. al.*, *Conservation law for distributed entanglement of formation and quantum discord*, Phys. Rev. A **84**, 012313 (2011)

[34] G. Adesso and A. Datta, *Quantum versus Classical Correlations in Gaussian States*, Phys. Rev. Lett. **105**, 030501 (2010).

[35] S. Rahimi-Keshari, C. M. Caves and T. C. Ralph, *Singular probability distribution of shot-noise driven systems*, Phys. Rev. A. **87**, 012119 (2013)

[36] G. Adesso and F. Illuminati, *Entanglement in continuous-variable systems: recent advances and current perspectives*, J. Phys. A: Math. Theor. **40**, 7821 (2007)

[37] A. Ferraro *et. al.*, *Almost all quantum states have nonclassical correlations*, Phys. Rev. A. **81**, 052318 (2010)

[38] M. Piani *et. al.*, *All Nonclassical Correlations Can Be Activated into Distillable Entanglement*, Phys. Rev. Lett. **106**, 220403 (2011)

[39] T. K. Chuan *et. al.*, *Quantum Discord Bounds the Amount of Distributed Entanglement*, Phys. Rev. Lett. **109**, 070501 (2012)

[40] V. Madhok and A. Datta, *Quantum correlations in two interacting atom ensembles*, Int. J. Mod. Phys. B. **27**, 1245041, (2013)

[41] M. de Almeida, *et. al.*, *Entanglement-free certification of entangling gates*, arXiv:1301.7110 [quant-ph]

Appendix A

A property of the partial transpose

We prove that, given $|\psi_A\rangle$,$|\psi_B\rangle$,$|\phi_A\rangle$ and $|\phi_B\rangle$, it is true that

$$\langle\psi_A| \otimes \langle\psi_B| (T \otimes I)(O_{AB}) |\phi_A\rangle \otimes |\phi_B\rangle = \langle\phi_A^*| \otimes \langle\psi_B| O_{AB} |\psi_A^*\rangle \otimes |\phi_B\rangle \qquad \text{(A.1)}$$

where $(T \otimes I)(O_{AB})$ is the partial transpose on the operator O_{AB} and $*$ denotes the complex conjugate.

Proof The operator O_{AB} has the general form

$$O_{AB} = \sum_{ijkl} c_{ij}^{kl} |i\rangle \langle j|_A \otimes |k\rangle \langle l|_B . \qquad \text{(A.2)}$$

Its partial transpose is

$$(T \otimes I)(O_{AB}) = \sum_{ijkl} c_{ij}^{kl} |j\rangle \langle i|_A \otimes |k\rangle \langle l|_B . \qquad \text{(A.3)}$$

and therefore

$$\begin{aligned}
\langle\psi_A| \otimes \langle\psi_B| (T \otimes I)(O_{AB}) |\phi_A\rangle \otimes |\phi_B\rangle &= \sum_{ijkl} c_{ij}^{kl} \langle\psi_A|j\rangle \langle i|\phi_A\rangle \langle\psi_B|k\rangle \langle l|\phi_B\rangle \\
&= \sum_{ijkl} c_{ij}^{kl} \langle\phi_A^*|i\rangle \langle j|\psi_A^*\rangle \langle\psi_B|k\rangle \langle l|\phi_B\rangle \\
&= \langle\phi_A^*| \otimes \langle\psi_B| O_{AB} |\psi_A^*\rangle \otimes |\phi_B\rangle
\end{aligned}$$

∎

Appendix B

Proof of ρ_{AC} separability

Here we prove that the more general (Eq. 4.16 with arbitrary states $|\alpha\rangle$ and $|\beta\rangle$)

$$\rho_{AC} = |c_1|^2 |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |c_2|^2 |\alpha\rangle\langle\alpha| \otimes |1\rangle\langle 1| + (\chi + \chi^\dagger) \tag{B.1}$$

where $\chi = \gamma + \zeta$ and

$$\gamma = c_1 c_2^* \langle 0|\beta\rangle \langle 0|\alpha\rangle |0\rangle\langle 0| \otimes |1\rangle\langle 0| \tag{B.2}$$

$$\zeta = c_1 c_2^* \langle 0|\beta\rangle \left(\sum_{j=1}^{d} \langle j|\alpha\rangle |j\rangle\langle 0| \right) \otimes |1\rangle\langle 0| \tag{B.3}$$

is separable if and only if $\zeta = 0$. We show that the partial transpose $(T \otimes I)(\rho_{AC})$ is not a positive operator if $\zeta \neq 0$ (Peres criterion, Thm. 2.5.2).

Proof Consider the vector

$$|\psi\rangle = |\alpha^{*\perp}\rangle \otimes |1\rangle + t\,|k\rangle \otimes |0\rangle \tag{B.4}$$

where $|\alpha^{*\perp}\rangle$ is *any* vector perpendicular to $|\alpha^*\rangle$ (the complex conjugate of $|\alpha\rangle$), $|k\rangle$ is any one of $k = 1, 2, ..., d$ and t is an arbitrary complex number. Taking the expected value of the operator $(T \otimes I)(\rho_{AC})$ gives (omitting tensor products $\otimes$ for

brevity, $|a\rangle \otimes |b\rangle \to |a,b\rangle$)

$$\begin{aligned}
&\langle\psi| (T\otimes I)(\rho_{AC}) |\psi\rangle \\
&= |c_1|^2 \langle\psi|0,0\rangle \langle 0,0|\psi\rangle + |c_2|^2 \langle\psi|\alpha^*,1\rangle \langle\alpha^*,1|\psi\rangle + \langle\psi| (T\otimes I)(\chi+\chi^\dagger) |\psi\rangle \\
&= \langle\psi| (T\otimes I)(\zeta+\zeta^\dagger) |\psi\rangle + \langle\psi| (T\otimes I)(\gamma+\gamma^\dagger) |\psi\rangle \\
&= \langle\psi| (T\otimes I)(\zeta) |\psi\rangle + \langle\psi| (T\otimes I)(\zeta^\dagger) |\psi\rangle + \langle\psi| \gamma+\gamma^\dagger |\psi\rangle \\
&= \langle\psi| (T\otimes I)(\zeta) |\psi\rangle + \langle\psi| (T\otimes I)(\zeta^\dagger) |\psi\rangle \\
&= \langle\psi| (T\otimes I)(\zeta) |\psi\rangle + \langle\psi| (T\otimes I)(\zeta)^\dagger |\psi\rangle \\
&= 2Re\left[\langle\psi| (T\otimes I)(\zeta) |\psi\rangle\right]
\end{aligned}$$

Expanding this last term gives us

$$\begin{aligned}
\langle\psi| (T\otimes I)(\zeta) |\psi\rangle &= \langle a^{*\perp},1| (T\otimes I)(\zeta) |a^{*\perp},1\rangle \\
&\quad + t \langle a^{*\perp},1| (T\otimes I)(\zeta) |k,0\rangle \\
&\quad + t^* \langle k,0| (T\otimes I)(\zeta) |a^{*\perp},1\rangle \\
&\quad + |t|^2 \langle k,0| (T\otimes I)(\zeta) |k,0\rangle \\
&= \langle a^\perp,1| \zeta |a^\perp,1\rangle \\
&\quad + t \langle k,1| \zeta |a^\perp,0\rangle \\
&\quad + t^* \langle a^\perp,0| \zeta |k,1\rangle \\
&\quad + |t|^2 \langle k,0| \zeta |k,0\rangle
\end{aligned}$$

where we have used the property from Appendix A in the second equality. The first term $\langle a^\perp,1| \zeta |a^\perp,1\rangle$ and the last term $|t|^2 \langle k,0| \zeta |k,0\rangle$ are zero. Finally, this means that

$$\langle\psi| (T\otimes I)(\rho_{AC}) |\psi\rangle = 4Re\left[t \langle k,1| \zeta |a^\perp,0\rangle\right]. \tag{B.5}$$

This must be non-negative for all t in order for the partial transpose of ρ_{AC} to be a positive operator. The only way for that to happen is if

$$\langle 1,k| \zeta |a^\perp,0\rangle = c_1 c_2^* \langle 0|\beta\rangle \langle k|\alpha\rangle \langle 0|\alpha^\perp\rangle = 0. \tag{B.6}$$

Since $|\alpha^\perp\rangle$ is an arbitrary vector perpendicular to the state $|\alpha\rangle$, it must be either $\langle 0|\beta\rangle = 0$ or $\langle k|\alpha\rangle = 0$. To see this more clearly, suppose $|\alpha\rangle = \sum_{j=0}^{d} c_j |j\rangle$. Then setting $|\alpha^\perp\rangle = |0\rangle - c_0^* |\alpha\rangle$ we get

$$\langle\alpha|\alpha^\perp\rangle = \langle\alpha|0\rangle - c_0^* \langle\alpha|\alpha\rangle = c_0^* - c_0^* = 0 \tag{B.7}$$

and

$$\langle 0|\alpha^{\perp}\rangle = \langle 0|0\rangle - c_0^* \langle 0|\alpha\rangle = 1 - |c_0|^2. \tag{B.8}$$

This is zero only when $|c_0| = 1$, i.e. $|\alpha\rangle \propto |0\rangle \implies \langle k|\alpha\rangle = 0$. We have thus shown that $\zeta = 0$ is necessary for separability. Of course it is sufficient since, in this case,

$$\begin{aligned}\rho_{AC} &= |c_1|^2 |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |c_2|^2 |\alpha\rangle\langle\alpha| \otimes |1\rangle\langle 1| + (\gamma + \gamma^\dagger) \\ &= |c_1|^2 |0\rangle\langle 0| \otimes \rho_0 + |c_2|^2 |\alpha\rangle\langle\alpha| \otimes |1\rangle\langle 1|\end{aligned}$$

where we have just factored out a $|0\rangle\langle 0|$ from $\gamma + \gamma^\dagger$. ∎

Appendix C

Sufficient condition for entanglement

The method used in Appendix B can be extended to provide a sufficient condition for entanglement which is easy to verify. We may write an arbitrary state in the basis $\{|a,b\rangle\}$ as

$$\rho = \sum_{ab} p_{ab} |a,b\rangle \langle a,b| + \chi \tag{C.1}$$

where χ denotes the off diagonal terms of ρ. Consider now the vector

$$|\psi\rangle = |j^*,k\rangle + t\,|m^*,n\rangle \tag{C.2}$$

where t is any complex number and $|j,k\rangle \neq |m,n\rangle$. The expected value of the partial transpose of ρ is

$$\begin{aligned}\langle\psi| (T\otimes I)(\rho) |\psi\rangle =& \sum_{ab} p_{ab} \langle\psi|a^*,b\rangle \langle a^*,b|\psi\rangle + \langle\psi| (T\otimes I)(\chi) |\psi\rangle \\ =& p_{jk} + |t|^2 p_{mn} + \langle\psi| (T\otimes I)(\chi) |\psi\rangle \end{aligned} \tag{C.3}$$

We calculate the third term using the property from Appendix A

$$\begin{aligned}\langle\psi|\,(T\otimes I)(\chi)\,|\psi\rangle &= \langle j^*,k|\,(T\otimes I)(\chi)\,|j^*,k\rangle \\ &\quad + t\,\langle j^*,k|\,(T\otimes I)(\chi)\,|m^*,n\rangle \\ &\quad + t^*\,\langle m^*,n|\,(T\otimes I)(\chi)\,|j^*,k\rangle \\ &\quad + |t^2|\,\langle m^*,n|\,(T\otimes I)(\chi)\,|m^*,n\rangle \\ &= \langle j,k|\,\chi\,|j,k\rangle \\ &\quad + t\,\langle m,k|\,\chi\,|j,n\rangle \\ &\quad + t^*\,\langle j,n|\,\chi\,|m,k\rangle \\ &\quad + |t^2|\,\langle m,n|\,\chi\,|m,n\rangle\end{aligned}$$

The first term $\langle j,k|\,\chi\,|j,k\rangle$ and the last term $|t^2|\,\langle m,n|\,\chi\,|m,n\rangle$ are zero since χ contains only off-diagonal terms. Therefore, since ρ is self-adjoint $\implies \chi = \chi^\dagger$, we have

$$\langle\psi|\,(T\otimes I)(\chi)\,|\psi\rangle = 2Re\left[t\,\langle m,k|\,\chi\,|j,n\rangle\right]. \tag{C.4}$$

Since $\langle m,k|\cdot|j,n\rangle$ is zero on the diagonal, we can rewrite Eq. C.4 as

$$\langle\psi|\,(T\otimes I)(\chi)\,|\psi\rangle = 2Re\left[t\,\langle m,k|\,\rho\,|j,n\rangle\right]. \tag{C.5}$$

We want Eq. C.3 to be negative for some s. Setting $y = \langle m,k|\,\rho\,|j,n\rangle$ and $t = y^*s$ where s is a real number, we have

$$\langle\psi|\,(T\otimes I)(\rho)\,|\psi\rangle = p_{jk} + s^2|y|^2p_{mn} + 2|y|^2s. \tag{C.6}$$

If this is to be negative, there should be multiple roots, so

$$|y|^2 > p_{jk}p_{mn} \tag{C.7}$$

guarantees there is entanglement. More explicitly

$$|\,\langle m,k|\,\rho\,|j,n\rangle\,|^2 > \langle j,k|\,\rho\,|j,k\rangle\,\langle m,n|\,\rho\,|m,n\rangle \tag{C.8}$$

implies the state ρ is entangled. Clearly this is not true for $j = m$ or $k = n$ since we get the same inequality whether we use ρ or $(T\otimes I)(\rho)$ and ρ is positive. We can therefore say that a state ρ is entangled if Eq. C.8 is true for some $j \neq m$, $k \neq n$. It

should be noted that $(T \otimes I)(\rho)$ might not be a positive operator and *not* satisfy Eq. C.8 for any j, k, m, n, thus making this weaker than Peres' criterion. It is, however, a much quicker check (no eigenvalues or partial transposes involved) of whether it *might* be positive. If M and N are the dimensions of each subsystem, then brute forcing this check takes at most $M(M-1)N(N-1)/2 \approx (MN)^2$ operations, while finding the eigenvalues would take $\approx (MN)^3$, incurs numerical error, plus it takes time to perform the partial transpose. Also, in our case, where we deal with a lot of variables, it makes sense to use something like this rather than symbolically evaluating eigenvalues.

An example making use of this condition is: an arbitrary pure two-qubit state $a|0,0\rangle + b|0,1\rangle + c|1,0\rangle + d|1,1\rangle$ is entangled if $|a||d| \neq |b||c|$ which is obtained immediately by choosing $|j,k\rangle = |0,0\rangle$ and $|m,n\rangle = |1,1\rangle$, followed by $|j,k\rangle = |0,1\rangle$ and $|m,n\rangle = |1,0\rangle$.

As another example, consider the Bell-diagonal states introduced in Eq. 4.5. Choosing again $|j,k\rangle = |0,0\rangle$ and $|m,n\rangle = |1,1\rangle$ followed by $|j,k\rangle = |0,1\rangle$ and $|m,n\rangle = |1,0\rangle$ gives the two inequalities

$$(p_1 - p_2)^2 > (p_3 + p_4)^2 = (1 - p_1 - p_2)^2$$
$$(p_3 - p_4)^2 > (p_1 + p_2)^2 = (1 - p_3 - p_4)^2.$$

If one of the $p_k > 1/2$ then one of these inequalities is satisfied. Therefore if any of the p_k are greater than $1/2$ this implies entanglement.

Finally, we reprove the result from Appendix B: let $|j,k\rangle = |0,1\rangle$ and $|m,n\rangle = |r,0\rangle$ where $r \neq 0$. We have $\langle r,0|\,\rho_{AC}\,|r,0\rangle = 0$ and $\langle r,1|\,\rho_{AC}\,|0,0\rangle = c_1 c_2^* \langle 0|\beta\rangle \langle r|\alpha\rangle$ so ρ_{AC} separable implies either $\langle 0|\beta\rangle = 0$ or $\langle r|\alpha\rangle = 0$.