Alma Mater Studiorum · Università di Bologna

Scuola di Scienze
Corso di Laurea Magistrale in Fisica

ACCESSIBLE INFORMATION IN A TWO-QUBIT SYSTEM THROUGH THE QUANTUM STEERING ELLIPSOIDS FORMALISM

Relatore:
Prof.ssa Elisa Ercolessi

Presentata da:
Lorenzo Catani

Correlatore:
Prof. Terence Rudolph

Sessione I
Anno Accademico 2013/2014

To Alice, my family and my friends.

Contents

List of Figures

List of Tables

Abstract

Capire come ottenere l'informazione accessibile, cioè quanta informazione classica si può estrarre da un processo quantistico, è una delle questioni più intricate e affascinanti nell'ambito della teoria dell'informazione quantistica. Nonostante l'importanza della nozione di informazione accessibile non esistono metodi generali per poterla calcolare, esistono soltanto dei limiti, i più famosi dei quali sono il limite superiore di Holevo e il limite inferiore di Josza-Robb-Wootters.

La seguente tesi fa riferimento a un processo che coinvolge due parti, Alice e Bob, che condividono due qubits. Si considera il caso in cui Bob effettua misure binarie sul suo qubit e quindi indirizza lo stato del qubit di Alice in due possibili stati. L'obiettivo di Alice è effettuare la misura ottimale nell'ottica di decretare in quale dei due stati si trova il suo qubit.

Lo strumento scelto per studiare questo processo va sotto il nome di *quantum steering ellipsoids formalism*. Esso afferma che lo stato di un sistema di due qubit può essere descritto dai vettori di Bloch di Alice e Bob e da un ellissoide nella sfera di Bloch di Alice generato da tutte le possibili misure di Bob. Tra tutti gli stati descritti da ellissoidi ce ne sono alcuni che manifestano particolari proprietà, per esempio gli stati di massimo volume.

Considerando stati di massimo volume e misure binarie si è riuscito a trovare un limite inferiore all'informazione accessibile per un sistema di due qubit migliore del limite inferiore di Josza-Robb-Wootters. Un altro risultato notevole e inaspettato è che l'intuitiva e giustificata relazione *distanza tra i punti nell'ellissoide - mutua informazione* non vale quando si confrontano coppie di punti "vicine" tra loro e lontane dai più distanti.

Acknowledgements

I really thank my supervisors Elisa Ercolessi and Terry Rudolph for the opportunity they gave me of undertaking a very stimulating project. I thank Elisa Ercolessi for the support and the competence. I thank Terry Rudolph for the great help and the smart suggestions during all the project.

Thanks are also due to Antony Milne and his precious advices and to everyone in the controlled quantum dynamics group for all the pleasant conversations.

Bologna, 18 July 2014 Lorenzo Catani

Introduction

The scope of this work is studying the accessible information in a two-qubit system. The tool used to reach this goal is the so called *quantum steering ellipsoids formalism.*

This work considers a quantum process in which two parties, Alice and Bob, share two qubits and Bob performs a binary measurement (*i.e.* composed of only two measurement elements) on his qubit so that he collapses Alice's qubit state to two possible states. The aim of Alice is to perform the best measurement in order to find in which state her qubit is. The accessible information is defined as the maximum of the mutual information over all the possible measurement schemes that Bob and Alice can undertake. It quantifies how much classical information can be extracted in a quantum process.

The accessible information issue is one of the most intricate and intriguing in quantum information theory since it captures in a quantitative way what Nielsen and Chuang ([11]) called *the hidden nature of quantum information* and, despite the importance of this notion, almost nothing is known about it. Unfortunately no general methods for calculating the accessible information are known; only a variety of important bounds exists, either on the number of the optimal measurement elements (*e.g.* the Davies theorems [2]) or on the accessible information itself (*e.g.* the Holevo upper bound and the Josza-Robb-Wootters lower bound [3]). The difficulties of obtaining an exact expression of the accessible information derive from the maximization procedure over all possible measurements and from the trascendent logarithmic expression of the mutual information. In order to face the problem of considering all possible measurement schemes it is necessary to develop a method to find the optimal measurement scheme, since it is not possible to explore all the possible ones. The maximum likelihood discrimination allows to find this optimal measurement scheme in a very simple and intuitive way. This method is strictly related to the concept of *trace distance*, a measure of the distinguishability between states which corresponds to the euclidean distance in the two-qubit systems case.

The idea of this work is studying the accessible information through the geometric tool of the quantum steering ellipsoids. As the state of a qubit system can be represented by a vector inside the Bloch sphere, the state of a two qubit system can be represented, according to the quantum steering ellipsoid formalism, by Alice's Bloch vector, Bob's Bloch vector and an ellipsoid inside Alice's Bloch sphere (or Bob's one). In particular it results that if Bob performs all the possible measurements on his qubit, the set of Bloch vectors that Bob can collapse Alice's qubit to forms an ellipsoid inside her Bloch Sphere: the quantum steering ellipsoid. The power of this formalism derives from the fact that the steering ellipsoid encodes all the correlation features of a two qubit state through geometrically (and so intuitively) describing it and its properties in three dimensions. It is a geometrical picture of correlations. This formalism has allowed to reach many results, for example one remarkable theorem states that a state

of a two qubit system is separable if and only if its steering ellipsoid fits inside a tetrahedron that fits inside the sphere; this is called the *nested tetrahedron condition*. There are some special states represented by steering ellipsoids with a null Bob's Bloch vector and an Alice's Bloch vector coinciding with the centre of the ellipsoid which show particular properties; they are called canonical states and they are derivable from a unitary transformation on the original state. Not all the steering ellipsoids describe physical states, there exist a limit on the volume of the ellipsoid over which the state represented by that ellipsoid is no more physical. This work deals with states corresponding to maximum volume ellipsoids, which are a special class of canonical states and show particular symmetries (they touch the Bloch sphere in only one point).

The assumptions of binary measurements and maximum volume states allows to treat quite easy calculations and formulate geometrical intuitions. The key intuition of this thesis is that, according to the maximum likelihood discrimination and the trace distance, the maximum of the mutual information should arise for the states described by the furthest points on the steering ellipsoid, since they are the most distant and so the closest to be distinguishable. Calculations in spherical coordinates show it is true and so the mutual information for the furthest points of the steering ellipsoid is a lower bound to the accessible information of a two-qubit system. Moreover it is a tighter lower bound than the already known Josza-Robb-Wootters lower bound and by considering the famous Holevo upper bound the conclusion of this work is that the accessible information for a two qubit system is included between the mutual information of the furthest points and the Holevo quantity.

Beyond this result, a quite unexpected behaviour emerges: the relation between the euclidean distance between points of the ellipsoid and the corresponding mutual information does not always hold. Sometimes the mutual information for a couple of closer points is greater than the mutual information for a couple of further points. In general it happens when the distance difference between the two couples is small and these couples are far from the couple of furthest points of the steering ellipsoid. Another special behaviour arises by considering couples of opposite points inside the steering ellipsoid: in the case that the distance of a couple of closer points becomes greater than the distance of a couple of further points, the value of the centre at which it arises does not coincide with the value of the centre at which their mutual information inverts. These special behaviours probably show that the maximum likelihood discrimination, based on the trace distance concept, is not the appropriate measure of distinguishability between quantum states for the current scope. It works only for quite distant couples of points. It may be appropriate to use a method related to another measure of distinguishability between states, such as the fidelity ([11]).

The next step in order to improve the knowledge of the accessible information and the lower bound consists of studying the case of measurements composed of three elements and refering to the more general canonical states. This fact implies more difficult calculations and a the necessity of a new method to substitute the optimal measurement one in order to maximise the mutual information. A common method in this case is the so called *pretty good measurements* method ([4]); a new one is the *SIC measurements* method ([8]).

The thesis is divided in four chapters and two appendices:

The first chapter consists of a review of all the basic notions of information theory. It begins with the definition of the Shannon and Von Neumann entropy in order to define the mutual information for two random variables. This work deals with the classical mutual information, which has a precise physical meaning, and

not with the quantum mutual information, which, as the state-of-art stands at the present, is only a mathematical expression. After that, the postulates of quantum mechanics are enunciated, especially the one refering to the quantum measurements, with a particular emphasis on the POVM and PVM. It is later introduced the distinguishability problem which is strictly related to the impossibility of cloning non orthogonal quantum states. All these concepts are a bridge for defining the maximum likelihood discrimination method and the accessible information in a quantum process, which is the main protagonist of all the work. All the results known about the accessible information are reported, *i.e.* bounds on the number of the optimal measurement elements (*e.g.* the Davies theorems) or on the accessible information itself (*e.g.* the Holevo upper bound and the Josza-Robb-Wootters lower bound).

The second chapter consists of a review of the quantum steering ellipsoids formalism. After a rapid discussion of how to represent two-qubit states and a section on the notations used, the key idea about the construction of steering ellipsoids is formulated. A very important class of states is given by the canonical states and a whole section describes them and their derivation. Canonical states are very suitable in order to illustrate the main results of the steering ellipsoids formalism: the nested tetrahedron condition, which provides a geometrical and intuitive way of viewing if a state is either entangled or separable; the physicality conditions, which point out the mathematical and geometrical constraints for a state and its ellipsoid to describe a physical state; a list of other results such as an inequality for the entanglement monogamy (strictly stronger than the famous Coffman-Kundu-Wootters inequality for the monogamy of concurrence), a generalization of the Euler theorem of classical geometry, a theorem of incomplete steering (it is possible that sometimes some decompositions of Alice's state are inaccessible) and a specific dissertation on the volume of the ellipsoids. The volume of an ellipsoid is a very important property of the ellipsoid describing the state and among the canonical states a very remarkable class of states is given by the maximum volume states, which show particular symmetries. This work deals always with maximum volume states.

The third chapter derives all the results of this thesis. It begins with the calculation of the mutual information in spherical coordinates for the couple of furthest and nearest points on the surface of the steering ellipsoid. This is the starting point for a gradual generalization to couples of opposite points on the surface of the steering ellipsoid and then couples of points inside the steering ellipsoid. In the latter case it is assumed, in order to make the calculations less cumbersome, that the points within a couple belong to an ellipsoid inside the steering one. A large dissertation on the results obtained, expecially the one highlighting a special behaviour of the mutual information for close couples of points far from the furthest one, concludes this chapter. A last chapter (4) points out the key concepts of this work and further considerations.

The appendices illustrate a theorem about Alice's qubit state decomposition in the case that Bob performs a binary PVM on his qubit and the maximum likelihood method in the case that Bob performs a binary POVM on his qubit.

Chapter 1

Introduction to accessible information

1.1 Basic Definitions

The purpose of this chapter is to precisely define the *accessible information.*

Before defining the accessible information, it is necessary to define the basic quantities and functions of the information theory, thus starting from the classical Shannon entropy and the quantum Von Neumann entropy.

1.1.1 Shannon entropy

The function *Shannon entropy* gives a quantitative meaning to the concept of (classical) information. It measures the amount , or the size, of the message that carries the information in a communication scenario which involves two parties transmitting a message (*e.g.* Alice and Bob). Consider the following game to understand the intuition behind it :

Bob hides a coin in one of eight equal boxes and Alice has to find where he hid it (figure 1.1). The information which Alice needs is precisely *where the coin is.*

This information can be quantified in an objective way through counting the number of *binary questions* Alice needs to ask in order to obtain the *missing information.* "Binary questions" mean those questions that halve the set of possible outcomes in two equally probable parts, in this case:

1st question - Is the coin in the right half of the eight boxes?

Figure 1.1: Game of the eight boxes and a coin. Which is the best strategy involving binary questions to obtain where the coin is hidden? The answer is the strategy that halves the set of possible outcomes in two equally probable parts in each question.

2nd question - Is the coin in the right half of the remaining four boxes?

3rd question - Is the coin in the right half of the remaining two boxes?

It results the smartest way to get the knowledge on where the coin is, *i.e.* involving the minor number of questions possible.

Alice would gain the same amount of information (which is fixed in the very description of the game) also with other questioning strategies (asking more questions), but it is clearly better to define the missing information in terms of the binary strategy.

Note that the amount of missing information is intrinsecally determinated by the probability distribution, in this case: {1/8,1/8,1/8,1/8,1/8,1/8,1/8,1/8}.

This game can be generalized through refering to a random variable X (the game in the current case) with probability distribution $p_i = \{p_1, ..., p_n\}$.

The measure of the missing information can be defined through the dimensionless and non negative function called *Shannon entropy* [1] :

$$H(p) = -\sum_{i=1}^{n} p_i \log p_i, with \sum_{i=1}^{n} p_i = 1. \tag{1.1}$$

It can also be interpreted either as a measure of the Alice uncertainty before she learns the value of X, or as a measure of how much information Alice has gained after she learns the value of X.

The amount of information in the previous example can be calculated through considering the logarithm to base two: $H(p) = log_2 8 = 3$. Hence 3 *bits* is the numerical value of the missing information in this game.

Note that adopting the binary smartest strategy Alice gains the maximum information from each question, *i.e.* one bit of information. Therefore the amount of missing information is equal to the number of questions Alice needs to ask to obtain the required information.

Note that it satisfies the following properties in order to undestand better why the Shannon entropy is the appropriate function to measure the missing information:

1. H is *continuous* in all his variables; it is expected that by making a small change in the probabilities,then the change in the uncertainty should also be small.

2. H reaches its *maximum* if all $p_i = 1/n$ and the maximum value is a monotonic increasing function of n (it is ugual to $\log d$, where d is the number of outcomes); it is expected a zero missing information in the case there is the certainty of an outcome and, on the contrary, a maximum missing information in the case all the outcomes are equiprobable. It has to increase if the number of possible outcomes increases.

3. H is the weighted sum of the individual values of H of each event composing the random variable (the questions in the game example); the missing information must *depend only on the distribution* $p_i = \{p_1, ..., p_n\}$ and must not depend on the strategy Bob chooses.

The great importance of the Shannon entropy derives firstly from the fact that it can be used to quantify the resources needed to store information (Shannon's noiseless coding theorem).

Consider the following communication process:

[1] It is sometimes written as $H(X)$ too.

Bob wants to send a message to Alice. The message is composed by a string of n characters, written in an alphabet of k letters $\{a_1, ..., a_k\}$. Every letter has a probability $p(a_i)$ to appear into the message, with the condition $\sum_{i=1}^{k} p(a_i) = 1$.

Supposing the simplest case of a binary alphabet ("1" with probability p and "0" with probability *1-p*) it is easy to see that the Shannon entropy quantifies the maximum possible compression of the message without loss of information:

assuming a large n, a typical message will contain $n(1-p)$ characters "0" and np "1". The number of possible messages written in this form is $\binom{n}{np}$ and the Stirling formula $logn! = nlogn - n$ implies

$\log \binom{n}{np} = n\log n - n - np\log np + np - n(1-p)\log n(1-p) + n(1-p) = n[-(p\log p + (1-p)\log(1-p))] = nH(p)$.

This can be easily generalized to the case of k letters, thus obtaining the Shannon entropy related to the distribution $X = \{x, p(x)\}$.

Hence Bob can compress his message of n classical states into $nH(X)$ bits. The Shannon entropy quantifies the optimal compression that may be achieved through considering a classical message.

1.1.2 Von Neumann entropy

The Shannon entropy can be generalized to the quantum case through considering quantum states instead of classical states, *i.e.* density operators[2] instead of probability distributions.

The Shannon entropy is repalced by the Von Neumann entropy:

$$S(\rho) = -\rho \log \rho, \tag{1.2}$$

where ρ is a quantum state and the logarithm is taken to base two. It can also be rewritten as:

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x, \tag{1.3}$$

where λ_x are the eigenvalues of ρ.

The main properties of the Von Neumann entropy are:

1. It is *continuous*.
2. It is *non-negative*. It is zero if and only if the state is pure.
3. Its *maximum* is $\log d$ in a d-dimensional Hilbert space. It reaches its maximum if and only if the system is in the completely mixed state $\mathbb{I}/d$.
4. If a composite system AB is in a pure state, then $S(A) = S(B)$.
5. It is a *concave* function of its inputs, *i.e.* $S(\sum_i p_i\rho_i) \geq \sum_i p_i S(\rho_i)$.

It can be now considered the previous classical process in the quantum version, *i.e.* considering a quantum source instead of a classical one. While the latter is defined by X (the set of probabilities $\{p_i\}$), the former is defined by the density operator (the set of probabilities $\{p_i\}$ and the corresponding quantum states $|\psi_i\rangle$).

[2] Positive unitary trace operators associated to some ensembles, such as $\{p_i, |\psi_i\rangle\}$. In the case it is a pure state it is also idempotent.

It results that if Bob wants to involve the best compression on his message of n quantum states, then he compresses it into $nS(X)$ qubits. In general the Von Neumann entropy for $\{p_i\}$ is strictly smaller than the Shannon entropy for $\{p_i\}$; the equality holds only if the states $|\psi_i\rangle$ are orthogonal. If, for example, a quantum source produces the state $|0\rangle$ with probability p and $(|0\rangle + |1\rangle)/2$ with probability *1-p*, then the compression involves less than $nH(p, 1-p)$ qubits per use of the source.

Therefore the Von Neumann entropy quantifies the optimal compression that may be achieved: the content of incomprimible information into a quantum source just like the Shannon entropy quantifies the content of incomprimible information in a classical source.

1.1.3 Mutual Information

The accessible information is defined through a procedure of maximization of the so called *mutual information*. This section contains the precise definition of the mutual information in both the classical and quantum case, through considering an abstract scenario in which no communication processes are involved, but probability distributions only.

The classical case

Suppose to consider two random variables X and Y , *e.g.* two games described by two probability distributions, respectively p_i and q_j, with $i = 1, 2, ..., n$ and $j = 1, 2, ..., m$, and to investigate the common information between these two variables.

Let us write the Shannon entropy defined on the joint probability $P(i, j)$ of occurence of the events X_i and Y_j :

$$H(X, Y) = -\sum_{i=1}^{n} P(i, j) \log P(i, j). \tag{1.4}$$

The probabilities p_i and q_i can be written as $p_i = -\sum_{j=1}^{m} P(i, j)$ and $q_j = -\sum_{i=1}^{n} P(i, j)$. This implies

$$H(X) + H(Y) \geq H(X, Y), \tag{1.5}$$

i.e.

$$-\sum_{i,j} P(i, j) \log \sum_{j=1}^{m} P(i, j) - \sum_{i,j} P(i, j) \log \sum_{i=1}^{n} P(i, j) \geq -\sum_{i,j} P(i, j) \log P(i, j).$$

It derives from the property of any two probability distributions:

$$-\sum_{i=1}^{n} q_i \log q_i \leq -\sum_{i=1}^{n} q_i \log p_i. \tag{1.6}$$

The equality holds in the case of two independent variables, *i.e.* $P(i, j) = p_i \cdot p_j$. While for two dependent sets of outcomes the missing information in the joint experiment (X, Y) will always be smaller than the missing information in the two experiments separately.

Let us now introduce *the conditional entropy*, linked to the conditional probabilities $P(j/i) = P(i,j)/p_i$:

$$\begin{aligned} H(Y/X) &= -\sum_i p_i \sum_j P(j/i) \log P(j,i) \\ &= -\sum_{i,j} P(i,j) \log P(j/i) \\ &= -\sum_{i,j} P(i,j) \log P(i,j) + \sum_{i,j} P(i,j) \log p_i \\ &= H(X,Y) - H(X). \end{aligned} \tag{1.7}$$

Therefore $H(X,Y)$ can be written as

$$\begin{aligned} H(X,Y) &= H(X) + H(Y/X) \\ &= H(Y) + H(X/Y). \end{aligned} \tag{1.8}$$

Hence, from (1.5) and (1.7), the missing information of Y can never increase by knowing X :

$$H(Y/X) \leq H(Y). \tag{1.9}$$

It is the average uncertainty about the value of Y when the value of X is known. Note that it is different to calculate the information in X given a single event Y_j, and the information on X given Y.

The main protagonist of this work, *the mutual information*, is defined as

$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y). \tag{1.10}$$

It can also be written as

$$\begin{aligned} H(X:Y) &= H(Y) - H(Y/X) \\ &= H(X) - H(X/Y). \end{aligned} \tag{1.11}$$

It is a measure of the extent of the dependence between X and Y or the average reduction in missing information about X that results from knowing Y and *vice versa*. Hence it is the measure of how much information X and Y have in common. The mutual information satisfies the following properties:

1. $H(X:Y) \geq 0$
2. $H(X:Y) = H(Y:X)$
3. $H(X:X) = H(X)$
4. $H(X:Y) = 0$ if the two experiments are independent.
5. $H(X:Y) \leq H(Y)$, with equality if and only if Y is a function of X, *i.e.* $H(Y/X) = 0$.

The first property can be easily proved:

$$\begin{aligned} H(X:Y) &= -\sum_{i=1}^{n} p_i \log p_i - \sum_{j=1}^{m} p_j \log p_j + \sum_{i,j} P(i,j) \log P(i,j) \\ &= \sum_{i,j} P(i,j) \log \frac{P(i,j)}{p_i \cdot p_j} \\ &= \sum_{i,j} P(i,j) \log f(i,j). \end{aligned} \tag{1.12}$$

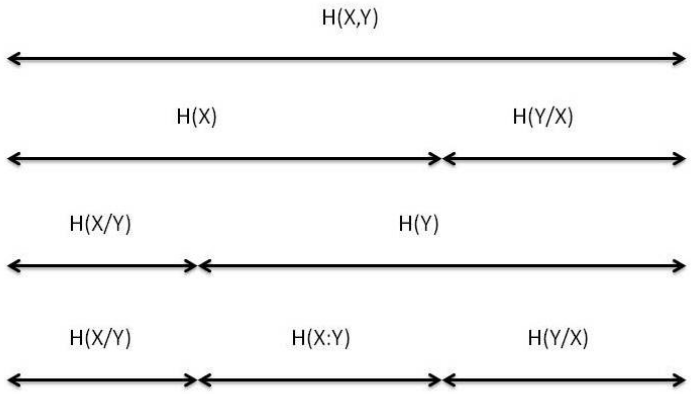


Figure 1.2: Relationship between the quantities $H(X), H(Y), H(X,Y), H(X:Y)$.

Where $f(i,j)$ is the correlation between the two events X_i and Y_j.

The other properties are obvious from the definition.

The definition can be straightforwardly generalized to the case of more-than-two variables.

Figure 1.2 represents the relations between the Shannon entropy, the conditional entropy and the mutual information.

The quantum case

Generalize the Shannon entropies defined above to the quantum case.

The joint quantum entropy for a composite quantum system composed by two parts A and B can be naively defined as

$$S(A,B) \equiv -tr(\rho^{AB} \log(\rho^{AB})), \tag{1.13}$$

where ρ^{AB} is the density matrix of the system AB.

Therefore *the quantum conditional entropy* and *the quantum mutual information* are defined as

$$S(A/B) \equiv S(A,B) - S(B) \tag{1.14}$$

$$\begin{aligned} S(A:B) &\equiv S(A) + S(B) - S(A,B) \\ &= S(A) - S(A/B) = S(B) - S(B/A). \end{aligned} \tag{1.15}$$

It is important to stress that while the classical mutual information can be interpreted as a measure of the classical correlation in a given process, the quantum mutual information has not an operatively clear meaning.

The *accessible information* consists of a maximization of the mutual information over all possible measurement schemes. This is why the next section will discuss the quantum measurements.

1.2 Quantum measurements

Before stating the definition of quantum measurements, it is necessary to define the of *states* in quantum mechanics and their evolution.

1.2.1 Fundamental principles

The state of an isolated physical system is described by a unit vector in an Hilbert space, univocally determined up to a global phase factor $e^{i\theta}$. In the general case of a quantum system which state is not completely known it can be described through an ensemble of the possible state vectors: $\{p_i, |\psi_i\rangle\}$, where the p_i are the probabilities associated to the state vectors $|\psi_i\rangle$. Therefore the state of the system is defined through the density operator given by

$$\rho = \sum_i p_i \, |\psi_i\rangle \, \langle\psi_i| \, . \tag{1.16}$$

When all the probabilities are zero except one (so there is the certainty of the state of the system), the state is called *pure*, otherwise it is *mixed*. In the case of pure states the framework of density operators is not necessary, the *state vector* is enough to describe the state of the system.

The *qubit* is the physical system this work will deal with. A qubit (quantum bit) is the quantum generalization of a classical bit. While a bit is described by a state either 0 or 1, a qubit is described by a superposition of states

$$|\psi\rangle = \alpha \, |0\rangle + \beta \, |1\rangle \, , \tag{1.17}$$

where α and β are complex numbers such that $|\alpha|^2$ and $|\beta|^2$ are the probabilities of obtaining respectively$|0\rangle$ and $|1\rangle$ when the qubit is measured. Obviously it results $|\alpha|^2 + |\beta|^2 = 1$. The state of a qubit is a vector in a two-dimensional complex vector space, where $|0\rangle$ and $|1\rangle$ form an orthonormal basis for this vector space called *computational basis states*.

Figure 1.2 represents the relations between Shannon entropy, conditional entropy and mutual information.

The state of a qubit can be represented as a vector inside a sphere: the *Bloch sphere* (figure 1.3). This is possible because a qubit in a mixed state ρ (Hermitean 2×2 matrix) can be written in the Pauli basis [3] as

$$\rho = c_0 \mathbb{I} + \vec{c} \cdot \vec{\sigma}. \tag{1.18}$$

Note $tr\rho = 1$ implies $c_0 = \frac{1}{2}$ and so

$$\rho = \begin{pmatrix} \frac{1}{2} + c_z & c_x - ic_y \\ c_x + ic_y & \frac{1}{2} - c_z \end{pmatrix},$$

where $\vec{c}$ has real components since $\rho = \rho^\dagger$ and the determinant of the matrix is $det\rho = \frac{1}{4} - ||\vec{c}||^2 \geq 0$. Hence $||\vec{c}|| = \frac{1}{2}||\vec{n}|| \leq \frac{1}{2} \Rightarrow ||\vec{n}|| \leq 1$ and

$$\rho = \frac{\mathbb{I} + \vec{n} \cdot \vec{\sigma}}{2}. \tag{1.19}$$

$\vec{n}$ is a vector belonging to the unitary ray tridimentional sphere of the "Pauli space", *i.e.* the Bloch sphere. If $||\vec{n}|| = 1$, then the state is pure. If $||\vec{n}|| < 1$, then the state is mixed.

[3] Remember the Pauli matrices are given by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Their main properties are $\{\sigma_i, \sigma_j\} = 0$, ${\sigma_i}^2 = \mathbb{I}$ and $tr[\sigma_i] = 0$. $\mathbb{I}, \sigma_x, \sigma_y, \sigma_z$ form an orthonormal basis by considering the scalar product between matrices generated by the trace.

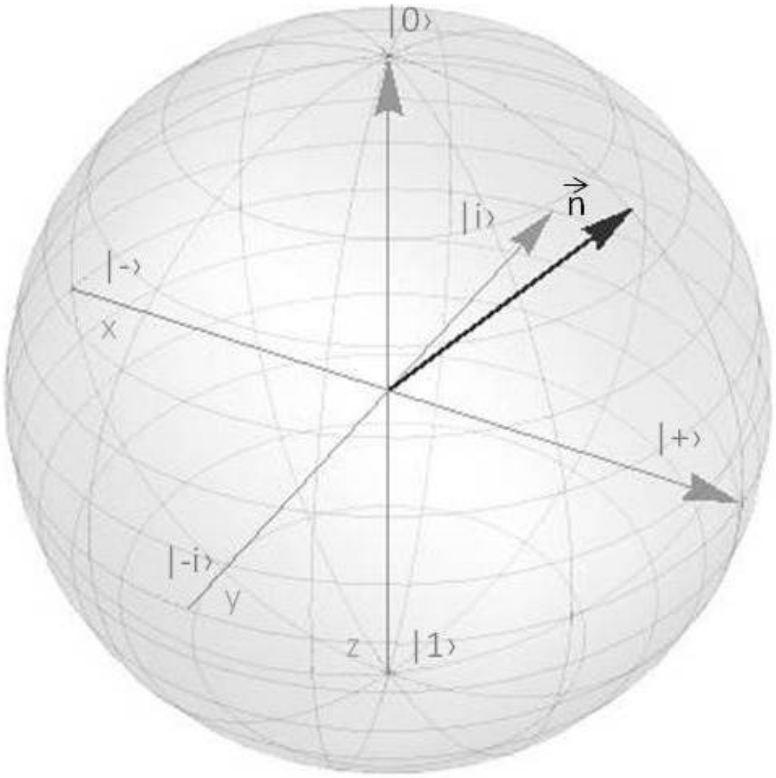


Figure 1.3: Bloch sphere. The vector $\vec{n}$ represents the state of a qubit. If $|\vec{n}| = 1$ the state is pure, if $|\vec{n}| < 1$ the state is mixed. The Bloch sphere is a geometrica tool which allows to intuitively study properties of the quantum system such as mixedness, coherence and dynamics.

The state of a composite physical system is the tensor product of the states composing the system:

$$\rho = \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n. \tag{1.20}$$

The evolution of a closed quantum system from a time t_1 to a time t_2 is described by a unitary trasformation $|\psi_i\rangle \to U|\psi_i\rangle$, hence

$$\rho' = U\rho U^\dagger, \tag{1.21}$$

where U depends only on the times t_1 and t_2.

The evolution is not unitary when the system interact with the observer's equipment (an external physical system which performs a measurement on the quantum system). Quantum measurements are described by a set of measurement operators $\{M_m\}$ acting on the Hilbert space of the system being measured and satisfying the completeness equation $\sum_m M_m^\dagger M_m = \mathbb{I}$, where m is the index of the possible measurement outcomes. The probability that m occurs is

$$p(m) = tr(M_m^\dagger M_m \rho), \tag{1.22}$$

where ρ is the state before the measurement. The state after the measurement is

given by

$$\rho' = \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)}. \tag{1.23}$$

For the case of a pure state described by the state vector $|\psi\rangle$ the results above can be replaced by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle \tag{1.24}$$

and

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{p(m)}}. \tag{1.25}$$

An example of quantum measurement is the measurement of a qubit in the computational basis, *i.e* described by the measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Suppose the state to measure is $|\psi\rangle = a|0\rangle + b|1\rangle$. Hence [4]:

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2,$$

$$p(1) = |b|^2,$$

$$|\psi'\rangle = \frac{M_0 |\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle,$$

$$|\psi''\rangle = \frac{M_1 |\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle.$$

By ignoring the "modulo one" multipliers because quantum states are defined up to a global phase factor, the states after the measurements effectively are $|0\rangle$ an $|1\rangle$.

Two specific quantum measurements can be now discussed: the *PVM* and *POVM.*

1.2.2 Projective measurements and POVM

The projective or Von Neumann measurements (often called PVM, Projective-Valued Measures) are a special class of measurements described by an observable M, *i.e.* an Hermitean operator on the Hilbert space of the system being observed. As every Hermitean operator, M can be write in its spectral decomposition:

$$M = \sum_m m P_m, \tag{1.26}$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. As in the previous case, the eigenvalue m is also the index indicating the possible outcomes.

The probability of obtaining the outcome m for the state ρ is

$$p(m) = tr(P_m \rho) \tag{1.27}$$

and the related state immediately after the measurement is

$$\rho' = \frac{P_m \rho}{p(m)}. \tag{1.28}$$

In the case of a pure state it results that

$$p(m) = \langle\psi| P_m |\psi\rangle \tag{1.29}$$

[4] Note M_0 and M_1 are hermitean operators.

and

$$|\psi'\rangle = \frac{P_m |\psi\rangle}{\sqrt{p(m)}}. \tag{1.30}$$

It is important to note that the general measurements described above reduce to PVM if the M_m are orthogonal projectors, *i.e.* Hermitean and such that $M_m M'_m = \delta_{mm'} M_m$. It is possible to refer to a PVM as the set of orthogonal projectors P_m satisfying $\sum_m P_m = \mathbb{I}$ and $P_m P'_m = \delta_{mm'} P_m$, without esplicitly writing the observable $M = \sum_m m P_m$. There also exists another way of refering to it as a *measure in basis* $|m\rangle$, where $|m\rangle$ form an orthogonal basis, refering to a PVM with projectors $P_m = |m\rangle \langle m|$.

It is useful to apply the above statements thus giving some examples of projective measurements: the measurements of the observables $\sigma_x, \sigma_y, \sigma_z$.

Let us write for example the measurement of σ_z on the state $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$, which gives the outcome $+1$ with probability $\langle +|0\rangle \langle 0|+\rangle = 1/2$ and outcome -1 with probability $1/2$.

This result derives from the fact that σ_z has eigenvalues $+1$ and -1 with corresponding eigenvectors $|0\rangle$ and $|1\rangle$. Therefore the spectral decompositions of all the Pauli matrices imply the possibility of performing measurements of a general observable $\vec{v} \cdot \vec{\sigma} = v_1\sigma_1 + v_2\sigma 2 + v_3\sigma 3$. These spectral decompositions are derivable from [5]:

$$\sigma_x |\pm\rangle = \pm |\pm\rangle \, , where \, |\pm\rangle = \frac{(|0\rangle \pm |1\rangle)}{\sqrt{2}} \tag{1.31}$$

$$\sigma_y |\pm i\rangle = \pm |\pm i\rangle \, , where \, |\pm i\rangle = \frac{(|0\rangle \pm i\,|1\rangle)}{\sqrt{2}} \tag{1.32}$$

$$\sigma_z |0\rangle = |0\rangle \, , \sigma_z |1\rangle = -|1\rangle \, where \, |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} and \, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.33}$$

We conclude about PVM noting that they are *repeatable*, *i.e.* if an observer performs a PVM obtaining m , then performing again the PVM he obtains m again without any change in the state.

The POVM formalism (Positive Operator-Valued Measure) is used when there is no interest in the post measurement state of the system. It consists of defining *POVM elements*

$$E_m = M_m^\dagger M_m, \tag{1.34}$$

where M_m is a generic measurement operator. Then, taking into account the general definitions of quantum measurements 1.2.1 and the completeness relation, it results that E_m is a positive operator such that $\sum_m E_m = \mathbb{I}$ and

$$p(m) = tr(E_m \rho). \tag{1.35}$$

The whole set $\{E_m\}$ is called *a POVM*. It is immediate to see that PVM are a special case of POVM where all E_m coincide with P_m.

PVM and POVM are fundamental notions for the following chapters.

[5] They are not the esplicitely spectral decompositions, but the eigenvalues equations only, because they are more suitable for the future applications.

1.3 The distinguishability problem

Accessing quantum information encoded in states about which we may have some prior information is strictly related to the indistinguishability of quantum non-orthogonal states and the impossibility of cloning a quantum state. This is why it is convenient to start considering the famous *no cloning theorem*. It states that is not possible to build a device which generates two copies of a given quantum state $|\psi\rangle$.

Suppose it is possible: prepare the arbitrary quantum state $|\psi\rangle$ and a 'virgin' state $|v\rangle$ through which it is possible to copy the state. Insert them in the special device, thus obtaining

$$|\psi\rangle |v\rangle \rightarrow |\psi\rangle |\psi\rangle .$$

Then perform the same operation in another arbitrary input state $|\psi'\rangle$, thus obtaining $|\psi'\rangle |v\rangle \rightarrow |\psi'\rangle |\psi'\rangle$. Now calculate the inner product of these two expressions (assuming $\langle v|v\rangle = 1$) and obtain $\langle\psi|\psi'\rangle = \langle\psi|\psi'\rangle^2$, *i.e.* either $\langle\psi|\psi'\rangle = 0$ or $\langle\psi|\psi'\rangle = 1$. However it contradicts the hypothesis on the arbitrariety of the states.

Note that it is possible to clone input states as $|0\rangle$ and $|1\rangle$. Therefore it is evident that the special behaviour of quantum states is linked to their non-orthogonality. If it is possible to clone an unknown quantum state it is possible to make many copies , perform some measurements and learn what it was. Moreover It is possible to measure the momentum of the first copy with high precision and also the position of the second copy with high precision, contradicting the uncertainty principle. However it has been proved that it is impossible.

1.3.1 Distinguishing non-orthogonal quantum states

The non-orthogonality of arbitrary quantum also states affects the capacity of distinguish them. Consider the following game involving two parties, Alice and Bob. Both parties know a fixed set of quantum states $\{|\psi_i\rangle\}$. Immagine Bob chooses one of these states $|\psi_i\rangle$ and gives it to Alice, whose task is to identify the index i of such a state.

If the states are orthonormal then Alice can perform a quantum measurement to distinguish them: she takes the measurement operators $M_i \equiv |\psi_i\rangle \langle\psi_i|$, one for each index i, and M_0 defined as the positive square root of $\mathbb{I} - \sum_{i\neq 0} |\psi_i\rangle \langle\psi_i|$ so that they satisfy the completeness relation. If Bob prepares the state $|\psi_i\rangle$ then Alice identifies the index i with probability $p(i) = \langle\psi_i| M_i |\psi_i\rangle = 1$.

On the other hand, if the states are not orthogonal, Alice cannot choose any measurement operators to distinguish them. Consider two of such states $|\psi_0\rangle$ and $|\psi_1\rangle$. The key point is that $|\psi_1\rangle$ can be decomposed into a non-zero component parallel to $|\psi_0\rangle$ and a non-zero component orthogonal to $|\psi_0\rangle$. Even by supposing Alice guesses the state was $|\psi_0\rangle$ when she observes an index j, then by considering the component of $|\psi_1\rangle$ parallel to $|\psi_0\rangle$, there is a non-zero probability of obtaining the result j when $|\psi_1\rangle$ is prepared, so sometimes Alice fails trying to identify which state was prepared.

This example implies the necessity to derive the fundamental limitation of distinguishing a pair of non-orthogonal states, by finding which are the best measurement operators to guess the state which is measured, *i.e* to maximize the probability of success in guessing it. This is why the next section will explain a procedure known as *maximum likelihood discrimination.*

1.3.2 Maximum Likelihood Discrimination

Consider the previous game in the case of only two states (prepared with a half of probability each):

$$|\psi_0\rangle = \cos(\frac{\alpha}{2})\,|0\rangle + \sin(\frac{\alpha}{2})\,|1\rangle$$
$$|\psi_1\rangle = \cos(\frac{\alpha}{2})\,|0\rangle - \sin(\frac{\alpha}{2})\,|1\rangle\,.$$

Alice wants to guess whether Bob has prepared either $|\psi_0\rangle$ or $|\psi_1\rangle$ through interacting with his qubit. She wants to reach the aim with as high a likelihood of success as possible.

Imagine Alice performs a PVM composed of two elements: $\{M_0, M_1\}$. If she obtains 0 (the M_0 outcome) she guesses $|\psi_0\rangle$.If she gets 1 (the M_1 outcome) she guesses $|\psi_1\rangle$. She wants to choose the best PVM elements in order to maximize the probability of success:

$$\begin{aligned} P(success) &= P(|\psi_0\rangle)P(success/\,|\psi_0\rangle) + P(|\psi_1\rangle)P(success/\,|\psi_1\rangle) \\ &= \frac{1}{2}\,\langle\psi_0|\,M_0\,|\psi_0\rangle + \frac{1}{2}\,\langle\psi_1|\,M_1\,|\psi_1\rangle \\ &= \frac{1}{2} + \frac{1}{2}(\langle\psi_0|\,M_0\,|\psi_0\rangle - \langle\psi_1|\,M_1\,|\psi_1\rangle) \\ &= \frac{1}{2} + Tr[M_0(|\psi_0\rangle\,\langle\psi_0| - |\psi_1\rangle\,\langle\psi_1|)], \end{aligned}$$

where in the second line it was considered $M_1 = \mathbb{I} - M_0$, as a consequence of the two-outcome measurement.

If we now evaluate the quantity $|\psi_0\rangle\,\langle\psi_0| - |\psi_1\rangle\,\langle\psi_1|$ in the computational basis, then

$$|\psi_0\rangle\,\langle\psi_0| - |\psi_1\rangle\,\langle\psi_1| = \sin(\alpha)\sigma_x.$$

Hence, according to the spectral decomposition of the $x-$Pauli matrix 1.2.2, the probability of success results

$$P(success) = \frac{1}{2} + \frac{1}{2}\sin\alpha Tr(\langle+|\,M_0\,|+\rangle - \langle-|\,M_0\,|-\rangle).$$

In order to maximise this quantity it is necessary to seek a M_0 that makes the term $\langle-|\,M_0\,|-\rangle$ as small as possible. So $M_0 = |+\rangle\,\langle+|$. Then

$$P^{max}(success) = \frac{1}{2} + \frac{1}{2}\sin\alpha. \tag{1.36}$$

When considering a mixed state of a qubit, by defining it through its Bloch vector it can be found an equivalent formulation. Label the Bloch vector of M_0 as $\vec{s}$ and so the Bloch vector of $M_1 = \mathbb{I} - M_0$ is $-\vec{s}$ (note that two orthogonal states are represented as two diametrically opposite vectors in the Bloch sphere). Label the Bloch vectors of the states, ρ_0 and ρ_1, Bob can prepare with equal probability as $\vec{r}_0$ and $\vec{r}_1$. Then the probability of success results

$$\begin{aligned} P(success) &= \frac{1}{2}Tr(\rho_0 M_0) + \frac{1}{2}Tr(\rho_1 M_1) \\ &= \frac{1}{2}\frac{1}{2}(1 + \vec{r}_0\mathbf{s}) + \frac{1}{2}\frac{1}{2}(1 - \vec{r}_1\vec{s}) \end{aligned}$$

$$= \frac{1}{2} + \frac{1}{4}\vec{s}(\vec{r}_0 - \vec{r}_1).$$

Therefore, considering that $\vec{s}$ is unitary because it represents a PVM [6] and that the purpose is to maximize this probability, then it is necessary to take $\vec{s}$ to be parallel to $\vec{r}_0 - \vec{r}_1$, and so

$$P^{max}(success) = \frac{1}{2} + \frac{1}{4}||\vec{r}_0 - \vec{r}_1||. \tag{1.37}$$

The *trace distance* between two qubit states appears in this formula: $D(\rho_0, \rho_1) = \frac{1}{2}||\vec{r}_0 - \vec{r}_1||$, that results to be half the ordinary Euclidean distance between the vectors on the Bloch sphere. The general definition of the trace distance between two quantum states is $D(\rho_0, \rho_1) = \frac{1}{2}|tr(\rho_0 - \rho_1)|$ and it reduces to the classical trace distance when ρ_0 and ρ_1 commute (because in this case they are diagonalizable in the same basis and it implies a difference only between the eigenvalues $\rho_{i_0}$and ρ_{i_1}): $D(\rho_0, \rho_1) = \frac{1}{2}\sum_i |\rho_{i_0} - \rho_{i_1}|$.

The best measurement operators to guess the qubit state, considered it can be either ρ_0 or ρ_1 (described respectively by the Bloch vectors $\vec{r}_0$ and $\vec{r}_1$) are given by the eigenvectors of $\rho_0 - \rho_1$, *i.e.* the operator Bloch vector $\vec{s}$ is parallel to $\vec{r}_0 - \vec{r}_1$. If the optimal measurement is a PVM, then the eigenvectors must be normalized, since they belong to the Bloch sphere surface, *i.e.* they are unit vectors (see B for a generalization). Figure 1.4 makes this reasoning more intuitive.

There are other state discrimination methods such as the *unambiguous discrimination* (*see* [12]) , but the maximum likelihood discrimination is the most useful for the future work. It will be often used in chapter 3.

1.4 Accessible information

Definition

Consider once again the game of subsection 1.3.1 when Bob preapares a quantum state ρ_X chosen from a fixed set $\{\rho_1, ..., \rho_n\}$ and gives it to Alice. Alice performs a quantum measurement on ρ^X and obtains the result Y, derived from the best guess she can do.

How much information has Alice gained from getting Y?

The mutual information $H(X : Y)$ between X and the measurement result Y 1.1.3 is a good function to measure it.

It is known that $H(X : Y) \leq H(X)$ and the inequality is saturated only if Alice can infer X from obtaining Y, so she wants to choose a measurement to obtain mutual information as close as possible to $H(X)$. Considering that, the *accessible information* is defined as *the maximum of the mutual information over all possible measurement schemes*. It is a measure of how well Alice can infer at the quantum state Bob gave to her.

The accessible information is an interesting quantity only in quantum theory because of the indistinguishability of non-orthogonal quantum states. [7] Try to understand why,

[6] In rough analogy, a POVM is to a PVM what a density matrix is to a pure state. A PVM is represented by a vector on the surface of the Bloch sphere. A POVM by a vector inside the Bloch Sphere. See 2.1.1 for a better understanding.

[7] Actually the accessible information makes sense also in the following *classical* case. Immagine Bob prepares the state 0 or 1 according to one of two possible probability distributions: either $\{p, 1-p\}$ or $\{q, 1-q\}$. Alice has to guess the probability distribution just from the knowledge the state Bob gives her. It is obvious it is not possible for Alice to obtain the answer with certainty. However this work will only refer to quantum theory in the future.

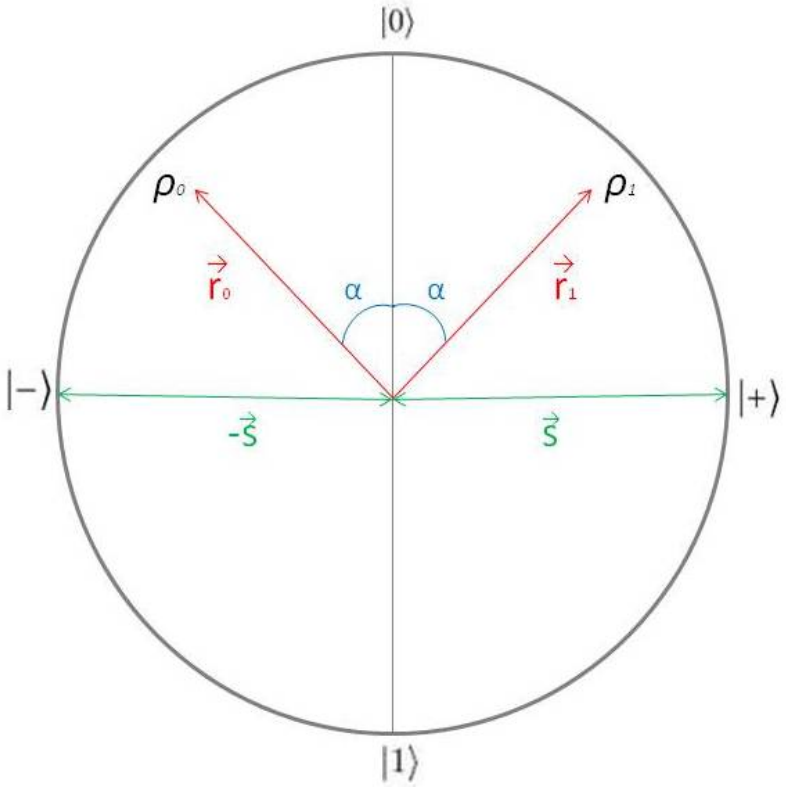


Figure 1.4: Maximum likelihood discrimination. Alice's optimal measurement ($\{\Pi, \mathbb{I} - \Pi\}$) to guess if the qubit state is either ρ_0 or ρ_1 (represented by state vectors $\vec{r}_0$ and $\vec{r}_1$) is given by the opposite Bloch vectors $\vec{s}$ and $-\vec{s}$, which are parallel to $\vec{r}_0 - \vec{r}_1$. Note that a vector inside the Bloch sphere makes sense only if it originates from the centre of the sphere. In the figure above we can see the case in which $\vec{r}_0 - \vec{r}_1$ is parallel to the x axis and so the optimal quantum measurement is the PVM in basis $|-\rangle$ and $|+\rangle$. In the case of pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ the Bloch vectors touch the surface of the sphere, however Alice's optimal measurement remains the same.

as it has already stated in the previous section, the accessible information is linked to "the indistinguishability of quantum non-orthogonal states and the impossibility of cloning a quantum state".

First of all note that if the two variables X and Y in the definition of the mutual information 1.1.3 are distinguishable then the mutual information reduces to $H(X)$ and if they are completely indistinguishable it reduces to 0. Then consider the *no cloning theorem*. Suppose Bob prepares one of two non-orthogonal quantum states $|\phi\rangle$ and $|\psi\rangle$ with probability p and $1 - p$ respectively. Assume Alice's accessible information about these states coincides with $H(p)$, *i.e* Alice is able to discriminate which is the state Bob has prepared. Then she can easily clone the states: after she has identified the state either $|\phi\rangle$ or$|\psi\rangle$ through the measurement, she can prepare as many copies as she wants of the state she has received from Bob. The no-cloning theorem is a consequence of the accessible information is always smaller than $H(p)$. *Vice versa* if she can clone states, she uses the *cloning device* to make as many copies as she wants of the state she

receives from Bob, obtaining either $|\phi\rangle^{\otimes n}$ or $|\psi\rangle^{\otimes n}$. In the limit of large n these states are always more orthogonal and so it is possible to distinguish them through PVM.

In conclusion the no-cloning theorem is equivalent to the statement the accessible information is always smaller than $H(p)$.

The accessible information is a really intriguing quantity as it quantifies how much classical information is recoverable in a quantum (and so "misterious") process. However it involves a really tricky issue, because of the difficulty in maximizing a logarithm expression. [8] and because of the lack of sufficiently powerful techniques for searching over all quantum measurement schemes (all POVM with arbitrary number of outcomes). Moreover it can be shown that it is a non linear and convex function on the set of all POVM's (*see* [5]). It results that only for extremely special systmes configuration it is possible to find an esplicit expression of the accessible information. [9] For the general case there only exist some results in the form of bounds:

1. bounds on the number of the optimal POVM elements (and outcomes),
2. bounds on the accessible information itself.

Some of them are illustrated below.

1. **The Davies Theorems**

   There exist a couple of theorems by Davies (*see* [2]) linked to the number of elements needed in an optimal POVM (*i.e. a POVM which maximizes the mutual information*).

   The first theorem states that there always exists an optimal POVM in a d-dimensional Hilbert space with n rank one operators where $d \leq n \leq d^2$. It is possible to formulate also a real version of this theorem (*i.e.* all states are real), stating that $n \leq \frac{d(d+1)}{2}$.

   The second theorem states that for a symmetric ensemble of states with irreducible representation σ there exists an optimal POVM which is a single orbit. This theorem can be reduced to the real version and can be generalized to the case of reducible representations (*see* [2]). This theorems has been studied by P. Shor, the first (*see* [16]) and T. Decker (*see* [2]) , the second, using special quantum states called *lifted trines*.

2. **Some Bounds** The most famous upper bound on the accessible information is certainly the *Holevo bound*. It states that:

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \tag{1.38}$$

   where $\rho = \sum_x p_x \rho_x$. The state ρ_X $(X = 1, \ldots, n)$ is the state prepared by Bob, with probabilities $p_0, \ldots, p_n$. Y is, as usual, the measurement outcome of the Alice's POVM.

[8] there exist other criteria for the quantum detection problem which are much simpler such as the minimization of specified Bayes costs (*see* [2]). However they are only useful when one has to reach a decision after performing a single quantum measurement (*see* [5]) .

[9] Maybe the less trivial example was formulated by M. Sasaki *et all* which have founded the optimal strategy for an ensemble of M qubit states with symmetry group Z_M, *i.e.* the group of integeres modulo M(bibiliography).

The most famous lower bound on the accessible information is the *Jozsa-Robb-Wootters bound*. It states that:

$$H(X:Y) \geq Q(\rho) - \sum_x p_x Q(\rho_x), \tag{1.39}$$

where $Q(\rho)$ is the a rather complicated quantity called the *subentropy* of ρ :

$$Q(\rho) = -\sum_{j=1}^{D} (\prod_{k \neq j} \frac{\lambda_j}{\lambda_j - \lambda_k}) \lambda_j \log \lambda_j, \tag{1.40}$$

where λ_j are the eigenvalues of ρ and D is the dimension of the Hilbert space of ρ (see [3] for further details).

These are the best bounds expressible solely in terms of ρ when ρ_x are pure states. It is possible to improve them including more details on the probabilities $p_0, \ldots, p_n$ and the density operators ρ_x themselves (*see* [3]).

Conclude this chapter noting that it is possible to define the *quantum* accessible information through considering the maximum of the *quantum* mutual information. However the next sections will always deal with the classical accessible information for quantum systems, because the puporse is to extracting the maximum *classical* information possible from a quantum process (between the two given variables X and Y).

The process analyzed in the next chapters consists of two parties, Alice and Bob, which share a pair of qubits. Bob performs measurements on his qubit and, in this way, he "steers" Alice's qubit to a certain state she wants to guess through quantum measurements. The aim consists of understanding which is the best measurement for Bob, and then for Alice, to maximize the mutual information in a binary case, *i.e.* the case in which Bob performs a measurement composed only by two elements.

However, before trying to calculate the accessible information, it is necessary to introduce a new and powerful theoretical tool to reach this purpose: the quantum steering ellipsoids formalism.

Chapter 2

Quantum steering ellipsoids

We have seen in chapter one that the Bloch sphere represents the state space of one qubit, which is described by a vector inside the sphere. The possibility of geometrically representing the state of a qubit allows to find new insights and intuitively understand fundamental features of the single qubit system. Is it possible to find such an intuitively representation for two qubit systems?

2.1 Representing two-qubit states

If the basic quantum unit for the information theory - the single qubit system - has an intuitively three-dimensional representation and it is described by the simple state 1.19, the basic quantum unit for the theory of bipartite quantum correlations - the two qubit system - is described by the state

$$\rho^{AB} = \frac{1}{4}(\mathbb{I}\otimes\mathbb{I} + \vec{a}\cdot\vec{\sigma}\otimes\mathbb{I} + \mathbb{I}\otimes\vec{b}\cdot\vec{\sigma} + \sum_{i,j=1}^{3} T_{ij}\sigma_i\otimes\sigma_j), \tag{2.1}$$

where $\vec{a}$ and $\vec{b}$ are respectively Alice's Bloch vector and Bob's Bloch vector. The matrix $T \in \mathbb{R}^{3\times3}$ describes correlations between Alice and Bob. ρ^{AB} is a 15-dimensional state (rank four matrix with unit trace) and it has been found by considering the quantum definition of composite states (1.20). Both the single-qubit state and the two-qubit state are hermitean and unit trace and they describe physical states if and only if they are positive semi-definite. For the former it implies the Bloch vector fits inside the sphere, for the latter it is decisely harder to say and we will discuss it further on. Dealing with two qubit systems is therefore a much more difficult task than the single qubit one.

A brilliant idea to study two qubit states consists of using the *quantum steering ellipsoids formalism*. According to this method, the two qubit state 2.1 is represented by both Alice's and Bob's state vectors ($\vec{a}$ and $\vec{b}$) and Alice's steering ellipsoid ε^A (all inside Alice's Bloch sphere), which describes the bipartite correlations[1] (Figure 2.1) . The inclusion of Bob's Bloch vector determines ρ^{AB} up to a choice of basis for Bob, which can be fixed by indicating the orientation of the ellipsoid. The fundamental role of the quantum steering ellipsoid is that it encodes all correlation features of a two

[1] it is obviously equivalent to use Bob's steering ellipsoid instead.

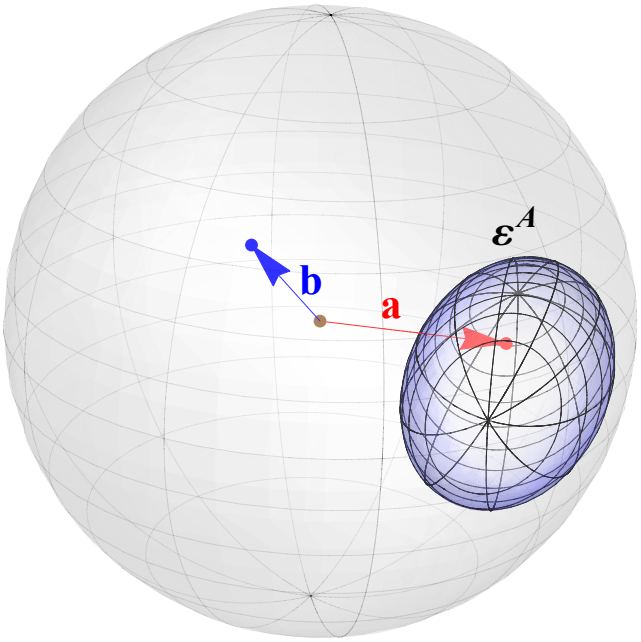


Figure 2.1: The quantum steering ellipsoid representing a two-qubit state. A two-qubit state ρ^{AB} can be described by Alice's and Bob's Bloch vectors $\vec{a}$ and $\vec{b}$ and Alice's steering ellipsoid ε^A all inside Alice's Bloch sphere. Note Alice's Bloch vector lies inside her steering ellipsoid.

qubit state through geometrically (and so intuitively) describing it and its properties in three dimensions. Hence it is the generalization of the Bloch sphere.

The quantum steering ellipsoid of a two qubit state inside Alice's Bloch sphere is the set of Bloch vectors that Bob can collapse Alice's qubit to,through performing all possible measurements on his qubit. It is important to show the intuitions why all Alice's steered state vectors form an ellipsoid that fits inside her Bloch sphere.

2.1.1 Notations

First of all it is necessary and useful to list the notations that will be used (and that has already been used). All 4×4 matrices are denoted by Greek capital letters, 3×3 matrices by Roman capital letters, *4*-vectors by the simbol *tilde* over the letter and *3*-vectors by the simbol *arrow* over the letter. The two qubit state ρ^{AB} shared between Alice and Bob (2.1) has reduced states ρ^A and ρ^B described by Bloch vectors $\vec{r}^A$ and $\vec{r}^B$.

We will always refer to states written in Pauli basis. It means that a single-qubit hermitean operator M is written as $M = \frac{1}{2}\sum_{\mu=0}^{3} X_\mu \sigma_\mu$, where $X_\mu = tr(M)\sigma_\mu$ are real coefficients. In the case the operator has unit trace, *e.g.* it identifies a qubit state, $X_0 = 1$. A two-qubit state like 2.1 can be written as $\rho^{AB} = \frac{1}{4}\sum_{\mu,\nu=0}^{3} \Theta_{\mu\nu}\sigma_\mu \otimes \sigma_\nu$, where $\Theta_{\mu\nu} = tr(\rho^{AB}\sigma_\mu \otimes \sigma_\nu)$. The block matrix Θ can be written as $\Theta = \begin{pmatrix} 1 & \vec{b}^T \\ \vec{a} & T \end{pmatrix}$.

Consider now that Bob performs a POVM measurement on his qubit, thus obtaining,

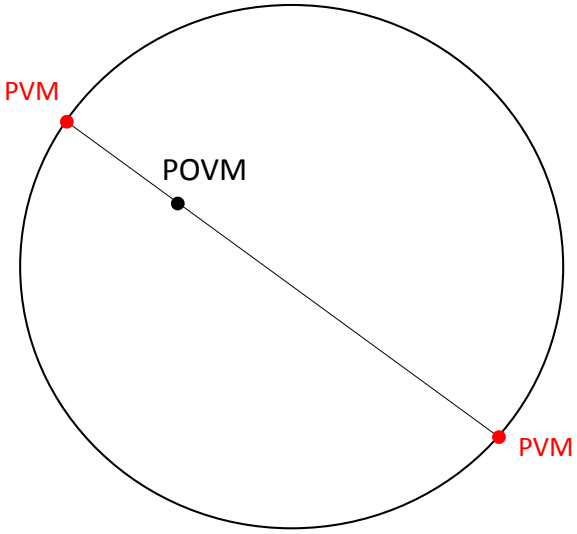


Figure 2.2: POVM inside the Bloch sphere. The figure shows the Bloch sphere in two dimensions. A POVM can be written as a combination of PVM.

for example, the outcome M_0. Hence he steers Alice's qubit to the state

$$\rho_0^A = \frac{1}{p_0} tr_B[\rho^{AB}(\mathbb{I} \otimes M_0)], \tag{2.2}$$

where p_0 is the probability associated with the outcome M_0. This work will always consider the case of two only possible outomes for Bob's POVM measurement (*binary case*), so it is appropriate to name the measurement elements as $M_0 = \Pi$, $M_1 = \mathbb{I} - \Pi$ and the probabilities as $p_0 = p$ and $p_1 = 1 - p$.

Note that according to the definition of projective measurements (1.2.2), a PVM element is identified, in Pauli basis, by an operator having $X_0 = 1$ and $|\vec{X}| = 1$.[2] This fact implies that a PVM is described by a unit vector in the Bloch sphere, *i.e.* a vector which touches the surface of the sphere. On the other hand, a POVM is described by a vector inside the sphere. A POVM can be written as a combination of projective measurements and this is easy to understood through viewing their picture in the Bloch sphere (see 2.2). It results that in the PVM case the probabilities p_0 and p_1 are equal to $\frac{1}{2}$ (see A). In rough analogy, we can think the relation between a POVM and a PVM similar to the relation between a mixed state and a pure state (1.2).

We will refer to Alice's state in Pauli basis as

$$\rho^A = \frac{1}{2}(\mathbb{I} + \vec{a} \cdot \vec{\sigma}), \tag{2.3}$$

but it can be also written as the combination of her collapsed states:

$$\rho^A = p\rho_0^A + (1-p)\rho_1^A. \tag{2.4}$$

Hence Bob's POVM induce a convex decomposition of Alice's local state into the ensemble $\{p_b, \rho_b^A\}$, $b = 0, 1$.

[2] It is sufficient to write a positive operator ρ as a 4-vector in Pauli basis such that it satisfies the completeness relation (*i.e.* representing a POVM) and add also the property $\rho = \rho^2$. Moreover it results that a PVM has eigenvalues $\lambda = 0, 1$.

Table 2.1: Notations for future use. Pauli representation through 4-vectors of (in order): Alice's state, Bob's state, Alice's steered states ($b = 0, 1$), Bob's generic measurement operator M_b^B, Bob's measurement operator $M_0^B = \Pi^B$ (remember $M_1^B = \mathbb{I} - M_0^B$), Alice's measurement operator $M_0^A = \Pi^A$ (remember $M_1^A = \mathbb{I} - M_0^A$).

Operator	*4-vector*
$\rho^A = \frac{1}{2}(\mathbb{I} + \vec{a} \cdot \vec{\sigma})$	$\tilde{a} = \begin{pmatrix} 1 \\ \vec{a} \end{pmatrix}$
$\rho^B = \frac{1}{2}(\mathbb{I} + \vec{b} \cdot \vec{\sigma})$	$\tilde{a} = \begin{pmatrix} 1 \\ \vec{b} \end{pmatrix}$
$\rho_b^A = \frac{1}{2}(\mathbb{I} + \vec{r}_b^A \cdot \vec{\sigma})$	$\tilde{r}_b^A = \begin{pmatrix} 1 \\ \vec{r}_b^A \end{pmatrix}$
$M_b^B = \frac{1}{2}(X_0^b \mathbb{I} + \vec{X^b} \cdot \vec{\sigma})$	$\tilde{X^b} = \begin{pmatrix} X_0^b \\ \vec{X^b} \end{pmatrix}$
$\Pi^B = \frac{1}{2}(X_0 \mathbb{I} + \vec{X} \cdot \vec{\sigma})$	$\tilde{X} = \begin{pmatrix} X_0 \\ \vec{X} \end{pmatrix}$
$\Pi^A = \frac{1}{2}(s_0 \mathbb{I} + \vec{s} \cdot \vec{\sigma})$	$\tilde{s} = \begin{pmatrix} s_0 \\ \vec{s} \end{pmatrix}$

In the following we will usually refer to the 4-vectors composed of the components of the states (see Table 2.1) .

We will also deal with probability distributions, denoted as follows.

- The probability that Bob performs, for example, Π^B (and that Alice's steered state is ρ_0^A):

$$p(M_0^B) = p(\Pi^B) = p(\rho_0^A) = p(\vec{r}_0^A) = p = tr(\rho^{AB} \mathbb{I} \otimes \Pi^B) = tr(\rho^B \Pi^B). \quad (2.5)$$

- The probability that Alice performs M_a^A given that Bob has performed M_b^B ($a, b = 0, 1$):

$$p(M_a^A / M_b^B) = tr(\rho_a^A M_b^B). \quad (2.6)$$

- Therefore the joint probability that Alice's outcome is a and Bob's outcome is b is

$$p_{ab}^{AB} = p(M_b^B) p(M_a^A / M_b^B) = p(M_b^B) tr(\rho_a^A M_b^B). \quad (2.7)$$

For example

$$p_{00}^{AB} = p \cdot p(M_0^a / M_0^B) = p \cdot p(\vec{s} / \vec{X}).$$

2.1.2 Constructing the ellipsoid

A very important result deriving from the above formulas is that

$$p_b \tilde{r}_b^A = \frac{1}{2} \Theta \tilde{X^b}. \quad (2.8)$$

This formula defines the relationship between Bob's POVM outcome b and the corresponding Alice's steered state, given an initial shared state defined by Θ. Moreover the condition that M_b^B are positive semi-definite, *i.e.* M_b^B's eigenvalues $\lambda_\pm$ are non negative, implies that

$$(X_0^b)^2 \geq |\vec{X^b}|^2. \quad (2.9)$$

This can be seen through esplicitely considering

$$M_b^B = \begin{pmatrix} X_0^b + X_3^b & X_1^b - iX_2^b \\ X_1^b + iX_2^b & X_0^b - X_3^b \end{pmatrix}.$$

The characteristic equation is

$$\lambda^2 - 2X_0^b\lambda + (X_0^b)^2 - |\vec{X}^b|^2 = 0,$$

so

$$\lambda_\pm = X_0^b \pm |\vec{X}^b|.$$

It implies $X_0^b \geq |\vec{X}^b|$. The inequality 2.9 can be more appropriately written as

$$\tilde{X^b}^T \eta \tilde{X^b} \geq 0,$$

where $\eta = (1, -1, -1, -1)$. This result constrains Alice's steered states to an ellipsoidal region

$$(\tilde{r}_b^A)^T(\Theta^{-T}\eta\Theta^{-1})\tilde{r}_b^A \geq 0, \tag{2.10}$$

where $\Theta^{-T} = (\Theta^{-1})^T$.

The relation 2.10 is the central equation of the steering ellipsoids formalism. However the easiest way to understand why all Alice's steered state vectors form an ellipsoid that fits inside her Bloch sphere consists of considering states with $\vec{b} = 0$ and supposing that Bob performs a PVM onto some pure state $\tilde{X} = \begin{pmatrix} 1 \\ \vec{v} \end{pmatrix}$ (remember $|\vec{X}| = 1$ for PVM). Hence

$$\tilde{r} = \Theta\tilde{X} = \begin{pmatrix} 1 & 0^T \\ \vec{a} & T \end{pmatrix} \begin{pmatrix} 1 \\ \vec{X} \end{pmatrix} = \begin{pmatrix} 1 \\ \vec{a} + T\vec{X} \end{pmatrix}. \tag{2.11}$$

Note that Alice's steered Bloch vector is $\vec{a} + T\vec{X}$. Therefore the set of all possible Alice's collapsed states is the unit sphere of possible $\vec{X}$, shrunk and rotated by T and translated by $\vec{a}$, *i.e.* an ellipsoid centred at $\vec{a}$ with orientation and semiaxes given by the eigenvectors and eigenvalues of TT^T. All points inside the ellipsoid are reached by taking Bob's POVM (convex combination of PVM) and the dimension of the ellipsoid is equal to $rank(\Theta) - 1$.

The rigorous derivation of the general case of $\vec{b} \neq 0$ can be found in [14]. It results that Alice's steering ellipsoid is centered at $\vec{c}_A = \frac{\vec{a} - T\vec{b}}{1-b^2}$ and matrix

$$Q_A = \frac{1}{1-b^2}(T - \vec{a}\vec{b}^T)(\mathbb{I} + \frac{\vec{b}\vec{b}^T}{1-b^2})(T^T - \vec{b}\vec{a}^T) \tag{2.12}$$

gives, through its eigenvectors and eigenvalues q_i, the semiaxes orientation and lengths $s_i = \sqrt{q_i}$. Q_A and $\vec{c}_A$ specify the ellipsoid ε^A. Therefore a two qubit state ρ^{AB} is represented by $(\varepsilon^A, \vec{a}, \vec{b})$. This representation is faithful: it can be proved ([14]) that also ρ^{AB} can be derived from an ellipsoid ε^A and the vectors $\vec{a}$ and $\vec{b}$ (the reverse procedure).

2.1.3 Canonical aligned states

The *15*-dimensional two-qubit state 2.1 can be reduced to a simpler standard form. Immagine of performing the following operations.

1. A local filtering operation on Bob's qubit

$$\rho^{AB} \to \tilde{\rho}^{AB} = \frac{1}{2}[\mathbb{I} \otimes (\rho^B)^{-\frac{1}{2}}]\rho^{AB}[\mathbb{I} \otimes (\rho^B)^{-\frac{1}{2}}],$$

where $\rho^B = tr_A \rho^{AB}$. The state $\tilde{\rho}^{AB}$ is called *canonical state* and its main features are: Bob's reduced state is maximally mixed, *i.e.* $\vec{\tilde{b}} = 0$, and Alice's state vector $\vec{\tilde{a}}$ coincides with the centre of her steering ellipsoid $\vec{c}_A$. Note that $\varepsilon^A = \tilde{\varepsilon}^A$, *i.e.* local filtering operations on Bob's qubit do not change Alice's steering ellipsoid. Therefore

$$\tilde{\rho}^{AB} = \frac{1}{4}(\mathbb{I} \otimes \mathbb{I} + \vec{c}_A \cdot \vec{\sigma} \otimes \mathbb{I} + \sum_{i,j=1}^{3} \tilde{T}_{ij}\sigma_i \otimes \sigma_j), \tag{2.13}$$

where $\tilde{T}$ is the canonical transformation of T. It implies that Q_A becomes $\tilde{T}\tilde{T}^T$.

2. State-dependent local unitary operations on $\rho^{\tilde{A}B}$

$$\tilde{\rho}^{AB} \to \tilde{\rho}'^{AB} = (U_A \otimes U_B)\rho^{AB}(U_A^\dagger \otimes U_B^\dagger),$$

where it is always possible to choose a unitary transformation (*a signed singular value decomposition* [6]) that gives a diagonal $\tilde{T}'$. Hence

$$\tilde{\rho}'^{AB} = \frac{1}{4}(\mathbb{I} \otimes \mathbb{I} + \vec{\tilde{c}}'_A \cdot \vec{\sigma} \otimes \mathbb{I} + \sum_{i=1}^{3} \tilde{T}'_{ii}\sigma_i \otimes \sigma_i). \tag{2.14}$$

The fact that $\tilde{T}'$ is diagonal means Alice's steering ellipsoid has its axes aligned with the coordinate axes. This last transformation consists of a rotation of $\tilde{\varepsilon}^A$ about the origin, treating the centre vector $\vec{c}_A$ as a rigid rod.

We can now define $\vec{t} = (\tilde{T}'_{11}, \tilde{T}'_{22}, \tilde{T}'_{33})$. The product of the components of $\vec{t}$, $t_1 t_2 t_3$, is the same for any choice of the signed singular value decomposition. It is possible to perform several rotations which aligns $\varepsilon^A(\tilde{\rho}^{AB})$ with the coordinate axes, but they can at most flip two signs among t_1, t_2, t_3.

The operations above imply some restrictions on Alice's and Bob's Bloch vectors $\vec{a}$ and $\vec{b}$. The local filtering operation implies $(\rho^B)^{-\frac{1}{2}}$ must exist, since $|\vec{b}| < 1$ ($|\vec{b}| = 1$ means a product state ρ^{AB} in which no steering is possible). Moreover Alice's state vector $\vec{a} = (1 - b^2)\vec{c}_A + T\vec{b}$ ([14]) and so $\vec{a}$ lies on an ellipsoid with the same centre as $\varepsilon^A(\rho^{AB})$ and semiaxes scaled by a factor $|\vec{b}|$. Hence $\vec{a}$ strictly lies inside $\varepsilon^A(\rho^{AB})$.

We have obtained a *6*-parameters state, the *canonical aligned state* (see figure 2.3).)

$$\tilde{\rho}'^{AB} = \frac{1}{4}(\mathbb{I} \otimes \mathbb{I} + \vec{c} \cdot \vec{\sigma} \otimes \mathbb{I} + \sum_{i=1}^{3} t_i \sigma_i \otimes \sigma_i). \tag{2.15}$$

It is possible to transform back th results obtained on 2.15 to the original state ones, through using rotationally invariant terms such as $detQ$, trQ and $|\vec{c}|^2$.

The results of this work will involve a special case of canonical aligned state (2.3).

2.2 Main results

Quantum steering ellipsoids are functions of the qubits correlations only, and they provide a picture to intuitively and geometrically intend these correlations. In order to understand how powerful is the quantum steering ellipsoids formalism we will list several results obtained through this tool.

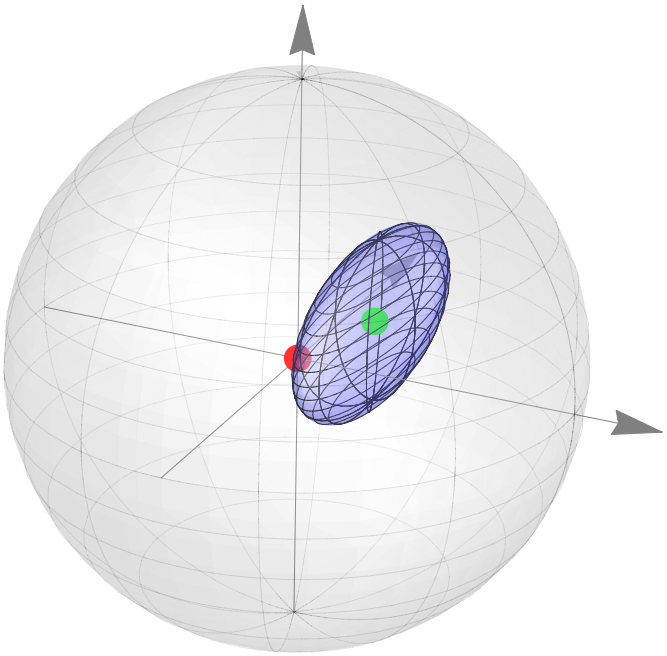


Figure 2.3: Canonical aligned states. They are states described by a canonical, aligned ellipsoid ε^A. The axes of the ellipsoid are parallel to the coordinate axes, the centre of the ellipsoid is represented by a green blob ($\vec{c} = \vec{a}$) and Bob's Bloch vector is represented by a red blob ($\vec{b} = 0$).

2.2.1 Conditions for separability

Given a mixed state $\rho^C = \sum_i p_i |\psi_i\rangle \langle\psi_i|$ (1.2), it is defined as *separable* if it can be written as

$$\rho^C = \sum_j c_j \rho_j^A \otimes \rho_j^B, \tag{2.16}$$

where the system C described by ρ^C is divided in two parties A and B described respectively by $\rho^A = \sum_i p_i |\psi_i\rangle \langle\psi_i|$ and $\rho^B \sum_i p_i |\psi_i\rangle \langle\psi_i|$. If the state ρ^C is not separable, then it is *entangled* [3].

The particular case of pure states is straightforward. The pure state $|\psi_C\rangle$ is separable if it can be written as a product state $|\psi_C\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$. Otherwise it is entangled. If $|\psi_C\rangle$ is separable, then the states ρ^A and ρ^B are pure. If it is entangled, then they are mixed. Note that for a product state the ellipsoid reduces to a point. For a pure entangled state the ellipsoid is steered to the whole Bloch sphere.

One of the most striking results of the quantum steering ellipsoids theory is the *nested tetrahedron condition*. It is a geometric criterion for separability and it states that *a two qubit state ρ^C is separable if and only if its steering ellipsoid ε^A fits inside a tetrahedron that fits inside the Bloch sphere.* It is quite easy to prove the necessity. Let us assume that Alice and Bob share a separable state $\rho^C = \sum_{j=1}^n c_j \rho_j^A \otimes \rho_j^B$. It is always possible to choose $n \leq 4$, so the Bloch vectors representing ρ_j^A define

[3] Note that entanglement refers to a given state and a given partition of the system. The same physical system could be either separable or entangled by simply changing partition.

a tetrahedron T within Alice's Bloch sphere (Note that T can also be degenerate). Immagine now that Bob performs a measurement with outcome M, then Alice is collapsed to the state $\sum_{j=1}^{n} \frac{c_j tr(M\rho_j^A)}{tr(M\rho^B)}\rho_j^A$. This implies that her steering ellipsoid is contained in T, because her new Bloch vector will be given by a convex combination of the Bloch vectors for the ρ_j^A. The sufficiency is not as straightforward as the necessity ([14]).

Therefore we have obtained an intuitively geometrical condition to state if a given state is entangled or separable, just by viewing its steering ellipsoid. Roughly speaking, if the state is entangled, then the ellipsoid is either too big or too near to the surface of the Bloch sphere (it cannot fit inside a tetrahedron inside the sphere).

2.2.2 Physicality conditions

The canonical aligned state 2.15 can be used to find the physicality conditions on the general two qubit state 2.1, since $\rho^{AB} \geq 0 \iff \tilde{\rho}'^{AB} \geq 0$. It results that ([9]) the necessary and sufficient geometrical conditions to have $\rho^{AB} \geq 0$ are:

$$\rho^{AB} \text{ is a physical state} \iff det\rho^{AB} \geq 0 \text{ and } \varepsilon(\rho^{AB}) \subseteq B,$$

where B denotes the Bloch sphere. The condition $\varepsilon(\rho^{Ab}) \subseteq B$ coincides with the condition that ρ^{AB} *is Bloch positive*, *i.e* it fulfils $\langle\psi|\rho^{AB}|\psi\rangle \geq 0$ for all product states $|\psi\rangle$.

There exists a useful quantity we have not still defined: the chirality of $\varepsilon(\rho^{AB})$. It is simply given by $w = sign(t_1 t_2 t_3)$. If $w = +1(-1)$ the state has *right-handed (left-handed)* chirality. It results that:

- for entangled states only the left-handed ellipsoids are physical states;
- for separable states both left and right handed ellipsoids are physical states.

What does a non-physical ellipsoid represent? There are two distinct ways in which the ellipsoid can be unphysical: either fitting into the Bloch sphere or piercing it. In the first case the ellipsoid represents an *entanglement witness*, in the second case it represents a truly unphysical state. The first case corresponds to an ellipsoid that has the 'wrong' chirality but represents an entangled state when flipped. An entanglement witness indicates the presence of entanglement in the system and it is defined as an Hermitean operator ρ which is block positive but not positive semi-definite, *i.e.* $\langle\psi|\rho|\psi\rangle \geq 0$ for all product states $|\psi\rangle$ but there exists some entangled states $|\phi\rangle$ for which $\langle\phi|\rho|\phi\rangle < 0$. It results that a two-qubit entanglement witness exactly has one negative eigenvalue and three positive eigenvalues ([9]).

A complete classification of all possible cases for states described by ellipsoids inside the Bloch sphere will clarify every doubt:

$$det\rho^{AB} \geq 0 \text{ and } \det(\rho^{AB})^{T_B} \geq 0 \iff \begin{cases} \rho^{AB} \text{is a separable state } (w = \pm 1, 0) \\ (\rho^{AB})^{T_B} \text{is a separable state } (w = \mp 1, 0) \end{cases}$$

$$det\rho^{AB} \geq 0 \text{ and } \det(\rho^{AB})^{T_B} < 0 \iff \begin{cases} \rho^{AB} \text{is an entangled state } (w = -1) \\ (\rho^{AB})^{T_B} \text{is an entanglement witness } (w = +1) \end{cases}$$

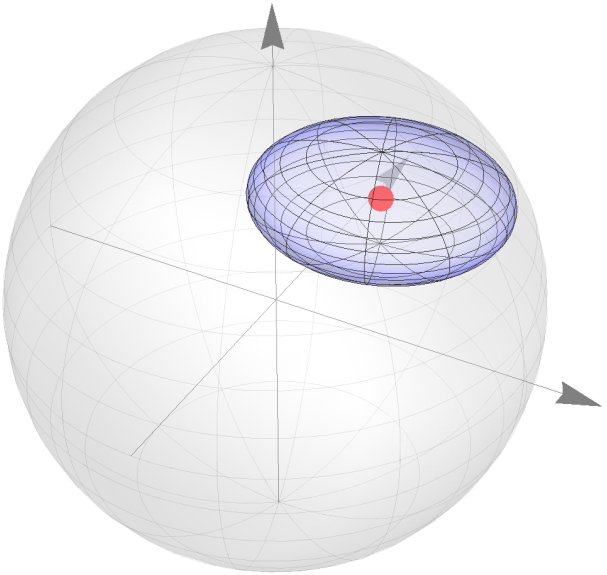


Figure 2.4: Ellipsoids describing entanglement witnesses. The figure shows an ellipsoid such that $det\rho^{AB} < 0$ and $\det(\rho^{AB})^{T_B} < 0$. It represents an entanglement witness.

$$det\rho^{AB} < 0 \text{ and } \det(\rho^{AB})^{T_B} \geq 0 \iff \begin{cases} \rho^{AB} \text{is an entanglement witness } (w = +1) \\ (\rho^{AB})^{T_B} \text{ is an entangled state } (w = -1) \end{cases}$$

$$det\rho^{AB} < 0 \text{ and } \det(\rho^{AB})^{T_B} < 0 \iff \begin{cases} \rho^{AB} \text{is an entanglement witness } (w = \pm 1, 0) \\ (\rho^{AB})^{T_B} \text{is an entanglement witness } (w = \mp 1, 0) \end{cases}$$

$(\rho^{AB})^{T_B}$ is the partially transposed state of ρ^{AB} and it is an important quantity because the Peres-Horodecki criterion ([7]) states that a two qubit state ρ^{AB} is separable if and only if $(\rho^{AB})^{T_B} \geq 0$.

Figure 2.6 shows an example of the first case above (separable states), figure 2.3 of the second case (physical state) and 2.4 of the third case (entanglement witnesses).

2.2.3 Other results

The quantum steering ellipsoids theory counts several results in addition to the ones already mentioned. This section will list some of them.

- Incomplete steering phenomenon. Given a separable state it is possible that some decompositions of Alice's state are inaccessible, *i.e.* there are some decompositions of Alice's reduced state which are not steered by any measurement of Bob. An example of such a state is $\rho^{AB} = \frac{1}{2}(|00\rangle\langle 00| + |1+\rangle\langle 1+|)$.
- Volume of the ellipsoid. The volume of an ellipsoid is given by $\frac{4\pi}{3}s_1s_2s_3$, so ε^A has volume $V_A = \frac{4\pi}{3}|\sqrt{detQ_a}| = \frac{64\pi}{3}\frac{|det\rho^{AB} - det(\rho^{AB})^{T_B}|}{(1-b^2)^2}$. The volume of an ellipsoid provides a new resource (different from entanglement) for two-qubit

information theory: the *obesity*. It is linked to the three-dimensionality of the ellipsoid which describes the two-qubit state. An obese state means a state with more-than-classical correlations between the shared qubits. It is a measure of quantum correlations between Alice and Bob ([9]). From the tetrahedron theorem it results that the maximum volume for a state to be separable is $V_{Sep} = \frac{4\pi}{81}$, so the volume is an entanglement witness. The maximum volume separable state is the so called Werner state. Its ellipsoid is a sphere (inside a tetrahedron) with radius $\frac{1}{3}$ centred in the origin of the Bloch sphere. Every ellipsoid with volume $V_A > V_{Sep}$ must represent an entangled state. It is also possible, fixed a centre, to find the maximum volume V_{Phys} for an ellipsoid to represent a physical state ($V_{Phys} \geq V_{Sep}$). We will refer to them as *maximum volume states* and we will illustrate them in the next section.

- Entanglement monogamy. Quantum steering ellipsoids can be also used for three-qubit system issues. Immagine Bob performs measurements on his qubit to steer Alice's and Charlie's qubit. It results that ([13])

$$\sqrt{V_{A|B}} + \sqrt{V_{C|B}} \leq \sqrt{\frac{4\pi}{3}},$$

where $V_{A|B}$ and $V_{C|B}$ are Alice's and Charlie's volume of their steering ellipsoids. The previous inequality is called the *monogamy of steering*. It is possible to derive the famous CKW (Coffman-Kundu-Wootters) inequality for the monogamy of concurrence [4] from the monogamy of steering, thus showing it is strictly stronger than the CKW result.

- Euler theorem. The quantum steering ellipsoids formalism also shows its power in different fields from quantum information theory, such as classical Euclidean geometry. A really curious and intriguing result involves a famous inequality of Euler: $r \leq \frac{R}{2}$, where R is the triangle circumradius and r is the triangle inradius. This theorem can be derived from the nested tetrahedron condition ([13]), which also generalizes it to the three-dimensional case of a tetrahedron and circumscribed and inscribed spheres: $c^2 \leq (R + r)(R - 3r)$.

Note that the most striking fact of the quantum steering ellipsoids formalism is how naively and intuitively are these results pictured. This is due to its geometrical nature.

2.3 Maximum volume states

The volume of ellipsoids is a fundamental feature to capture much of the non-trivial quantum correlations and states corresponding to maximum volume ellipsoids , fixed a centre c, have really special properties. 'Maximum volume' means the volume over which the ellipsoid no longer describes a physical state.

In order to study the physical-unphysical boundary we start by considering *inept states* ([15]), *i.e.* states given by

$$\rho^{AB} = r \left|\phi_\varepsilon\right\rangle \left\langle\phi_\varepsilon\right| + (1 - r)\rho'^{AB} \otimes \rho'^{AB},$$

[4] The concurrence is an entanglement monotone connected with the entanglement of formation, thus linked to the quantification of entanglement in a quantum system. A more precise definition can be found in [18].

where $|\phi_\varepsilon\rangle = \sqrt{\varepsilon}\,|00\rangle + \sqrt{1-\varepsilon}\,|11\rangle$ and $\rho'^{AB} = tr_A(|\phi_\varepsilon\rangle\langle\phi_\varepsilon|) = tr_B(|\phi_\varepsilon\rangle\langle\phi_\varepsilon|)$. An inept state is described by a steering ellipsoid ε^A that consists of a sphere of radius r, centre $\vec{c} = (0,0,(2\varepsilon-1)(1-r))$ and $Q = diag(r^2,r^2,r^2)$. Note that if $\varepsilon = \frac{1}{2}$, then both Alice's and Bob's Bloch vectors are null and $\vec{c} = (0,0,0)$, so it coincides with the Werner state.

It is now necessary to state an important theorem (*algebric physicality condition*, see [13] for the proof). Consider ρ^{AB} as an operator of the form 2.15 represented by the ellipsoid ε^A with centre $\vec{c}_A$, matrix Q_A and chirality χ. ρ^{AB} represents a physical state($\rho^{AB} \geq 0$) if and only if

$$g_1 = c^4 - 2uc^2 + q \geq 0,$$

$$g_2 = 1 - trQ_A - 2\chi\sqrt{detQ_A} - c^2 \geq 0,$$

where $u = 1 - trQ_A + 2\hat{c}_A^T Q_A \hat{c}_A$ and $q = 1 + 2tr(Q_A^2) - 2trQ_A - (trQ_A)^2 - 8\chi\sqrt{detQ_A}$. This theorem and the fact that entangled states must be left-handed states are sufficient to find the ellipsoid representing the maximum volume state. Therefore we need to seek the extremal ellipsoid that achieves $\rho^{AB} \geq 0$ with $\chi = -1$,[5] *i.e.* maximize $V = \frac{4\pi}{3} s_1 s_2 s_3$ for a given c in presence of constraints $g_1 \geq 0$ and $g_2 \geq 0$. This task can be achieved through a generalization of the method of Lagrange multipliers: the Karush-Kuhn-Tucker (KKT) conditions ([17]). Let us write the Lagrangian $\mathcal{L} = V + \lambda_1 g_1 + \lambda_2 g_2$, where λ_1 and λ_1 are KKT mutlipliers. Hence it is necessary to solve

$$\begin{cases} \dfrac{\partial \mathcal{L}}{\partial \vec{s}} = \vec{0} \\ \lambda_1 g_1 + \lambda_2 g_2 = 0 \\ \lambda_1, \lambda_2, g_1, g_2 \geq 0 \end{cases} .$$

This system can be simplified because of symmetry reasons. Any maximum ellipsoid must have one axis aligned radially and the other two axes which are equal. For an *aligned* state this implies we can choose $\vec{c} = (0,0,c)$ and $\vec{s}_1 = \vec{s}_2$. Therefore maximum ellipsoids could be *oblate spheroids* ($s_1 = s_2 > s_3$), *prolate spheroids*($s_1 = s_2 < s_3$) and *sphere*($s_1 = s_2 = s_3$).

Coming back to inept states, the previous proof implies the physical-unphysical boundary is $r = 1 - c$, *i.e.* the maximum volume sphere touches the Bloch sphere in one point. The physicality constraint for inept states coincides with the fact that the steering sphere must lie inside the Bloch sphere.

If we generalize the case of inept states to generic *canonical states*, then the largest volume physical ellipsoid ε_A centred at $\vec{c}$ is an oblate spheroid with its minor axis oriented radially. The next chapter will assume ellipsoids ε_c^{max} with $\vec{c} = (0,0,c)$, with $0 \leq c \leq 1$ so the major semiaxes are $s_1 = s_2 = \sqrt{1-c}$ and the minor semiaxis is $s_3 = 1 - c$ (see figure 3.1). They are the *maximum volume states* we will refer to. They are entangled states, except the case of $c = 1$, which corresponds to a product state. The state described by ε_c^{max} can be written as

$$\rho_c^{max} = (1 - \frac{c}{2})\,|\psi_c\rangle\langle\psi_c| + \frac{c}{2}\,|00\rangle\langle 00|\,, \tag{2.17}$$

where $|\psi_c\rangle = \frac{1}{\sqrt{2-c}}(|01\rangle + \sqrt{1-c}\,|10\rangle)$. They are rank-2 'X states', *i.e.* states described by density matrices that, in the computational basis, have elements different from zero only in the diagonal and anti-diagonal.

[5] Remember $V_{Phys} \geq V_{Sep}$.

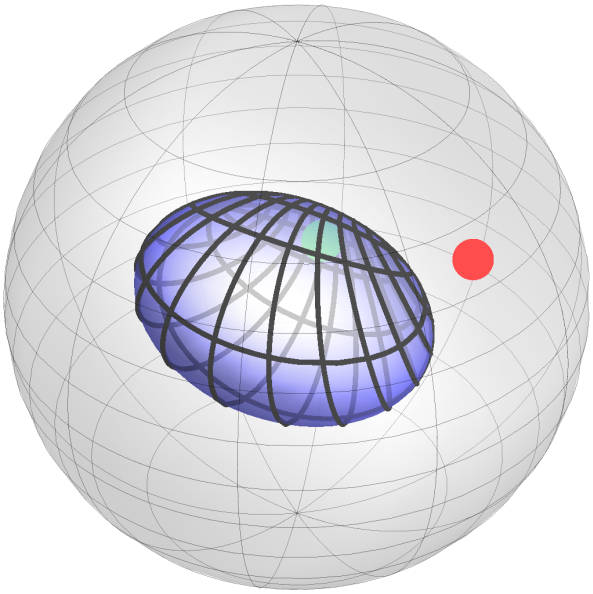


Figure 2.5: Ellipsoid describing an entangled state. In the case of pure states, the ellipsoid of an entangled state concides with the Bloch sphere; the ellipsoid of a product state coincides with a point. In the case of mixed states the ellipsoid cannot fit inside a tetrahedron because it is either too big or too near to the surface of the Bloch sphere.

Maximum volume states have a precise physical interpretation: if Alice and Bob share the Bell state $|+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and Alice passes her qubit through a Choi-isomorphic channel[6], then the result is a maximum volume state centred at $\vec{c} = (0, 0, c)$. Another remarkable fact is that the volume of maximum volume states allows to write an upper bound to the concurrence ([13]).

The next chapter will concern the accessible information in maximum volume states in the case that Bob performs a measurement composed by only two elements. Despite the strong symmetry constraint, it will be an difficult task to deal with.

We conclude this Chapter through considering figure 2.5, 2.6, 2.7, 2.8, 2.9 which shows several cases of ellipsoids corresponding to different states.

[6]Choi-isomorphic channel: ρ_c^{max} is isomorphic to the trace-preserving single qubit amplitude-damping channel with decay probability c (see [1] for further details).

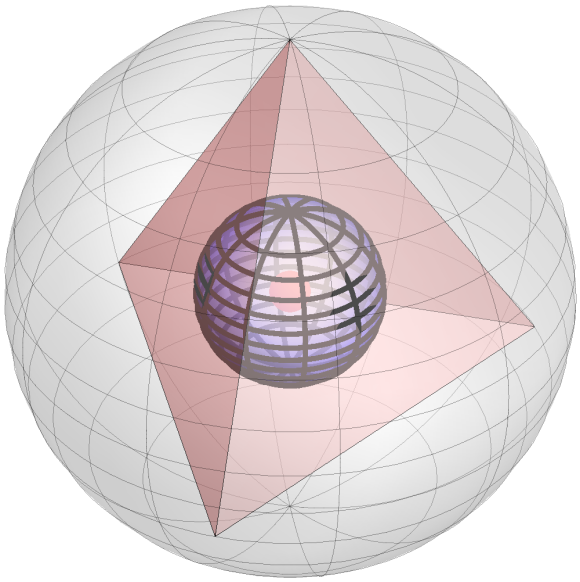


Figure 2.6: The Werner state. It is a special example of a separable state: It is the maximum volume separable state and it is represented by a sphere, which fits inside a tetrahedron, with radius $\frac{1}{3}$ centred in the origin of the Bloch sphere.

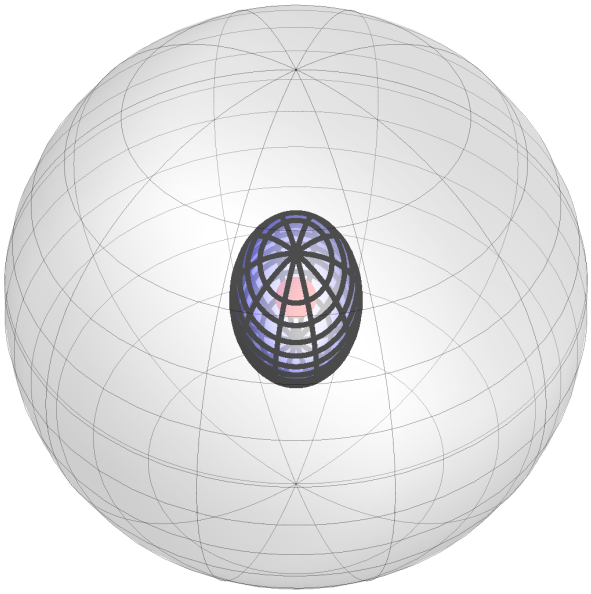


Figure 2.7: The Bell-diagonal state. It is described by an ellipsoid centred at the origin and its semiaxes are given by the three singular value of T. See [14] for more details.

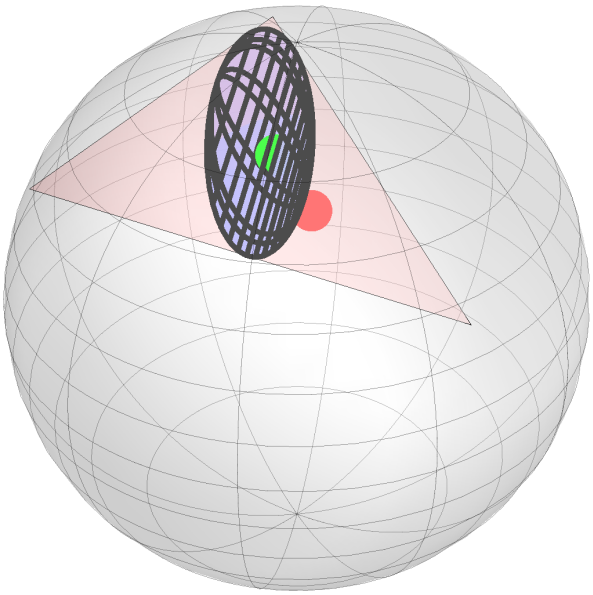


Figure 2.8: Ellipsoid reducing to a steering pancakes. The set of Alice's steered states can be degenerate and, for example, generates a two-dimensional set. The figure shows a separable pancake which fits inside a triangle (a three-dimensional tetrahedron).

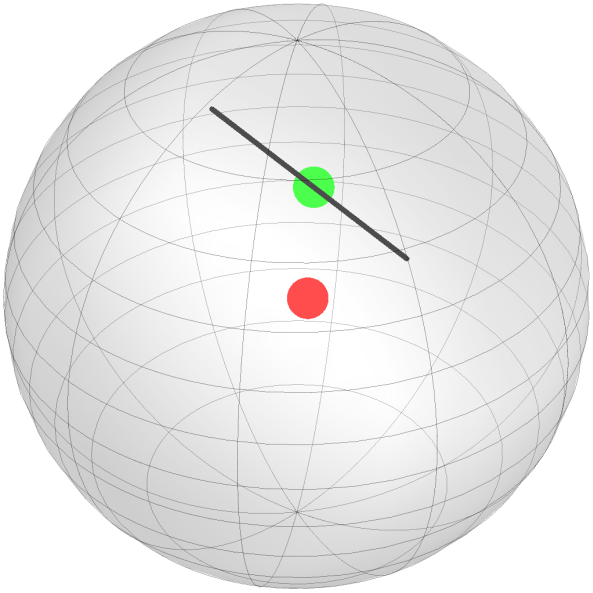


Figure 2.9: Ellipsoids reducing to a steering needle. The set of Alice's steered states can be even more degenerate and generates a one-dimensional set. The figure shows a line segment, often called a steering needle.

Chapter 3

Binary accessible information in maximum volume states

Imagine Alice and Bob were to share two qubits described by two states ρ^A and ρ^B (the whole system is described by the state ρ^{AB}). Bob performs a quantum measurement in his qubit, the elements of which are $\{M_0, M_1, \ldots, M_n\}$, and he collapses Alice's qubit to one state taken among $\{\rho_0, \rho_1, \ldots, \rho_n\}$ with respective probabilities $\{p_0, p_1 \ldots, p_n\}$. Each collapsed state is represented by a vector on her ellipsoid. After Bob's measurement, Alice wants to guess in which state her qubit is. Hence she performs a quantum measurement and wants it to maximize the mutual information for this quantum process.

We underline once again that this work will deal with *classical* mutual information, because this expresses the classical correlation that can be extracted from the quantum process. It is not possible to give such an operationally clear meaning for *quantum* mutual information.

Finding the optimal measurement in the above situation actually involves two optimizations: the first related to Bob's measurement and the second related to Alice's measurement.This work will not deal with the first optimization because it will always assume the *binary case*, *i.e* two measurement elements $\{M_0, M_1\}$ and so two possible state vectors on Alice's ellipsoid, with probabilities $\{p_0, p_1\}$. The aim is to find the binary accessible information in a two qubit system when Alice's ellipsoid describes a *maximum volume state* (2.3), which is a particular case of canonical states.

The reason of this assumption derives from the fact that maximum volume states show symmetry and special properties. This means Alice's steered state is described by an oblate spheroid ε_c^{max}, with its minor axis oriented radially and touching the Bloch sphere surface at one point. Without loss of generality, we can also assume the ellipsoid is centered on the z *axis*, so $\vec{c} = (0, 0, c)$, with $0 \leq c \leq 1$. For such an ellipsoid the major semiaxes are (figure 3.1)

$$s_1 = s_2 = \sqrt{1 - c} \tag{3.1}$$

and the minor semiaxis is

$$s_3 = 1 - c. \tag{3.2}$$

The state represented by the maximum volume ellipsoid depends only on the parameter

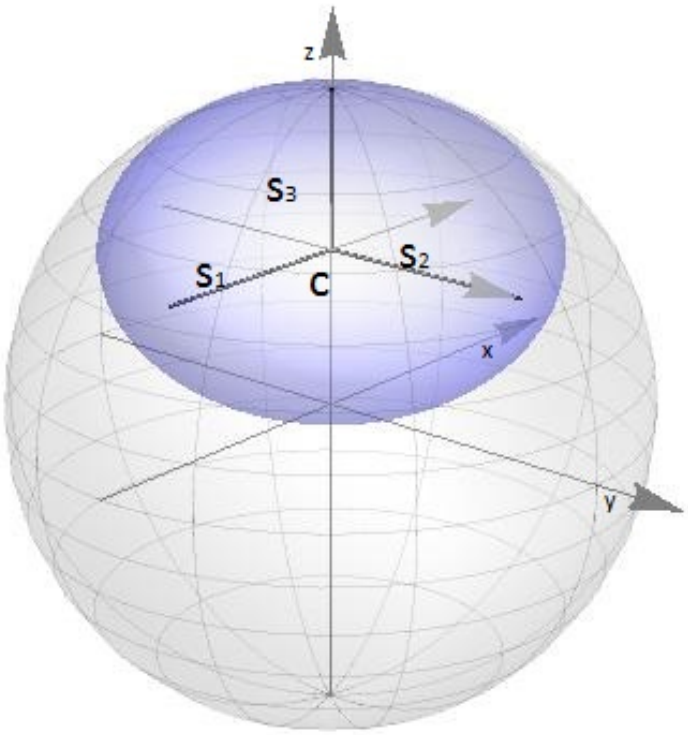


Figure 3.1: Maximum volume states. The figure above shows the special maximum volume state we will deal with. It is an oblate spheroid with $\vec{c} = (0, 0, c)$, $s_1 = s_2 = \sqrt{1-c}$ and the minor semiaxis is $s_3 = 1 - c$.

c and it can be written as

$$\rho_c^{max} = (1 - \frac{c}{2}) \left|\psi_c\right\rangle \left\langle\psi_c\right| + \frac{c}{2} \left|00\right\rangle \left\langle 00\right|, \tag{3.3}$$

where $\left|\psi_c\right\rangle = \frac{1}{\sqrt{2-c}}(\left|01\right\rangle + \sqrt{1-c}\left|10\right\rangle)$. It corresponds to an entangled state, except the case of $c = 1$, which describes a product state, so it has chirality $\chi = -1$, *i.e.* it is described by a left-handed steering ellipsoid. This fact implies that the semiaxes are

$$\vec{t} = (\sqrt{1-c}, \sqrt{1-c}, c-1), \tag{3.4}$$

where the sign of the third semiaxis has been flipped.

Starting from these assumptions we procede as follows:

We first consider the mutual information for couples of opposite points (state vectors) on the surface of Alice's ellipsoid, and then we refer to couples of points inside the ellipsoid. The first case corresponds to a PVM performed by Bob, the secondFr to a POVM (see the Appendix).

It is expected that the maximum value of the mutual information in this particular case of maximum volume states will be reached if we consider the furthest points on the ellipsoids. This is because the mutual information reaches its maximum for classical

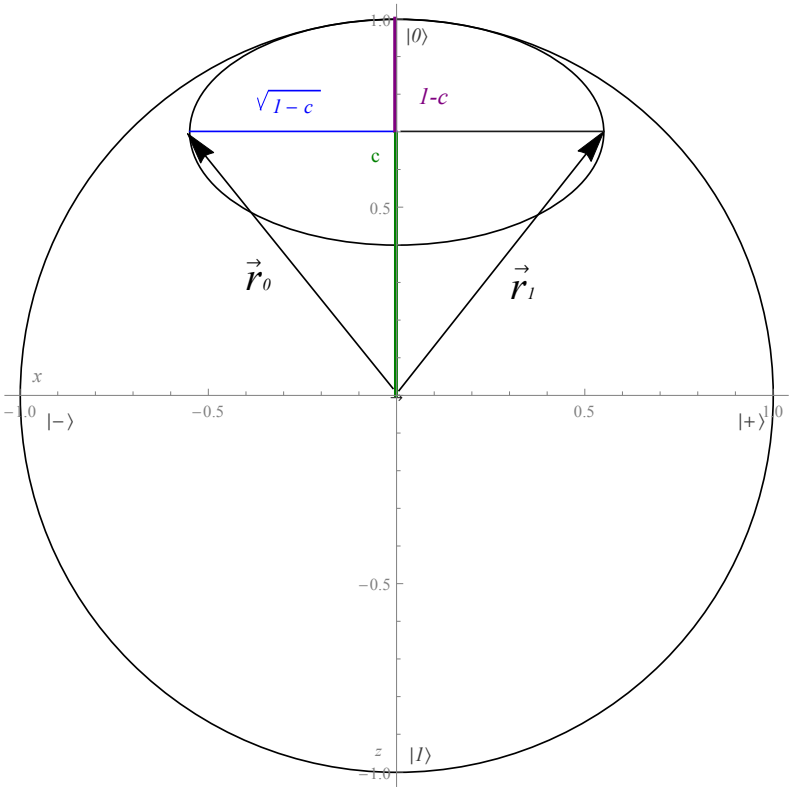


Figure 3.2: Alice's collapsed states ρ_0^A and ρ_1^A. They are represented by their Bloch vectors $\vec{r}_0^A$ and $\vec{r}_1^A$. The figure above also shows the values of semiaxes and the Pauli basis vectors $\{|-\rangle, |+\rangle, |0\rangle, |1\rangle\}$ along the axes.

distinguishable states, and the more distant the points in the Bloch sphere are, the nearer to be classical the behaviour of the corresponding states is.

If the above intuition is right, then it implies a lower bound of the accessible information for a two qubit system because in a general *non-binary* quantum task the mutual information could be greater.

3.1 State vectors on an ellipsoid's surface, Bob's PVM

3.1.1 Furthest and nearest points on the ellipsoid's surface

Let us try to find the mutual information for the furthest points case, *i.e.* the extreme points on the major axis. How distant are they?

We name Alice's two collapsed states ρ_0^A and ρ_1^A; the corresponding state vectors are (figure 3.2)

$$\vec{r}_0^A = (-\sqrt{1-c}, 0, 0) \tag{3.5}$$

and

$$\vec{r}_1^A = (\sqrt{1-c}, 0, 0). \tag{3.6}$$

Their euclidean distance is simply given by

$$d(\rho_0^A, \rho_1^A) = ||\vec{r}_0^A - \vec{r}_1^A|| = 2\sqrt{1-c}. \tag{3.7}$$

In the case of general canonical states, it is $2\max_i |t_i|$, where the index i denotes the three semiaxes.

Alice's two collapsed states in the Pauli basis are

$$\rho_0^A = \frac{1}{2}(\mathbb{I} - \sqrt{1-c}\cdot\sigma_x + c\sigma_z) \tag{3.8}$$

$$\rho_1^A = \frac{1}{2}(\mathbb{I} + \sqrt{1-c}\cdot\sigma_x + c\sigma_z). \tag{3.9}$$

We refer now to the mutual information 1.1.3:

$$H(A:B) = H(A) + H(B) - H(A,B). \tag{3.10}$$

We evaluate separately each quantity of it. Note that the optimal measurement for Alice here is in basis $\{|-\rangle, |+\rangle\}$, according to the maximum likelihood discrimination (1.3.2).

$$\begin{aligned} H(A) &= -p_-^A \log p_-^A - p_+^A \log p_+^A, \\ H(B) &= -p_0^B \log p_0^B - p_1^B \log p_1^B, \\ H(A,B) &= -p_{-0}^{AB} \log p_{-0}^{AB} - p_{+0}^{AB} \log p_{+0}^{AB} - p_{-1}^{AB} \log p_{-1}^{AB} - p_{+1}^{AB} \log p_{+1}^{AB}; \end{aligned} \tag{3.11}$$

where $p_-^A = p_+^A = \frac{1}{2}$ are the probabilities for Alice of respectively measuring $|-\rangle$ and $|+\rangle$, and $p_0^B = p_1^B = \frac{1}{2}$ are the probabilities for Bob of respectively measuring M_0 and M_1. The reason these probabilities are necessary equal to $\frac{1}{2}$ derives from the fact that Bob performs PVM and the fact that maximum volume states are a particular case of canonical states for which Bob's Bloch vector $\mathbf{b}$ is null. A precise explanation can be found in the Appendix.

We name M_0 and M_1 as Π_0 and $\Pi_1 = \mathbb{I} - \Pi_0$ since they are PVM elements. p_{ab}^{AB} are the joint probabilities of obtaining a for Alice's measurement and b for Bob's measurement; $a = -, +$ and $b = 0, 1$. They are given by

$$\begin{aligned} p_{ab}^{AB} &\equiv p_b^B \cdot p(|a\rangle / \Pi_b) \\ &\equiv Tr(\rho^{AB} |a\rangle \langle a| \otimes \Pi_b) \\ &= \frac{1}{2} \langle a| \rho_b^A |a\rangle \end{aligned} \tag{3.12}$$

Substitute now 3.8 and 3.9 in the expression 3.12 above and evaluate 3.11, thus obtaining

$$\langle -| \rho_0^A |-\rangle = \langle +| \rho_1^A |+\rangle = \frac{1}{2}(1 + \sqrt{1-c}) \tag{3.13}$$

$$\langle +| \rho_0^A |+\rangle = \langle -| \rho_1^A |-\rangle = \frac{1}{2}(1 - \sqrt{1-c}) \tag{3.14}$$

and so the mutual information for the furthest points of Alice's steering ellipsoid is

$$H(A:B) = 2 + \frac{1}{2}(1-\sqrt{1-c})\log[\frac{1}{4}(1-\sqrt{1-c})] + \frac{1}{2}(1+\sqrt{1-c})\log[\frac{1}{4}(1+\sqrt{1-c})]$$

$$= 2 + \frac{1}{2}\log[\frac{1}{16}(1+\sqrt{1-c})(1-\sqrt{1-c})] + \frac{1}{2}\sqrt{1-c}\log(\frac{1+\sqrt{1-c}}{1-\sqrt{1-c}})$$

$$= 2 + \frac{1}{2}\log 2^{-4} + \frac{1}{2}\log c + \frac{1}{2}\sqrt{1-c}\log(\frac{(1+\sqrt{1-c})^2}{c})$$

$$= \frac{1}{2}[\log c + 2\sqrt{1-c}\log(\frac{1+\sqrt{1-c}}{\sqrt{c}})] \equiv f(c), \tag{3.15}$$

where the properties 1.2.2 of Chapter one have been used. Note that $H(A)+H(B) = 2$.

Before going on, note that all the previous reasonings deal with a completely abstract scenario in which no communication processes are involved. It is possible to consider a communication process consisting of two parties, Charlie and Dick. Dick wants to communicate a classical message to Charlie and encondes it in two quantum states ρ_0 and ρ_1 with probabilities p_0 and p_1. Charlie performs a quantum measurement described by the elements $\{M_0, M_1\}$ to guess the message.

All the passages performed before could be replaced through substituting Alice and Bob with Charlie and Dick. In both the Abstract and Communication scenario the mathematics is the same. It is important to highlight this possibility, because most authors in the literature usually deal with the communication scenario [1]. This is mathematically equivalent to the Abstract scenario of the current work. Moreover note that in both scenarios the issue is almost completely classical since it mostly involves classical probability distributions, except when quantum measurements are involved (it is the only quantum task). Let us now compare the mutual information obtained for the furthest points with the mutual information calculated for generic couples of points on the surface of Alice's ellipsoid.

Firstly start calculating the mutual information for the nearest points on the surface of the ellipsoid, *i.e.* the extreme points on the minor axis. It should be the lower value of the mutual information for couples of points on the surface of the ellipsoid, according to our previous intuition.

It is possible to evaluate the quantities appearing in the formula 3.10 as before. The quantities of interest are now

$$\vec{r}_0^{\,\prime A} = (0,0,2c-1) \to \rho_0^{\prime A} = \frac{1}{2}(\mathbb{I} + (2c-1)\sigma_z) \tag{3.16}$$

$$\vec{r}_1^{\,\prime A} = (0,0,1) \to \rho_1^{\prime A} = \frac{1}{2}(\mathbb{I} + \sigma_z) \tag{3.17}$$

and so

$$p_{00}^{\prime AB} = p_0^{\prime B}\langle 0|\rho_0^{\prime A}|0\rangle = \frac{c}{2}$$

$$p_{10}^{\prime AB} = p_0^{\prime B}\langle 1|\rho_0^{\prime A}|1\rangle = \frac{1-c}{2}$$

$$p_{01}^{\prime AB} = p_1^{\prime B}\langle 0|\rho_1^{\prime A}|0\rangle = \frac{1}{2}$$

$$p_{11}^{\prime AB} = p_1^{\prime B}\langle 1|\rho_1^{\prime A}|1\rangle = 0.$$

[1] The communication scenario certifies the application of the classical mutual information in the information theory.

$$p_0^{'A} = p_{00}^{'AB} + p_{01}^{'AB} = \frac{1+c}{2}$$
$$p_1^{'A} = p_{10}^{'AB} + p_{11}^{'AB} = \frac{1-c}{2}$$
$$p_0^{'B} = \frac{1}{2}$$
$$p_1^{'B} = \frac{1}{2}.$$

Note that now the optimal measurement for Alice is in basis $\{|0\rangle, |1\rangle\}$, according to the maximum likelihood discrimination (1.3.2). Figure 3.2 shows why, geometrically, in this case the probabilities $p_0^{'A}$ and $p_1^{'A}$ are not equal to $\frac{1}{2}$: the nearest points are not "centered" between $|0\rangle$ and $|1\rangle$. On the other hand the furthest points are centered between $|-\rangle$ and $|+\rangle$, so $p_0^A = p_1^A = \frac{1}{2}$.

The mutual information for the nearest points of Alice's steering ellipsoid is

$$H(A:B) = -\frac{1+c}{2}\log\frac{1+c}{2} + \frac{1}{2} + \frac{c}{2}\log\frac{c}{2}$$

$$= \frac{1}{2}[c\log c - (1+c)\log(1+c) - c + (1+c) + 1]$$

$$= \frac{1}{2}[c\log c - (1+c)\log(1+c) + 2]$$

$$= \frac{1}{2}[c\log\frac{c}{1+c} - \log(1+c) + 2] \equiv n(c). \tag{3.18}$$

Figure 3.3 plots what it has been found.

It is clear that $f(c) \geq n(c)$, where the equality holds only for $c = 0, 1$ and it is obvious to expect the region included between $f(c)$ and $n(c)$ to be the region of the possible values of the mutual information for generic couples of points on the ellipsoid surface.

The function f(c) can also be plotted with respect to the half-distance between the points in the couple (see figure 3.4), *i.e.* the maximum half-distance d for couples of points on the ellipsoid surface. It is possible to rewrite 3.15 as

$$f(d) = \frac{1}{2}[\log(1-d^2) + 2d\log(\frac{1+d}{\sqrt{1-d^2}})$$

$$= \frac{1}{2}[\log(1-d^2) + d\log(\frac{1+d}{1-d})], \tag{3.19}$$

where $d = \sqrt{1-c}$. It is a monotonically increasing function of d and it reaches its maximum for $d = 1$, when the ellipsoid coincides with the whole Bloch sphere, *i.e.* the two qubits become distinguishable. It vanishes when $d = 0$, *i.e* when the ellipsoid reduces to a point and the two qubits are completely indistinguishable.

At this point we discuss the case of generic couples on the ellipsoid surface. We expect to find functions of c located between $n(c)$ and $f(c)$ (3.3).

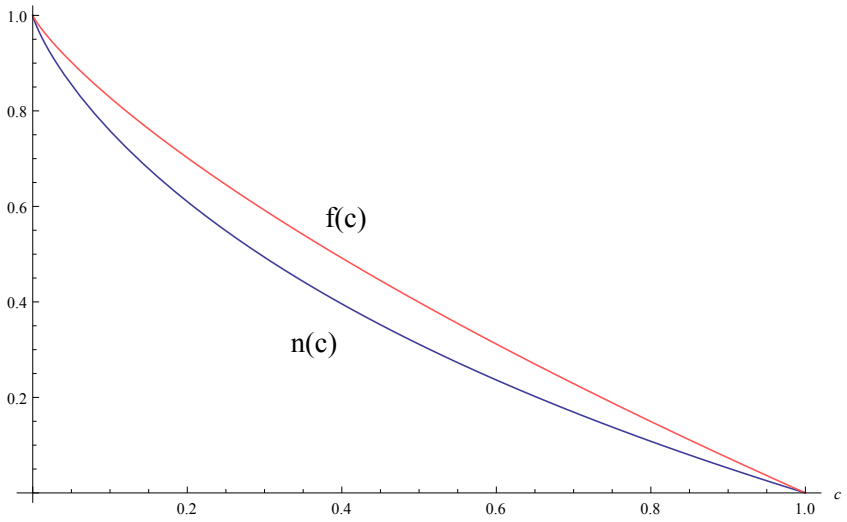


Figure 3.3: Mutual information for the furthest and nearest points on the maximum volume ellipsoid. It is clear that the mutual information is greater for the furthest points. The region included between the two curves should be the one containing the mutual information functions for general couples of points on the surface of the ellipsoid.

3.1.2 Generic couples of points on the ellipsoid's surface

Let us start from the maximum likelihood discrimination. It states that the optimal operator elements are given by the eigenvectors of the difference betweeen Alice's two collapsed states : $\rho_0^{''A} - \rho_1^{''A}$.

These two qubit states have state vectors $\vec{r}_0^{\,''A}$ and $\vec{r}_1^{\,''A}$. This implies the eigenvectors of their difference are

$$\pm\,\vec{s} = \pm\frac{1}{2}[\vec{r}_0^{\,''A} - \vec{r}_1^{\,''A}]. \tag{3.20}$$

$\pm\vec{s}$ must be normalized because they correspond to PVM elements. Therefore the appropriate unit vectors are

$$\pm\,\hat{s} = \pm\frac{\vec{s}}{|\vec{s}|}. \tag{3.21}$$

Hence the conditional probability $p(\Pi_b^{''A}/\Pi_b^{''B}) = p(\pm\vec{s}/\vec{r}_b^{\,''A})$, where $\Pi_b^{''B}$ and $\Pi_b^{''A}$ respectively indicates Bob's PVM elements and Alice's PVM elements and $b = 0, 1$ [2], is

$$p(\pm\hat{s}/\vec{r}_b) = Tr(\rho_a^{''A}\Pi_b^{''A}) = Tr[\frac{1}{2}(\mathbb{I} + \vec{r}_b^{\,''A}\cdot\vec{\sigma})\cdot\frac{1}{2}(\mathbb{I} \pm \hat{s}\cdot\vec{\sigma})] = \frac{1}{2}(1 \pm \vec{r}_b^{\,''A}\cdot\hat{s}). \tag{3.22}$$

It is now possible to calculate the joint probability 3.12 and so the mutual information 3.10.

The quantities of interest are

[2] Indicating Alice's measurement through the index $b = 0, 1$ is an abuse of notation. However this notation should be clearer and unambiguous.

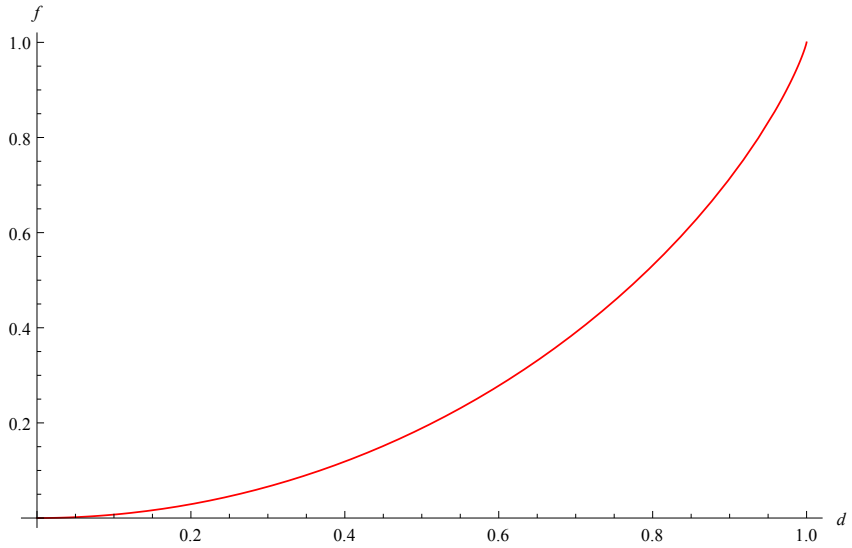


Figure 3.4: Mutual information for the couple of furthest points on the maximum volume ellipsoid with respect to the half-distance d between them. It is a monotonic increasing function of d and it reaches its maximum when the ellipsoid coincides with the whole Bloch sphere.

$$\begin{aligned} p_{-0}^{''AB} &= \frac{1}{4}(1 - \vec{r}_0^{\,''A} \cdot \hat{s}) \\ p_{+0}^{''AB} &= \frac{1}{4}(1 + \vec{r}_0^{\,''A} \cdot \hat{s}) \\ p_{-1}^{''AB} &= \frac{1}{4}(1 - \vec{r}_1^{\,''A} \cdot \hat{s}) \\ p_{+1}^{''AB} &= \frac{1}{4}(1 + \vec{r}_1^{\,''A} \cdot \hat{s}). \end{aligned} \tag{3.23}$$

$$\begin{aligned} p_{-}^{''A} = p_{-0}^{''AB} + p_{-1}^{''AB} &= \frac{1}{4}(2 - (\vec{r}_0^{\,''A} + \vec{r}_1^{\,''A}) \cdot \hat{s}) \\ p_{+}^{''A} = p_{+0}^{''AB} + p_{+1}^{''AB} &= \frac{1}{4}(2 + (\vec{r}_0^{\,''A} + \vec{r}_1^{\,''A}) \cdot \hat{s}) \\ p_{0}^{''B} &= \frac{1}{2} \\ p_{1}^{''B} &= \frac{1}{2}. \end{aligned} \tag{3.24}$$

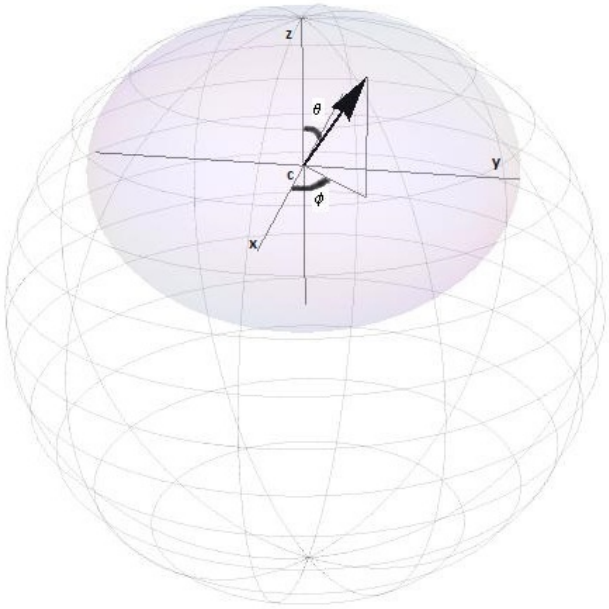


Figure 3.5: Spherical coordinates of centre $\vec{c} = (0, 0, c)$. $0 \leq \vartheta \leq \pi$ and $0 \leq \varphi \leq 2\pi$.

The mutual information is

$$\begin{aligned} H(A:B) = 1 &- \frac{1}{4}(2 - (\vec{r}_0^{\,\prime\prime A} + \vec{r}_1^{\,\prime\prime A}) \cdot \hat{s}) log[\frac{1}{4}(2 - (\vec{r}_0^{\,\prime\prime A} + \vec{r}_1^{\,\prime\prime A}) \cdot \hat{s})] \\ &- \frac{1}{4}(2 + (\vec{r}_0^{\,\prime\prime A} + \vec{r}_1^{\,\prime\prime A}) \cdot \hat{s}) log[\frac{1}{4}(2 + (\vec{r}_0^{\,\prime\prime A} + \vec{r}_1^{\,\prime\prime A}) \cdot \hat{s})] \\ &+ \frac{1}{4}(1 - \vec{r}_0^{\,\prime\prime A} \cdot \hat{s}) log[\frac{1}{4}(1 - \vec{r}_0^{\,\prime\prime A} \cdot \hat{s})] \\ &+ \frac{1}{4}(1 + \vec{r}_0^{\,\prime\prime A} \cdot \hat{s}) log[\frac{1}{4}(1 + \vec{r}_0^{\,\prime\prime A} \cdot \hat{s})] \\ &+ \frac{1}{4}(1 - \vec{r}_1^{\,\prime\prime A} \cdot \hat{s}) log[\frac{1}{4}(1 - \vec{r}_1^{\,\prime\prime A} \cdot \hat{s})] \\ &+ \frac{1}{4}(1 + \vec{r}_1^{\,\prime\prime A} \cdot \hat{s}) log[\frac{1}{4}(1 + \vec{r}_1^{\,\prime\prime A} \cdot \hat{s})]. \end{aligned} \tag{3.25}$$

It is appropriate to write $\rho_0^{\prime\prime A}$, $\rho_1^{\prime\prime A}$ and $\hat{s}$ in spherical coordinates (figure 3.5).

$$\vec{r}_0^{\,\prime\prime A} = \begin{cases} x_0 = -\sqrt{1-c}\sin\vartheta\cos\varphi \\ y_0 = -\sqrt{1-c}\sin\vartheta\sin\varphi \\ z_0 = -(1-c)\cos\vartheta + c \end{cases} \tag{3.26}$$

$$\vec{r}_1^{\,\prime\prime A} = \begin{cases} x_1 = \sqrt{1-c}\sin\vartheta\cos\varphi \\ y_1 = \sqrt{1-c}\sin\vartheta\sin\varphi \\ z_1 = (1-c)\cos\vartheta + c \end{cases} \tag{3.27}$$

$$\vec{s} = \begin{cases} s_x = -\sqrt{1-c}\sin\vartheta\cos\varphi \\ s_y = -\sqrt{1-c}\sin\vartheta\sin\varphi \\ s_z = -(1-c)\cos\vartheta \end{cases}, \tag{3.28}$$

where $0 \leq \vartheta \leq \pi$ and $0 \leq \varphi \leq 2\pi$. Note the third semiaxis is not flipped because of the necessity of positive lengths (remember $0 \leq c \leq 1$). Moreover

$$|\vec{s}| = \sqrt{(1-c)\sin^2\vartheta + (1-c)^2\cos^2\vartheta}. \tag{3.29}$$

A quick check to verify that $\hat{s}$ is the right vector to indicate Alice's optimal measurement consists of substituting, for example, $\vartheta = 0$ (the nearest points case). It results that $\hat{s} = (0, 0, \pm 1)$, *i.e.* $-\hat{s} = |0\rangle$ and $+\hat{s} = |1\rangle$ as expected.

Other useful quantities are

$$(\vec{r}_0^{\,\prime\prime A} + \vec{r}_1^{\,\prime\prime A}) \cdot \hat{s} = -\frac{2c(1-c)\cos\vartheta}{|\vec{s}|}$$

$$\vec{r}_0^{\,\prime\prime A} \cdot \hat{s} = \frac{(1-c)[1 - c\cos\vartheta(1+\cos\vartheta)]}{|\vec{s}|}$$

$$\vec{r}_1^{\,\prime\prime A} \cdot \hat{s} = -\frac{(1-c)[1 + c\cos\vartheta(1-\cos\vartheta)]}{|\vec{s}|}$$

It is now possible to evaluate again the mutual information:

$$\begin{aligned} H(A:B) = 1 &- \frac{1}{2}(1 + \frac{c(1-c)\cos\vartheta}{|\vec{s}|}))log[\frac{1}{2}(1 + \frac{c(1-c)\cos\vartheta}{|\vec{s}|})] \\ &- \frac{1}{2}(1 - \frac{c(1-c)\cos\vartheta}{|\vec{s}|})log[\frac{1}{2}(1 - \frac{c(1-c)\cos\vartheta}{|\vec{s}|})] \\ &+ \frac{1}{4}(1 - \frac{(1-c)[1 - c\cos\vartheta(1+\cos\vartheta)]}{|\vec{s}|})log[\frac{1}{4}(1 - \frac{(1-c)[1 - c\cos\vartheta(1+\cos\vartheta)]}{|\vec{s}|})] \\ &+ \frac{1}{4}(1 + \frac{(1-c)[1 - c\cos\vartheta(1+\cos\vartheta)]}{|\vec{s}|})log[\frac{1}{4}(1 + \frac{(1-c)[1 - c\cos\vartheta(1+\cos\vartheta)]}{|\vec{s}|})] \\ &+ \frac{1}{4}(1 + \frac{(1-c)[1 + c\cos\vartheta(1-\cos\vartheta)]}{|\vec{s}|})log[\frac{1}{4}(1 + \frac{(1-c)[1 + c\cos\vartheta(1-\cos\vartheta)]}{|\vec{s}|})] \\ &+ \frac{1}{4}(1 - \frac{(1-c)[1 + c\cos\vartheta(1-\cos\vartheta)]}{|\vec{s}|})log[\frac{1}{4}(1 - \frac{(1-c)[1 + c\cos\vartheta(1-\cos\vartheta)]}{|\vec{s}|})] \\ &\equiv g(c,\vartheta). \end{aligned} \tag{3.30}$$

Figure 3.6 plots the mutual information $g(c, \vartheta)$ for several values of ϑ. Some comments are now necessary.

1. $g(c, \vartheta)$ does not depend on φ. It is invariant over rotations around z-axis. This fact derives from the geometry of the ellipsoid: it is an oblate spheroid.

2. $g(c)$ reduces to $f(c)$ for $\vartheta = \frac{\pi}{2}$ as expected.

3. $g(c)$ reduces to $n(c)$ for $\vartheta \to 0$ as expected.

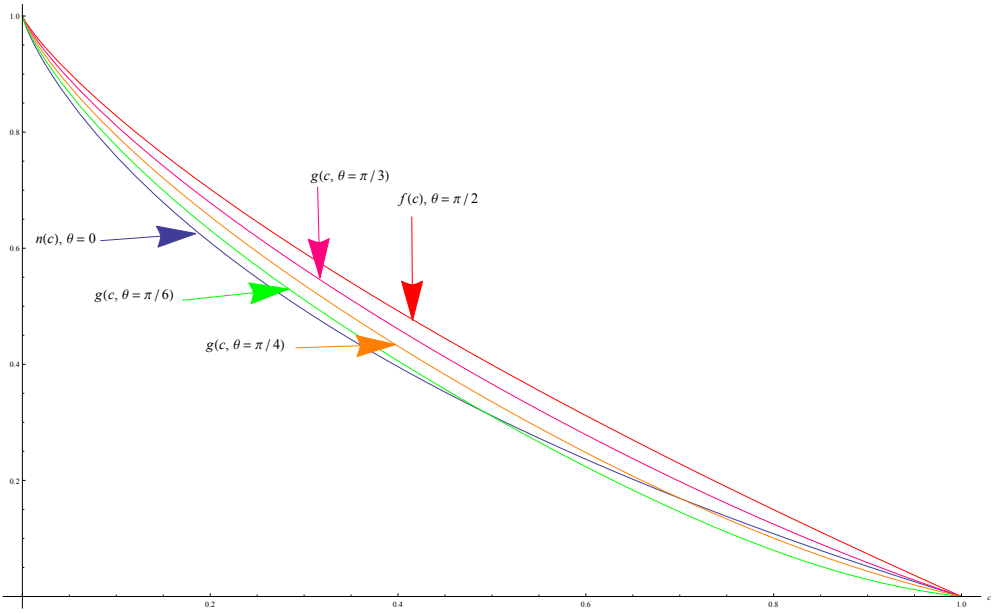


Figure 3.6: Mutual information for general couples of points on the maximum volume ellipsoid. The plot shows the mutual information for several values of ϑ: $0, \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}$. Note that $f(c)$ is the greatest function for every value of c, but $n(c)$ is not the lowest function for every value of c. This contradict our expectations. For values of ϑ such that $0 < \vartheta < \vartheta^* \simeq 0,31313 \simeq \frac{\pi}{3}$, $g(c)$ crosses $n(c)$. It means that over a certain value of c, in correspondence of the crossing point, $g(c) < n(c)$, *i.e.* the mutual information is lower for further points, even if we thought they should be more distinguishable.

4. The most astonishing fact is that while $f(c)$ is the greatest function for every value of c, $n(c)$ is not the lowest function for every value of c as expected. For values of ϑ such that $0 < \vartheta < \vartheta^* \simeq 0,31313 \simeq \frac{\pi}{3}$, $g(c)$ crosses $n(c)$.[3] This means that over a certain value of $c = c^*$, in correspondence to the crossing point, $g(c) < n(c)$, *i.e.* the mutual information is lower for further points, thus contradicting our previous intuitions. The idea of a direct dependence between points distance and mutual information crashes down. It is very unexpected because we thought of further points as more distinguishable: nearer to being classical and so corresponding to greater mutual information. What should this feature mean?

   Let us try to understand what geometrically and dynamically happens through studying the relation $c^* = c^*(\vartheta)$.

5. The crossing point $g(c^*) \to 1$ (for $c^* \to 0$) if $\vartheta \to 0$. $g(c^*) \to 0$ (for $c^* \to 1$) if $\vartheta \to \vartheta^*$. This means that if c^* is *small*, *i.e.* the ellipsoid is similar to the whole Bloch sphere, then this special behaviour can be observed only for small angles. On the other hand, if c^* is big, *i.e.* the ellipsoid is a small disk near to being a point of the sphere (the contact point between the ellipsoid and the Bloch sphere), then this special behaviour can be observed also for angles near

[3] the limit angle $\vartheta^* \simeq 0,31313$ has been found through an approximation based on a plots analysis.

to $\vartheta^* \simeq \frac{\pi}{3}$.

Figure 3.7 shows the relation $c^* = c^*(\vartheta)$, which is derived from from a numerical estimation because of the difficulty of solving the trascendental equation $g(c, \vartheta) = n(c)$.

6. It can be helpful to study the behaviour of the difference $\Delta H(A:B) = g(c, \vartheta') - n(c)$, for a fixed angle $0 < \vartheta' < \vartheta^*$, with respect to the centre of the ellipsoid c (see Figure 3.8). Firstly imagine the ellipsoid coincides with the Bloch sphere, *i.e.* $c = 0$, and calculate $\Delta H(A:B)$. Then imagine the centre of the ellipsoid increases. The ellipsoid shrinks and approaches the contact point. This implies that if we consider the nearest points on the surface N_1 and N_2 and two other generic opposite points on the surface G_1 and G_2, then $\Delta d = d(G_1, G_2) - d(N_1, N_2)$ increases[4] until a certain point c_{max} and then it rapidly decreases (see figure 3.9); *i.e.* N_1 and N_2 get close more rapidly than G_1 and G_2 until a given value $c = c_{max}(\vartheta)$, then Δd inverts its behaviour. It could be expected that $\Delta H(A:B)$ increases when Δd increases and it decreases when Δd decreases, but this is not the case. $\Delta H(A:B)$ changes sign when $c = c^* \neq c_{max}$.

   We have found neither a direct relation between the mutual information $H(A:B)$ and the distance $d(P_1, P_2)$ between two points on the ellipsoid , nor a relation between $H(A:B)$ and the *rapidity* with which the distance $d(P_1, P_2)$ changes.

7. It is interesting to note that by comparing for instance $g(c, \frac{\pi}{8})$ and $g(c, \frac{\pi}{12})$ the special behaviour does not arise just before $c = 1$, but in a small region between $C = 0.5$ and $c = 1$, leaving the region just before $c = 1$ unaffected by the special behaviour. In other words, the two functions intersect at two points in addition to $c = 0, 1$ instead of one, as for $n(c)$ and $g(c, \vartheta')$, with $\vartheta' < \vartheta^*$.

The next section will discuss what happens for generic couples *inside* the ellipsoid. We expect to find functions of c always located under $f(c)$ (3.3).

3.2 State vectors inside the ellipsoid, Bob's POVM

The first question to answer in Bob's POVM case is whether the number N_b of Bob's POVM elements coincides with the number N_a of Alice's optimal measurement elements on her N_b states. The answer is not so simple; it results that it is always possible to consider a situation in which $N_b = N_a$, even if , in general, $N_b \leq N_a$. This work will always assume $N_b = N_a = 2$ (because of the binary case).

The second necessary consideration is associated with the strategy to adopt. If we choose to consider generic couples of points inside Alice's steering ellipsoid it could make the calculations very cumbersome. One appropriate way to proceed is to consider couples of *opposite* points situated on the surface of ellipsoids centred at $\vec{c} = (0, 0, c)$ inside the steering one. Let us see how it works and why it is an appropriate choice.

3.2.1 Ellipsoids inside the steering one

If we assume that Alice's collapsed states are described by two opposite points on the surface of an ellipsoid inside the steering one, then they can be written in spherical coordinates as

[4]The function $d(P_1, P_2)$ indicates the euclidean distance between two points P_1 and P_2.

$$\vec{r}_0^{\,A} = \begin{cases} x_0 = -\alpha\sqrt{1-c}\sin\vartheta\cos\varphi \\ y_0 = -\beta\sqrt{1-c}\sin\vartheta\sin\varphi \\ z_0 = -\gamma(1-c)\cos\vartheta + c \end{cases} \tag{3.31}$$

$$\vec{r}_1^{\,A} = \begin{cases} x_1 = \alpha\sqrt{1-c}\sin\vartheta\cos\varphi \\ y_1 = \beta\sqrt{1-c}\sin\vartheta\sin\varphi \\ z_1 = \gamma(1-c)\cos\vartheta + c \end{cases}, \tag{3.32}$$

where α, β, γ are real coefficients such that $0 < \alpha, \beta, \gamma \leq 1$. The 4-vector describing Alice's optimal measurement $\tilde{s}$ is given, according to the maximum likelihood discrimination (see B), by $s_0 = 1$ and $\vec{s} = \frac{X_0}{2}\vec{r}_0^{\,A} - (1 - \frac{X_0}{2})\vec{r}_1^{\,A}$, where X_0 denotes the first component of the 4-vector describing Bob's measurement element Π^B. In order to evaluate $\vec{s}$, note that

$$\frac{X_0}{2}\rho_0^A + (1 - \frac{X_0}{2})\rho_1^A = \rho^A = \frac{1}{2}(\mathbb{I} + c\sigma_z)$$

$$\frac{X_0}{2}[\frac{1}{2}(\mathbb{I} + \vec{r}_0^{\,A}\vec{\sigma})] + (1 - \frac{X_0}{2})[\frac{1}{2}(\mathbb{I} + \vec{r}_1^{\,A}\vec{\sigma})] = \frac{1}{2}\mathbb{I} + \frac{c}{2}\sigma_z$$

$$\frac{1}{2}\mathbb{I} + [\frac{X_0}{4}(\vec{r}_0^{\,A} - \vec{r}_1^{\,A}) + \frac{\vec{r}_1^{\,A}}{2}] = \frac{1}{2}\mathbb{I} + \frac{c}{2}\sigma_z,$$

hence

$$\begin{cases} -\frac{X_0}{2}\alpha\sqrt{1-c}\sin\vartheta\cos\varphi + \frac{1}{2}\alpha\sqrt{1-c}\sin\vartheta\cos\varphi = 0 \\ -\frac{X_0}{2}\beta\sqrt{1-c}\sin\vartheta\sin\varphi + \frac{1}{2}\beta\sqrt{1-c}\sin\vartheta\sin\varphi = 0 \\ -\frac{X_0}{2}\gamma(1-c)\cos\vartheta + \frac{1}{2}(c + \gamma(1-c)\cos\vartheta) = c \end{cases},$$

and so

$$\begin{cases} X_0\alpha\sqrt{1-c}\sin\vartheta\cos\varphi = \alpha\sqrt{1-c}\sin\vartheta\cos\varphi \\ X_0\beta\sqrt{1-c}\sin\vartheta\sin\varphi = \beta\sqrt{1-c}\sin\vartheta\sin\varphi \\ X_0\gamma(1-c)\cos\vartheta = \gamma(1-c)\cos\vartheta \end{cases}.$$

This system of equations has a solution if and only if $X_0 = 1$. This result implies that $p = p(\Pi^B) = tr(\rho^B\Pi^B) = \frac{X_0}{2} = \frac{1}{2}$ and so the probability distributions 3.23 and 3.24 are still valid. The fact that $p = \frac{1}{2}$ could also be intuitively deduced by considering that opposite points on an ellipsoid are equally distant from its centre which, in this case, corresponds to the state vector representing ρ^A. This very useful simplification implies that

$$\vec{s} = \begin{cases} s_x = -\alpha\sqrt{1-c}\sin\vartheta\cos\varphi \\ s_y = -\beta\sqrt{1-c}\sin\vartheta\sin\varphi \\ s_z = -\gamma(1-c)\cos\vartheta \end{cases}. \tag{3.33}$$

Some necessary quantities to calculate the mutual information are

$$(\vec{r}_0^{\,A} + \vec{r}_1^{\,A}) \cdot \hat{s} = -\frac{2c\gamma(1-c)\cos\vartheta}{|\vec{s}|}$$

$$\vec{r}_0^A \cdot \hat{s} = \frac{(1-c)\sin^2\vartheta(\alpha^2\cos^2\varphi\alpha^2 + \beta^2\sin^2\varphi) - \gamma(1-c)c\cos\vartheta + \gamma^2(1-c)^2\cos^2\vartheta}{|\vec{s}|}$$

$$\vec{r}_1^A \cdot \hat{s} = \frac{-(1-c)\sin^2\vartheta(\alpha^2\cos^2\varphi\alpha^2 + \beta^2\sin^2\varphi) - \gamma(1-c)c\cos\vartheta - \gamma^2(1-c)^2\cos^2\vartheta}{|\vec{s}|},$$

where $\hat{s} = \frac{\vec{s}}{|\vec{s}|}$ and

$$|\vec{s}| = \sqrt{\alpha^2(1-c)\sin^2\vartheta\cos^2\varphi + \beta^2(1-c)\sin^2\vartheta\sin^2\varphi + \gamma^2(1-c)^2\cos^2\vartheta} \tag{3.34}$$

It is now possible to evaluate the mutual information for couples of opposite points inside the steering ellipsoid, situated on the surface of an ellipsoid centered at $\vec{c} = (0, 0, c)$:

$$\begin{aligned} H(A:B) = 1 &- \frac{1}{4}(2 - (\vec{r}_0^A + \vec{r}_1^A)\cdot\hat{s})log[\frac{1}{4}(2 - (\vec{r}_0^A + \vec{r}_1^A)\cdot\hat{s})] \\ &- \frac{1}{4}(2 + (\vec{r}_0^A + \vec{r}_1^A)\cdot\hat{s})log[\frac{1}{4}(2 + (\vec{r}_0^A + \vec{r}_1^A)\cdot\hat{s})] \\ &+ \frac{1}{4}(1 - \vec{r}_0^A\cdot\hat{s})log[\frac{1}{4}(1 - \vec{r}_0^A\cdot\hat{s})] \\ &+ \frac{1}{4}(1 + \vec{r}_0^A\cdot\hat{s})log[\frac{1}{4}(1 + \vec{r}_0^A\cdot\hat{s})] \\ &+ \frac{1}{4}(1 - \vec{r}_1^A\cdot\hat{s})log[\frac{1}{4}(1 - \vec{r}_1^A\cdot\hat{s})] \\ &+ \frac{1}{4}(1 + \vec{r}_1^A\cdot\hat{s})log[\frac{1}{4}(1 + \vec{r}_1^A\cdot\hat{s})] \\ &\equiv i(c, \vartheta, \varphi, \alpha, \beta, \gamma). \end{aligned} \tag{3.35}$$

Let us now try to interpret the above expression.

3.2.2 Classification of results

The mutual information 3.35 depends on six variables. The idea is to choose a fixed value of $\varphi, \alpha, \beta, \gamma$ and see the behaviour of the function $i(c, \vartheta, \varphi, \alpha, \beta, \gamma)$ with respect to c for different values of ϑ. We will start by considering a quite general case: $\alpha \geq \beta \geq \gamma$, *e.g.* $\alpha = 0.6, \beta = 0.5, \gamma = 0.4$ (so the z-axis is always the smallest and the x-axis is always the greatest). Its plot shows, for fixed values of φ, a behaviour as a *fan*, instead of the typical behaviour as a *banana* for the mutual information of couples of opposite points on the surface of the steering ellipsoid. Note that the fan behaviour includes also the special behaviour.

Except for the special behaviour, the fan behaviour can be explained in terms of a direct relation between the euclidean distance and the mutual information. The lowest function corresponds to the couple of nearest points and by increasing the value of ϑ the function increases. The functions do not cross at $c = 0$ because at $c = 0$ the ellipsoid does not become a sphere as it does for the steering ellipsoid. Moreover, it results that varying the value of φ from $\frac{\pi}{2}$ to 0 the special behaviour is shifted towards $c = 1$ and also the limit angle ϑ^* gradually has a lower value. In order to get a better understanding of the case above and how far a direct relation between the euclidean distance and the mutual information can hold, let us see some particular cases:

1. $\alpha = \beta = \gamma$. the opposite points are situated on the surface of an ellipsoid similar to the steering one.

2. $\alpha = \gamma$ or $\beta = \gamma$. the opposite points are situated on the surface of an ellipsoid which mantains the same proportion between one of the major axes and the minor axis with respect to the steering ellipsoid.

3. $\alpha = \beta \gg \gamma$. The opposite points are situated on the surface of an oblate spheroid which looks like an orizontal disk.

Case 1 shows, as intuitively expected, a banana behaviour like the case of the opposite points on the surface of the steering ellipsoid. The only difference is that now all the different functions (with different values of ϑ) intersect (at $c = 0$) at $i(c) \neq 1$. If the values of the coefficients are much smaller than the ones in the figure (*e.g.* $\alpha = \beta = \gamma = 0.1$), it is very difficult to recognize a Banana, because all functions become almost the same and very closer to the x-axis (this derives from the fact that all points become closer).

Case 2 needs further explaination:

1. if $\alpha = \gamma$ and $\varphi = 0$ or if $\beta = \gamma$ and $\varphi = \frac{\pi}{2}$, then the plot shows a banana behaviour with a crossing point(at $c = 0$) at $i(c) \neq 1$. If the values of the coefficients are smaller than those in the figure, the banana turns into a fan. Therefore the fan can be interpreted as a right part of the banana.

2. if φ is respectively different from 0 and $\frac{\pi}{2}$, then the plot shows a fan.

Case 3 shows a fan behaviour, but without the presence of the special behaviour. It derives from the fact that the nearest points are very closer to one another. In particular if the values of α, β are a bit closer to γ, then the fan shows the special behaviour and this case reduces to the general one. Instead of an orizontal disk ($\alpha = 0.8, \beta = 0.8, \gamma = 0.1$) we can also consider, for instance, an orizontal needle ($\alpha = 0.8, \beta = 0.1, \gamma = 0.1, \varphi = 0$) or a vertical needle ($\alpha = 0.1, \beta = 0.1, \gamma = 0.8$), and the behaviour is the same.

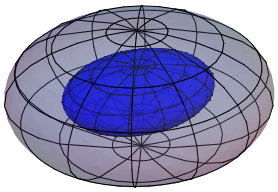
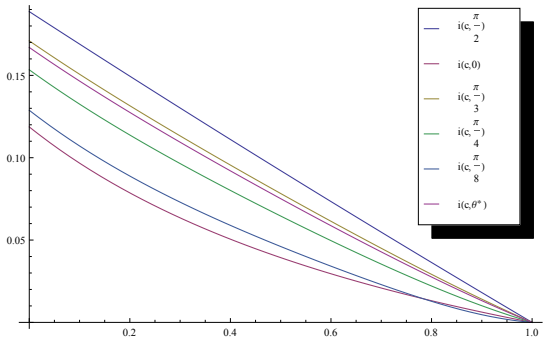
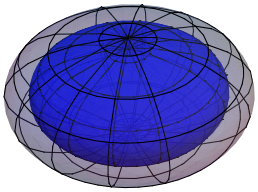
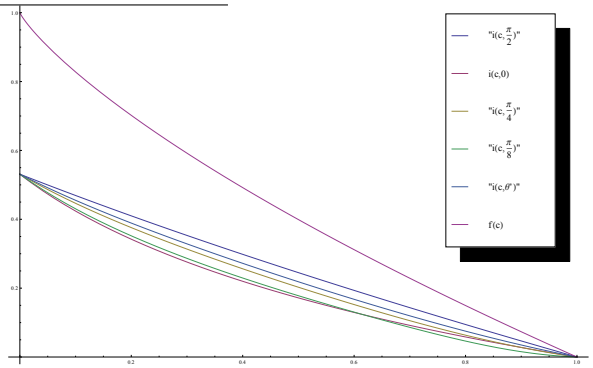
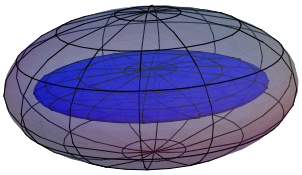
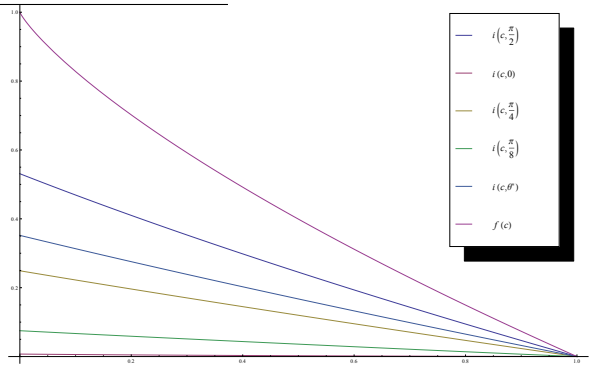
We can sum up the previous reasonings by stating that, in general, the plots are easily interpretable in terms of the relation between the euclidean distance and the mutual information, except for the *special* behaviour which arises, as expected, like in the steering ellipsoid case. It is possible to intuitively interpret the behaviour of the mutual information in terms of the euclidean distance when the difference between the distances of couples of points is significant, *i.e.* the coulples of points considered are not close to each other (in general high values of ϑ and small values of φ). When these differences are slightly perceptible, *i.e.* small values of ϑ and high values of φ, the special behaviour arises.

The table 3.1 shows all the above cases.

In order to understand the special behaviour, consider now the interesting case in which one of the steering ellipsoid's major axes are reduced more than the minor axis, *e.g.* $\alpha = 0.6, \beta = 0.3, \gamma = 0.4$, so the x-axis is always the greatest, but for the smallest axis the situation is different: if $c < \bar{c} = 0.4375$ the y-axis is the smallest, if $c > \bar{c}$ the z-axis is the smallest (see figure 3.10). Table 3.2 shows all the possible kind of behaviours varying φ. It results that going from $\varphi = 0$ to $\varphi = \frac{\pi}{2}$ the plots show the following situation:

- if $\varphi = 0$ the plot is a fan with the special behaviour which is practically nonexistent because it is really close to $c = 1$.

Table 3.1: Mutual information for points inside the steering ellipsoid: some cases. The table shows, in order,
1) A general case with $\alpha = 0.6, \beta = 0.5, \gamma = 0.4$ and $\varphi = \frac{\pi}{2}$ (it is not important the value of φ), but note that $\alpha, \beta > \gamma$.
2) An ellipsoid similar to the steering one, $\alpha = \beta = \gamma = 0.8$. The same plot arises by taking either $\alpha = \gamma$ and $\varphi = 0$ or $\beta = \gamma$ and $\varphi = \frac{\pi}{2}$.
3)An orizontal Disk, $\alpha = \beta = 0.8, \gamma = 0.1$. It could be chosen, for example, a vertical needle ($\alpha = 0.1, \beta = 0.1, \gamma = 0.8$) or an orizontal needle ($\alpha = 0.8, \beta = 0.1, \gamma = 0.1, \varphi = 0$).
Note that every plot shows that all functions are lower than $f(c)$. It is a lower bound to the accessible information for a two qubit system.

Case	Plot
	
	
	

- if $\varphi = \frac{\pi}{4}$ the plot is a fan, but the special behaviour is now well visible because it is further from $c = 1$ than the previous case. Note that the fan tends to shrink near $c = 0$.

- if $\varphi = \frac{\pi}{3}$ the plot is almost a banana.The fan is completely shrunk until reaching a crossing point at (almost) $c = 0$.

- if $\varphi = \frac{17\pi}{48}$ the plot shows a *hair clip* behaviour, *i.e.* the banana crossing point shifts down towards $c = 1$ and leave at its left an opposite behaviour with respect to its right: the function which were greater become smaller and vice versa. The hair clip behaviour shows the special behaviour for certain values of ϑ.

- if $\varphi = \frac{\pi}{2}$ the plot is a hair clip, but there are many different crossing points in correspondence with the different values of ϑ. The hair clip behaviour is shifted towards $c = 1$.

The evolution of the plot is clear: for $\varphi = 0$ it is an 'open' fan with the strange behaviour near $c = 1$, then the crossing point c^* denoting the stange behaviour gradually 'climbs' the slope of the functions until arriving, at $\varphi \simeq \frac{\pi}{3}$, at $c = 0$. At that point the strange behaviour arises again near $c = 1$. After the banana behaviour the crossing point which arose at $c = 0$ moves down towards $c = 1$ and, at its left, the plot shows the inverse behaviour with respect to its right: the function which were greater become smaller and vice versa . This may happen in correpsondence with the inversion of the behaviour between the distances: couples of points which were closer than others, become more distant. By varying φ towards $\frac{\pi}{2}$ the hair clip moves down to $c = 1$ and it no longer shows a single crossing point.

The most interesting aspect of this case is the hairclip behaviour. We expect that the typical crossing point of the hair clip appears in correspondence with the point at which there is the inversion of the distances. However it is not true. There exists a slight deviation. Consider for example the sharp case of $\varphi = \frac{17\pi}{48}$ and the functions corresponding to $\vartheta = 0$ and $\vartheta = \frac{\pi}{8}$ (see figure 3.11). In this case the point at which the distances invert their behaviour is given by the solution of the equation

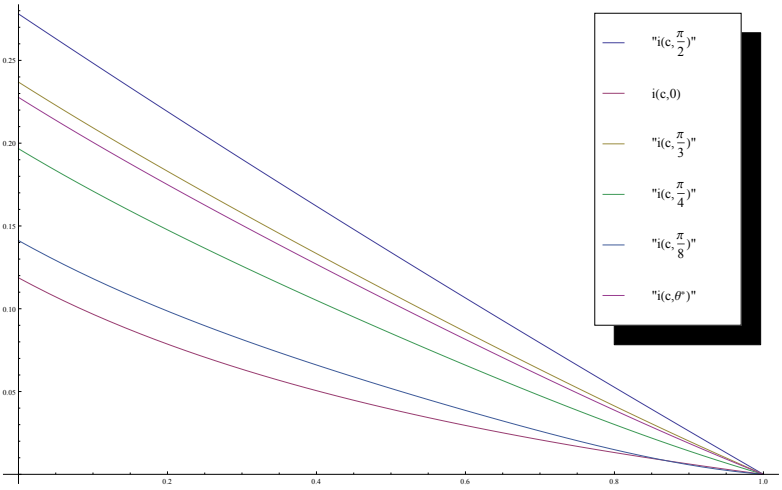
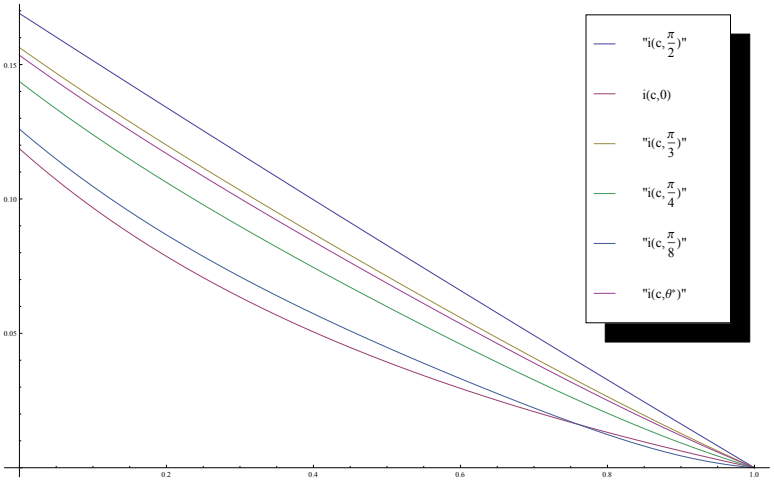
$$\sqrt{(0.6\sqrt{(1-c)}\sin\frac{\pi}{8}\cos\frac{17\pi}{48})^2 + (0.3\sqrt{(1-c)}\sin\frac{\pi}{8}\sin\frac{17\pi}{48})^2 + (0.4(1-c)\cos\frac{\pi}{8})^2}$$
$$= 0.4(1-c)\cos 0,$$

which is $\bar{c}' = 0.107392$. The crossing point between the functions representing the mutual information is $\bar{c}^* = 0.12217$. Therefore our expectation is incorrect. There exists another special behaviour: for c such that $\bar{c}' < c < \bar{c}^*$ couples of nearer opposite points have a greater mutual information than couples of further opposite points.

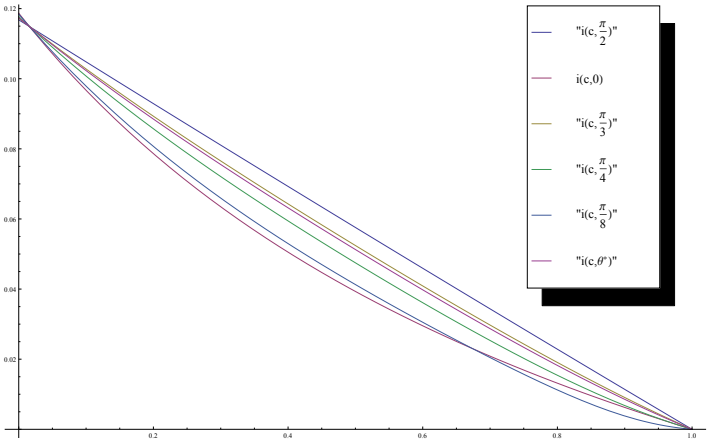
There may exist an identity between the difference $D = \bar{c}^* - \bar{c}'$ (inversion-mutual information-point and inversion-distance-point) and $D' = c^* - 1$ (crossing point of the usual special behaviour and $c = 1$, where the distances between all points coincide), even if in the first case the inversion behaviour of the mutual information is delayed and in the second case it is in advance with respect to the inversion behaviour of the distances. Unfortunately $D = 0.014778 \neq D' \simeq -0.37$ and it is a very difficult task to find a relation between $D(\vartheta, \varphi)$ and $D'(\vartheta, \varphi)$.

We can conclude this cumbersome reasoning by highlighting that when the difference between the distances of couples of points is slightly perceptible, really particular behaviours arise.

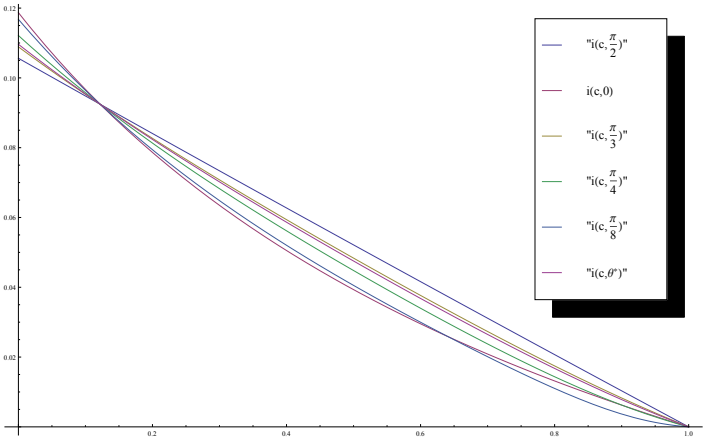
Table 3.2: The evolution of the mutual information for points inside the steering ellipsoid with $\alpha = 0.6, \beta = 0.3, \gamma = 0.4$ for different values of φ. When $\varphi = 0$ the plot is an 'open' fan with the strange behaviour near $c = 1$, then the crossing point c^* denoting the stange behaviour gradually 'climbs' the slope of the functions (as for $\varphi = \frac{\pi}{4}$) till arriving, at $\varphi \simeq \frac{\pi}{3}$, at $c = 0$. At that point the strange behaviour arises again near $c = 1$. After the banana behaviour, at $\varphi = \frac{17\pi}{48}$, the crossing point which arose at $c = 0$ moves down towards $c = 1$ and, at its left, the plot shows the inverse behaviour with respect to its right: the function which were greater become smaller and vice versa .It is interesting that it does not happen in correpsondence with the inversion of the behaviour between the distances, but for bigger values of c . Varying φ towards $\frac{\pi}{2}$ the hair clip moves down to $c = 1$ and it does not show a single crossing point anymore.

Case	Plot
$\varphi = 0$, Open Fan Behaviour	
$\varphi = \frac{\pi}{4}$, Fan Behaviour	

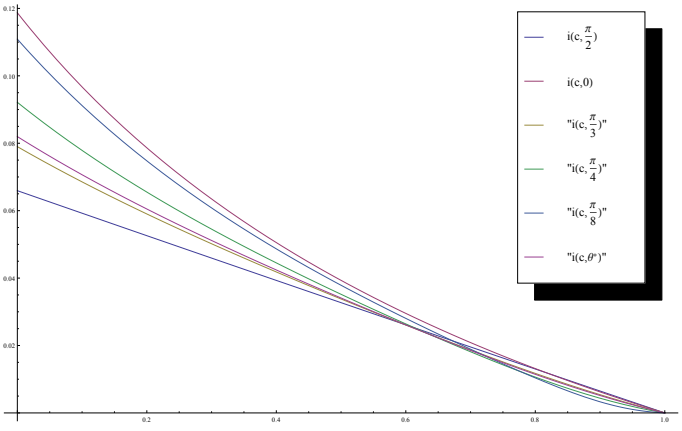
$\varphi = \frac{\pi}{3}$, Banana Behaviour



$\varphi = \frac{17\pi}{48}$, Hair Clip Behaviour (Single Crossing Point)



$\varphi = \frac{\pi}{2}$, Hair Clip Behaviour (Multiple Crossing Point)



The introduction of the symmetry between points inside the steering ellipsoid (opposite to the centre of an ellipsoid) has allowed us to simplify the calculations ($X_0 = 1$, $p = \frac{1}{2}$) and describe more features of the mutual information also in the case of Bob's POVM. It would be useful to consider generic couples of points inside Alice's steering ellipsoid ($X_0 \neq 1$, $p \neq \frac{1}{2}$). However this implies the addition of other four parameters to the function: three to define the components of $\vec{r}_1^A$ and another which is $X_0 \neq 1$ and the calculations result really cumbersome.

We expect to find the functions expressing the mutual information always lower than $f(c)$, since we have experienced that special behaviours of the mutual information arise far from $f(c)$. For the purpose of this work we have sufficient results for reliable considerations.

Beyond all these attempts to interpret the behaviour of the mutual information for points inside the steering ellipsoid, in order to find the accessible information the principal aspect to stress is that $i(c, \vartheta, \varphi, \alpha, \beta, \gamma) \leq f(c)$ for each value of $\vartheta, \varphi, \alpha, \beta, \gamma$ in their domain and the equality holds only if $\{\vartheta = \frac{\pi}{2}, \varphi = 0, \alpha = \beta = \gamma = 1\}$ or if $\{c = 0, \alpha = \beta = \gamma = 1\}$ (couples of points on the surface of the steering ellipsoid which coincides with the whole Bloch sphere) or if c=1 (the steering ellipsoid coincides with a point).

Hence $f(c)$ is a lower bound for the accessible information in a two-qubit system. It is possible that by involving more than two measurement elements or considering more general states, *e.g.* generic canonical states, the mutual information becomes greater than $f(c)$, but we are certain that the accessible information, *i.e.* the maximum of the mutual information over all possible schemes of measure, is not smaller than $f(c)$.

It is important now to compare the lower bound $f(c)$ with the most famous of the already known lower bounds: the Josza-Robb-Wootters lower bound (1.39). In the current case it states that:

$$H(A:B) \geq Q(\rho^A) - \frac{1}{2}Q(\rho_0^A) - \frac{1}{2}Q(\rho_1^A) \equiv l(c), \tag{3.36}$$

where the subentropy $Q(\rho^A)$ of ρ^A is given by

$$Q(\rho^A) = \frac{\lambda_0^A}{\lambda_0^A - \lambda_1^A}\lambda_0^A \log \lambda_0^A + \frac{\lambda_1^A}{\lambda_1^A - \lambda_0^A}\lambda_1^A \log \lambda_1^A. \tag{3.37}$$

The eigenvalues of $\rho^A = \frac{1}{2}(\mathbb{I} + c\sigma_z) = \begin{pmatrix} \frac{1+c}{2} & 0 \\ 0 & \frac{1-c}{2} \end{pmatrix}$ are $\lambda_0^A = \frac{1+c}{2}$ and $\lambda_1^A = \frac{1-c}{2}$. Through considering the furthest points decomposition of ρ^A,[5] $\rho_0^A = \frac{1}{2}(\mathbb{I} - \sqrt{1-c}\sigma_x + c\sigma_z) = \begin{pmatrix} \frac{1+c}{2} & \frac{-\sqrt{1-c}}{2} \\ \frac{-\sqrt{1-c}}{2} & \frac{1-c}{2} \end{pmatrix}$ and $\rho_1^A = \frac{1}{2}(\mathbb{I} + \sqrt{1-c}\sigma_x + c\sigma_z) = \begin{pmatrix} \frac{1+c}{2} & \frac{\sqrt{1-c}}{2} \\ \frac{\sqrt{1-c}}{2} & \frac{1-c}{2} \end{pmatrix}$, then the eigenvalues are $\lambda_0^0 = \lambda_0^1 = \frac{1}{2}(1 - \sqrt{1-c+c^2})$ and $\lambda_1^0 = \lambda_1^1 = \frac{1}{2}(1 + \sqrt{1-c+c^2})$. By substituting the above values in $l(c)$ it is possible to compare $f(c)$ and $l(c)$. Figure 3.12 shows that $l(c)$ is a worse lower bound than $f(c)$ since it is always lower (except, obviously, at $c = 0, 1$). The figure also shows the Holevo upper bound. In the current case it is given by

$$H(A:B) \leq S(\rho^A) - \frac{1}{2}S(\rho_0^A) - \frac{1}{2}S(\rho_1^A) \equiv \chi(c), \tag{3.38}$$

[5] It is obviously the most natural choice in order to maximise the value of $l(c)$.

where $S(\rho^A)$ is the well known Von Neumann entropy 1.2.

In the end we can conclude that the accessible information certainly belongs to the region $f(c) \leq H(A:B) \leq \chi(c)$.

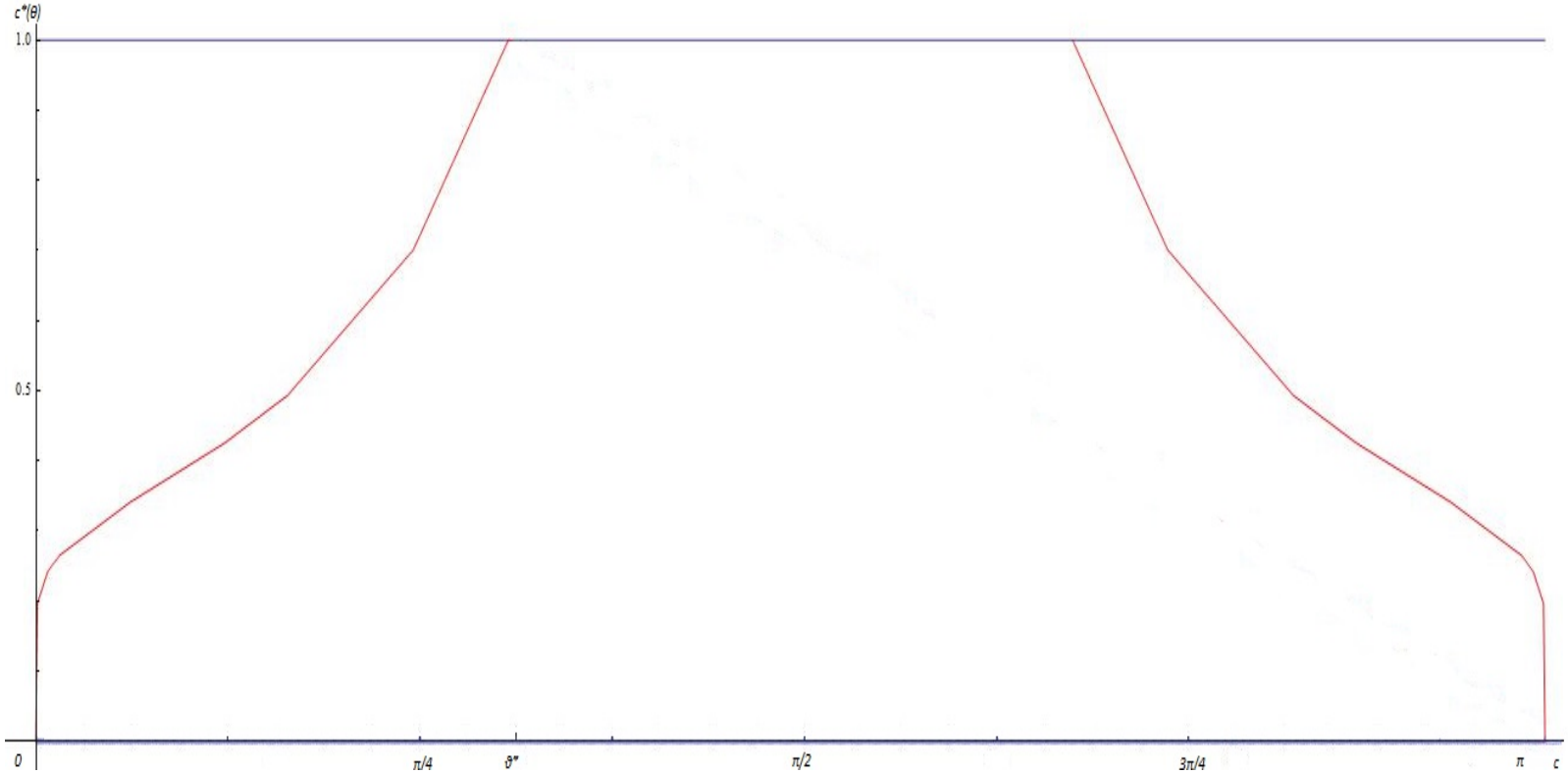


Figure 3.7: Relation between the crossing point and the angle $c^* = c^*(\vartheta)$. Note that for $c = 0, 1$ all functions - for every value of ϑ - coincide. The 'special' crossing point c^* arises for those functions $g(c, \vartheta)$ such that either $0 < \vartheta < \vartheta^*$ or $\pi - \vartheta^* < \vartheta < \pi$.

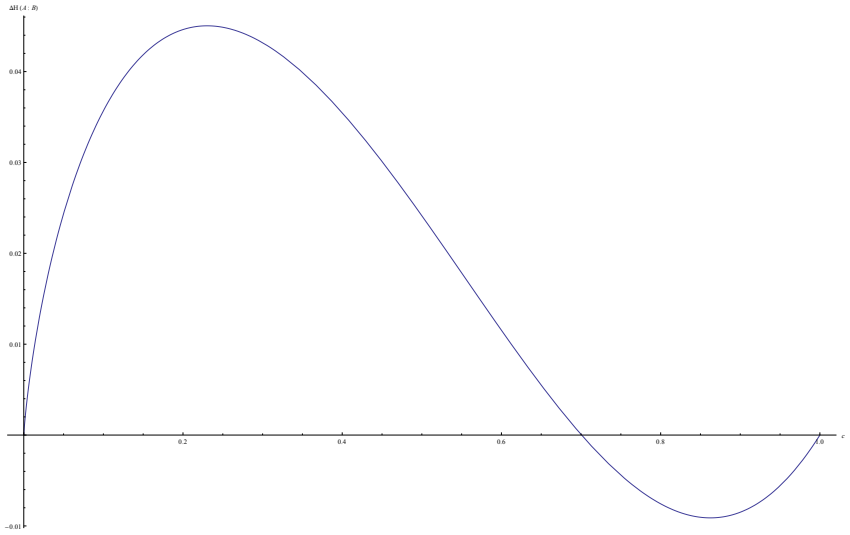


Figure 3.8: Difference of mutual information between general couples of points and the nearest points on the ellipsoid's surface for $\vartheta = \frac{\pi}{4}$. Note that in correspondence of the crossing point $c^* \simeq 0,700645$, $\Delta H(A:B) = g(c,\vartheta') - n(c)$ changes its sign. It decreases when c approaches c^* and it increases when c overreaches c^*. When c approaches 'one' it decreases again like every $g(c,\vartheta)$ do for each value of ϑ, according to the fact that the ellipsoid reduces to a point for $c = 1$. Moreover comparing the above figure with figure 3.9 we can see that there is no relation between $H(A:B)$ and the *rapidity* with which the distance $d(P_1,P_2)$ between two points changes.

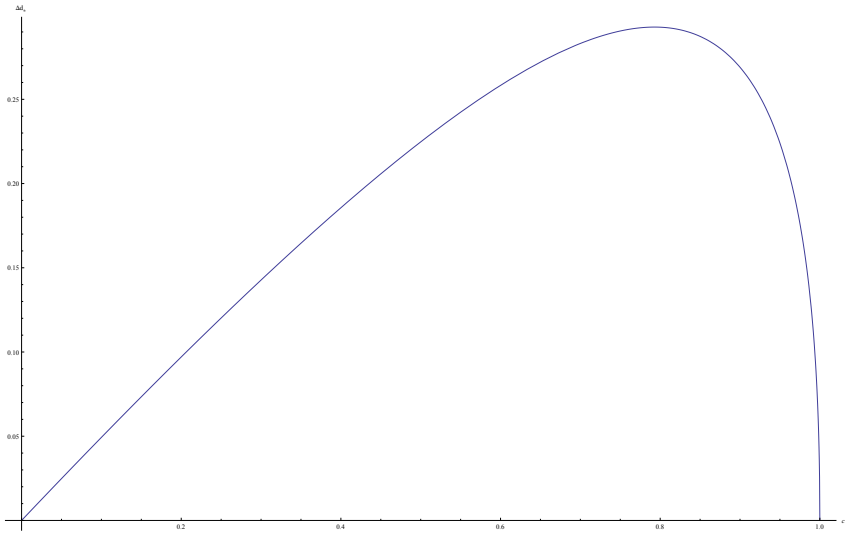


Figure 3.9: Difference between distances of couples of points on the surface of the ellipsoid as a function of c for $\vartheta = \frac{\pi}{4}$.Note that the function increases until c is near to one. This implies that it decreases very rapidly at the end.

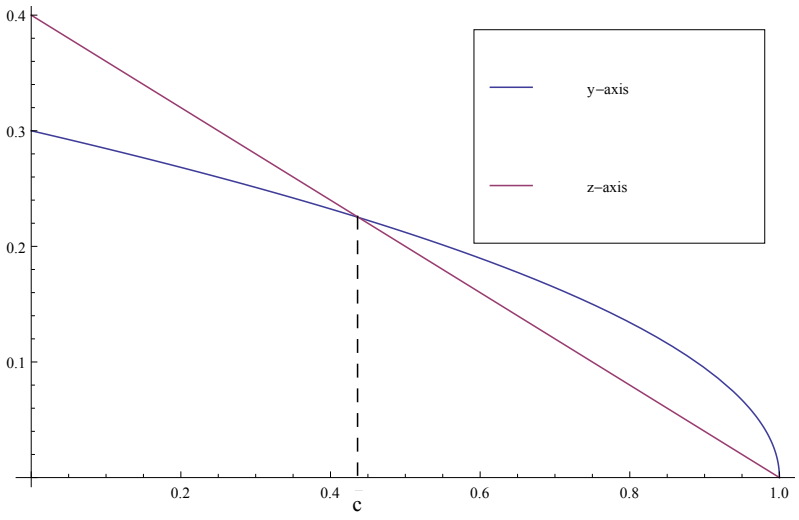


Figure 3.10: $y-$axis and $z-$axis behaviour for $\alpha = 0.6, \beta = 0.3, \gamma = 0.4$. Note that at $\bar{c} = 0.4375$ the $z-$axis becomes smaller than the $y-$axis.

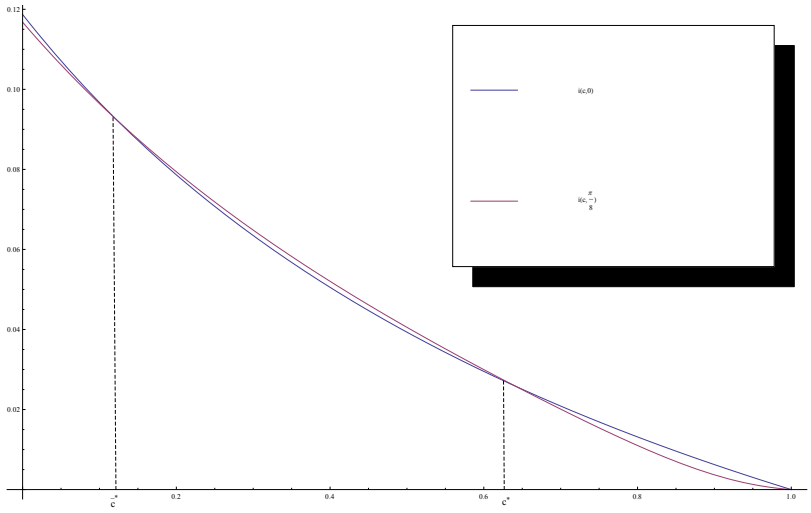


Figure 3.11: Mutual Information for couples of opposite points inside the steering ellipsoid with $\alpha = 0.6, \beta = 0.3, \gamma = 0.4, \varphi = \frac{17\pi}{48}$ for $\vartheta = 0$ and $\vartheta = \frac{\pi}{8}$. Note that the plot shows both the usual special behaviour near $c = 1$ and another crossing point. The latter should be linked to the inversion of the behaviour of the distances, but it does not happen for the same value of c.

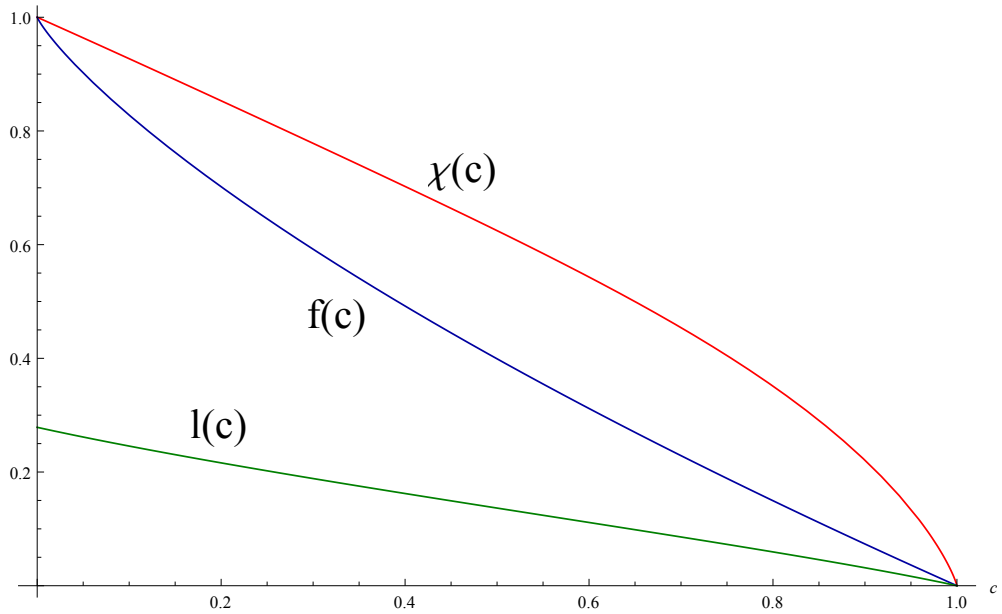


Figure 3.12: Mutual information: lower and upper bounds. The accessible information certainly belongs to the region $f(c) \leq H(A:B) \leq \chi(c)$, *i.e.* between the quantity $f(c)$ and the Holevo quantity $\chi(c)$. Note that the Josza-Robb-Wootters quantity $l(c)$ is a worse lower bound than $f(c)$ in the general two qubit case.

Chapter 4

Conclusion

Dealing with the accessible information in a two qubit system is an intricate issue, since it involves a maximization over all possible measurement schemes and trascendent logarithmic expressions. The assumption of the binary measurement elements case considerably simplifies the situation, but it does not remove the pitfalls. In order to face the problem of considering all possible measurement schemes it is necessary to develop a method to find the optimal measurement scheme, since it is not possible to explore all the possible ones. The maximum likelihood discrimination allows to find this optimal measurement scheme in a very simple and intuitive way. This method is strictly related to the concept of *trace distance*, a measure of the distinguishability between states.

The quantum steering ellipsoids formalism and the specific choice of considering maximum volume states allows to geometrically see the states and their correlations and perform quite easy calculations. The choice of using the trace distance for two qubits implies to think of two states represented by vectors belonging to the steering ellipsoid as more distinguishable if they are more distant.[1] Therefore their mutual information, which is directly related to the distinguishability of two states, has to increase if the states are more distinguishable, and so described by more distant points.

Unexpectedly sometimes the mutual information for a couple of closer points is greater than the mutual information for a couple of further points. In general it happens when the distance difference between the two couples is small and these couples are far from the couple of furthest points of the steering ellipsoid. Another special behaviour arises by considering couples of opposite points inside the steering ellipsoid: in the case that the distance of a couple of closer points becomes greater than the distance of a couple of further points, the value of the centre at which it arises does not coincide with the value of the centre at which their mutual information inverts. It is not clear how to proceed to understand these special behaviours, despite several attempts have been done, *e.g* studying how rapidly the distances between couples of points change with respect to the centre. These special behaviours probably show that the maximum likelihood discrimination, based on the trace distance concept, is not the appropriate measure of distinguishability between quantum states. It works only for quite distant couples of points.

The other famous measure of distinguishability between states is the *fidelity* (see [11]), but it has not a clear and intuitive interpretation as the trace distance (for

[1] This fact derives from the expression of the trace distance 1.3.2 for two qubits in terms of the euclidean distance between their state vectors in the Bloch sphere.

example it is not a metric). The next step in order to obtain new insights about the special behaviours of the mutual information may consist of choosing an optimal measurement method related to fidelity and studying its relation with the mutual information.

Another comment on the choice of the system of coordinates. The spherical coordinates system seems to be the best and most natural system of coordinates in order to study the mutual information for couples of opposite points on an ellipsoid, but another choice could highlight some key features which are now obscure, *e.g.* ellipsoidal coordinates system.

Beyond these special behaviours, the main result of this work is that the mutual information of the couple of furthest points on the steering ellipsoid $f(c)$ is a lower bound to the accessible information of a two-qubit system. It is given by

$$f(c) = \frac{1}{2}[\log c + 2\sqrt{1-c}\log(\frac{1+\sqrt{1-c}}{\sqrt{c}})].$$

It could be that involving more than two measurement elements or considering more general states, *e.g.* generic canonical states, the mutual information becomes greater than $f(c)$, but it is certain that the accessible information is not lower than $f(c)$. The mutual information $f(c)$ arises when Bob performs a PVM in basis $\{|-\rangle, |+\rangle\}$ and Alice performs a PVM in basis $\{|-\rangle, |+\rangle\}$.

It results that $f(c)$ is a tighter lower bound than the already known Josza-Robb-Wootters lower bound and by considering the famous Holevo upper bound we conclude that the accessible information for a two qubit system belongs to $f(c) \leq H(A:B) \leq \chi(c)$.

The next step in order to improve this limit and the knowledge of the accessible information consists of studying the case of measurements composed of three elements and refering to the more general canonical states. This fact implies more difficult calculations and a the necessity of a new method to substitute the optimal measurement one in order to maximise the mutual information. A common method in this case is the so called *pretty good measurements* method ([4]); a new one is the *SIC measurements* method ([8]).

Appendix A

Bob's PVM

The purpose of this Appendix is to state and prove the following theorems.

Suppose Bob steers Alice's qubit to two states ρ_0 and ρ_1 represented by state vectors $\vec{r}_0$ and $\vec{r}_1$ with respective probabilities p_0 and p_1.

Suppose also Alice's steering ellipsoid represents a *maximum volume state*, a special case of *canonical states*, *i.e.* $\vec{a} = \vec{c}$ and $\vec{b} = 0$.

Theorem 1.

If Alice's state vectors $\vec{r}_0$ and $\vec{r}_1$ are opposite vectors situated on the surface *of her steered ellipsoid, then*

1. $p_0 = \frac{1}{2} = p_1$.
2. *Bob has performed a PVM.*

Theorem 2.

Vice versa *if Bob performs a* PVM *composed by two elements $\{M_0, M_1 = \mathbb{I} - M_0\}$, then*

1. $p_0 = \frac{1}{2} = p_1$.
2. *$\vec{r}_0$ and $\vec{r}_1$ are opposite vectors situated on the* surface *of Alice's steered ellipsoid.*

Therefore, for maximum volume states, the fact that Bob performs a PVM is equivalent to say that Alice's state vectors are situated on the surface of her steered ellipsoid.

Proof 1. It is appropriate to write ρ_0 and ρ_1 in spherical coordinates (figure 3.5) with respect to the centre of the ellipsoid $\vec{c} = (0, 0, c)$

$$r_0 = \begin{cases} x_0 = -\sqrt{1-c}\sin\vartheta\cos\varphi \\ y_0 = -\sqrt{1-c}\sin\vartheta\sin\varphi \\ z_0 = -(1-c)\cos\vartheta + c \end{cases} \tag{A.1}$$

$$r_1 = \begin{cases} x_1 = \sqrt{1-c}\sin\vartheta\cos\varphi \\ y_1 = \sqrt{1-c}\sin\vartheta\sin\varphi \\ z_1 = (1-c)\cos\vartheta + c \end{cases}, \tag{A.2}$$

where $0 \leq \vartheta \leq \pi$ and $0 \leq \varphi \leq 2\pi$. Note the third semiaxis is not flipped because of the necessity of positive lengths.

1. Alice's qubit state can be written as

$$\rho^A = \frac{1}{2}(\mathbb{I} + c\sigma_z) = p\rho_0^A + (1-p)\rho_1^A, \tag{A.3}$$

where $p_0 = p$ and $p_1 = 1 - p$ because of the binary measurement case. Through substituting A.1 and A.2 it results

$$\begin{aligned}
\frac{1}{2}(\mathbb{I} + c\sigma_z) &= p\{\frac{1}{2}(\mathbb{I} - \sqrt{1-c}\sin\vartheta\cos\varphi\sigma_x \\
&\quad - \sqrt{1-c}\sin\vartheta\sin\varphi\sigma_y - [(1-c)\cos\vartheta + c]\sigma_z\} \\
&\quad + (1-p)\{\frac{1}{2}(\mathbb{I} + \sqrt{1-c}\sin\vartheta\cos\varphi\sigma_x \\
&\quad + \sqrt{1-c}\sin\vartheta\sin\varphi\sigma_y + [(1-c)\cos\vartheta + c]\sigma_z\} \\
&= \frac{1}{2}\{\mathbb{I} + \sqrt{1-c}\sin\vartheta\cos\varphi\sigma_x \\
&\quad + \sqrt{1-c}\sin\vartheta\sin\varphi\sigma_y + [(1-c)\cos\vartheta + c]\sigma_z\} \\
&\quad + p[-\sqrt{1-c}\sin\vartheta\cos\varphi\sigma_x \\
&\quad - \sqrt{1-c}\sin\vartheta\sin\varphi\sigma_y - (1-c)\cos\vartheta\sigma_z] \\
&= \frac{1}{2}(\mathbb{I} + c\sigma_z) \\
&\quad + (\frac{1}{2} - p)[\sqrt{1-c}\sin\vartheta\sin\varphi\sigma_x \\
&\quad + \sqrt{1-c}\sin\vartheta\sin\varphi\sigma_y + (1-c)\cos\vartheta\sigma_z]
\end{aligned}$$

Hence it is obvious p must be $\frac{1}{2}$.

2. Alice's qubit state can be written as

$$\rho_b^A = \frac{1}{p} tr_B[\rho^{AB}(\mathbb{I} \otimes M_b)], \tag{A.4}$$

where $b = 0, 1$. M_b indicates Bob's measurement element. We denote $M_0 = \Pi$ and $M_1 = \mathbb{I} - \Pi$. A generic measurement element can be written as $\Pi = \frac{1}{2}(X_0\mathbb{I} + \vec{X}\cdot\vec{\sigma})$. It represents a PVM if and only if $X_0 = 1$ and $||\vec{X}|| = 1$ (see 2.1.1). A generic two-qubit canonical aligned state can be written as $\rho^{AB} = \frac{1}{4}(\mathbb{I}\otimes\mathbb{I} + \vec{c}\cdot\vec{\sigma} + \sum_{i=1}^{3} t_i\sigma_i\otimes\sigma_i)$, where $\vec{t} = (\sqrt{1-c}, \sqrt{1-c}, c-1)$.

Therefore we evaluate A.4 for $a = 0$ and we equal it to ρ_0^A (A.1), thus checking

Π satisfies $X_0 = 1$ and $||\vec{X}|| = 1$.

$$\rho_0^A = \frac{1}{p} tr_B[\rho^{AB}(\mathbb{I} \otimes \Pi)] = 2 \cdot \frac{1}{4} tr_B(\mathbb{I} \otimes \Pi + \vec{c} \cdot \vec{\sigma} \otimes \Pi + \sum_{i=1}^{3} t_i \sigma_i \otimes \sigma_i \Pi)$$
$$= \frac{1}{4} tr_B[X_0 \mathbb{I} \otimes \mathbb{I} + \mathbb{I} \otimes \vec{X} \cdot \vec{\sigma} + X_0 \vec{c} \cdot \vec{\sigma} \otimes \mathbb{I} + \vec{c} \cdot \vec{\sigma} \otimes \vec{X} \cdot \vec{\sigma}$$
$$+ \sum_{i=1}^{3} t_i (X_0 \sigma_i \otimes \sigma_i \cdot \mathbb{I} + \sigma_i \otimes \sigma_i \cdot \vec{X} \cdot \vec{\sigma})]$$
$$= \frac{1}{4}(2X_0 \mathbb{I} + 2X_0 \vec{c} \cdot \vec{\sigma} + 2 \sum_{i=1}^{3} t_i \sigma_i X_i) =$$
$$= \frac{1}{2}[X_0 \mathbb{I} + X_0 c \sigma_z + \sqrt{1-c} \sigma_x X_1 + \sqrt{1-c} \sigma_y X_2 + (c-1)\sigma_z X_3]$$
$$\equiv \frac{1}{2}\{\mathbb{I} - \sqrt{1-c} \sin\vartheta \cos\varphi \sigma_x - \sqrt{1-c} \sin\vartheta \sin\varphi \sigma_y + [c - (1-c)\cos\vartheta]\sigma_z\}$$

It results:

$$\begin{cases} X_0 = 1 \\ \sqrt{1-c} X_1 = -\sqrt{1-c} \sin\vartheta \cos\varphi \\ \sqrt{1-c} X_2 = -\sqrt{1-c} \sin\vartheta \sin\varphi \\ (c-1)X_3 + c = -(1-c)\cos\vartheta + c \end{cases}$$

Hence $X_0 = 1$ and $||\vec{X}|| = \sqrt{X_1^2 + X_2^2 + X_3^2} = \sqrt{\sin\vartheta^2 \cos\varphi^2 + \sin\vartheta^2 \sin\varphi^2 + \cos\vartheta^2} = 1$. $\square$

It is also possible to reach this result through considering the 4-vectors $\tilde{r}_b$ and $\tilde{X}$ of the Pauli components of Alice's collapsed states and Bob's measurement elements.

Consider for example ρ_0 for the furthest points case $\rho_0 = \frac{1}{2}(\mathbb{I} - \sqrt{1-c}\sigma_x + c\sigma_z)$. It is represented by $\tilde{r}_0 = \begin{pmatrix} 1 \\ -\sqrt{1-c} \\ 0 \\ c \end{pmatrix}$. Bob's measurement element $\Pi = \frac{1}{2}(X_0 \mathbb{I} + \vec{X} \cdot \vec{\sigma})$ is represented by $\tilde{X} = \begin{pmatrix} X_0 \\ \vec{X} \end{pmatrix}$.The relation (2.8) $p\tilde{r}_0 = \frac{1}{2}\Theta\tilde{X}$ can be inverted (the matrix Θ which represents the state ρ^{AB} here is $\Theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-c} & 0 & 0 \\ 0 & 0 & \sqrt{1-c} & 0 \\ c & 0 & 0 & c-1 \end{pmatrix}$) and it gives

$$\tilde{X} = \theta^{-1}\tilde{r_0} = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}. \tag{A.5}$$

Therefore $\Pi = \frac{1}{2}(\mathbb{I} - \sigma_x.)$ Bob has measured on σ_x as intuitively expected.

Note that knowing Bob's measurement elements is not useful for calculating the mutual information, however it is a a good way of understanding what happens in the whole process.

Proof 2. Consider that Bob's measurement Π can be written as $\frac{1}{2}(\mathbb{I} + \vec{X}\vec{\sigma})$, where $\vec{X} = (X_1, X_2, X_3)$ is such that $||\vec{X}|| = \sqrt{X_1^2 + X_2^2 + X_3^2} = 1$.

1. It is possible to write $p_0 = p$ as the probability that Bob performs Π, so

$$p = p(\Pi) = tr(\rho_B \Pi) = tr[\frac{\mathbb{I}}{2}\frac{1}{2}(\mathbb{I} + \vec{X}\vec{\sigma})] = \frac{1}{2}.$$

   Note that, according to the canonical state case, $\rho_B = \frac{\mathbb{I}}{2}$ and, since Bob has performed a PVM, then $X_0 = 1$.

2. Through using the relation 2.8, $\tilde{r_0}$ is

$$\tilde{r_0} = \Theta\tilde{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-c} & 0 & 0 \\ 0 & 0 & \sqrt{1-c} & 0 \\ c & 0 & 0 & c-1 \end{pmatrix} \begin{pmatrix} 1 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} 1 \\ \sqrt{1-c}X_1 \\ \sqrt{1-c}X_2 \\ c + (c-1)X_3 \end{pmatrix}.$$

   Hence $\vec{r_0} = \begin{pmatrix} \sqrt{1-c}X_1 \\ \sqrt{1-c}X_2 \\ c + (c-1)X_3 \end{pmatrix}$.

   Considering that $M_1 = \mathbb{I} - \Pi = \frac{1}{2}(\mathbb{I} - \vec{X}\vec{\sigma})$, $\tilde{r_1}$ is given by:

$$\tilde{r_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-c} & 0 & 0 \\ 0 & 0 & \sqrt{1-c} & 0 \\ c & 0 & 0 & c-1 \end{pmatrix} \begin{pmatrix} 1 \\ -X_1 \\ -X_2 \\ -X_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -\sqrt{1-c}X_1 \\ -\sqrt{1-c}X_2 \\ c - (c-1)X_3 \end{pmatrix}.$$

   Hence $\vec{r_1} = \begin{pmatrix} -\sqrt{1-c}X_1 \\ -\sqrt{1-c}X_2 \\ c - (c-1)X_3 \end{pmatrix}$.

   It is necessary to prove that $\vec{r_0}$ and $\vec{r_1}$ are opposite vectors on the surface of the ellipsoid and that they belong to the surface of the ellipsoid, *i.e.* they satisfy the equation of an ellipsoid. It is immediate to see that

$$\frac{(1-c)X_1^2}{1-c} + \frac{(1-c)X_2^2}{1-c} + \frac{(1-c)^2X_3^2}{(1-c)^2} = X_1^2 + X_2^2 + X_3^2 = 1.$$

   Moreover, through comparing the vector components, it is obvious they are opposite vectors on the surface of the ellipsoid.

□

Note that if Bob performs a POVM, then, in general, it implies Alice's state vectors are not situated on the surface of the ellipsoid.

Appendix B

Maximum likelihood discrimination - Bob's POVM

Immagine Alice and Bob share two qubits. Bob performs a binary POVM on his qubit composed of two elements $\{\Pi^B, \mathbb{I} - \Pi^B\}$, where the operator Π^B is represented by the 4-vector $\begin{pmatrix} X_0 \\ \vec{X} \end{pmatrix}$. In this situation Alice's state ρ^A is steered to two collapsed states ρ_0^A and ρ_1^A. The probabilities associated with these two states are respectively given by [1] $p = p(\rho_0^A) = p(\Pi^B) = tr(\rho^B \Pi^B) = \frac{X_0}{2}$ and $P(\rho_1^A) = 1 - p = 1 - \frac{X_0}{2}$.

Alice's aim is to perform the best measurement in order to guess whether her state is either ρ_0^A or ρ_1^A. She wants to reach the aim with as high a likelihood of success as possible.

Imagine Alice performs a binary measurement composed of two elements: $\{\Pi^A, \mathbb{I} - \Pi^A\}$, where the operator Π^A is represented by the 4-vector $\begin{pmatrix} s_0 \\ \vec{s} \end{pmatrix}$. If she obtains 0 (the Π^A outcome) she guesses ρ_0^A.If she obtains 1 she guesses ρ_1^A. She wants to choose the best measurement elements in order to maximize the probability of success:

$$\begin{aligned} P(success) &= \frac{X_0}{2} Tr[\rho_0^A \Pi^A] + (1 - \frac{X_0}{2}) Tr[\rho_1^A (\mathbb{I} - \Pi^A)] \\ &= 1 - \frac{X_0}{2} - tr[(\frac{X_0}{2}\rho_0^A - (1 - \frac{X_0}{2})\rho_1^A)\Pi^A]. \end{aligned}$$

Considering that $1 - \frac{X_0}{2}$ is a fixed quantity, the obvious way to maximize $P(success)$ consists of choosing $\vec{s}$ parallel to $\frac{X_0}{2} r_0^A - (1 - \frac{X_0}{2}) r_1^A$, where r_0^A and r_1^A represent Alice's collapsed states . Hence the most natural and appropriate choice for Alice consists of performing a PVM: $s_0 = 1$ and $\hat{s} = \frac{\vec{s}}{|\vec{s}|}$, where $\vec{s} = \frac{X_0}{2} r_0^A - (1 - \frac{X_0}{2}) r_1^A$ must be normalized according to the fact that a PVM is represented by a unit vector. Note that this choice is in accordance with the definition of general measurements (1.2).

In conclusion Alice can always choose a PVM as her optimal measurement, even if Bob performs a POVM.

[1] We always assume the maximum volume state case.

Bibliography

[1] K. Bartkiewicz B. Horst and A. Miranowicz. In: *Phys. Rev. A* 87 (2013), p. 042108 (cit. on p. 28).

[2] Thomas Decker. "Symmetric measurements attaining the accessible information". In: (19 september 2005). DOI: arXiv:quant-ph/0509122v1 (cit. on pp. xi, 15).

[3] Christopher A. Fuchs. "Indistinguishability and Accessible information in Quantum Theory". In: (23 January 1996). DOI: arXiv:quant-ph/9601020v1 (cit. on pp. xi, 16).

[4] P. Hausladen and W. K. Wootters. In: *J. Mod. Opt.* 41 (1994), p. 2385 (cit. on pp. xii, 58).

[5] Osamu Hirota. "Accessible information and optimal strategies for real symmetrical quantum sources". In: (18 January 1999). DOI: arXiv:quant-ph/9812062v3 (cit. on p. 15).

[6] R. Horodecki and M. Horodecki. "Information-theoretic aspects of inseparability of mixed states". In: *Phys. Rev. A* 54 (1996), p. 031838 (cit. on p. 22).

[7] P. Horodecki M. Horodecki and R. Horodecki. "Separability of mixed states: necessary sufficient conditions". In: *Phys. Rev. A* 223 (1996), pp. 1–8 (cit. on p. 25).

[8] Francesco Buscemi Michele Dall'Arno and Masanao Ozawa. "Tight Bounds on Accessible Information and Informational Power". In: (21 May 2014). DOI: arXiv:1402.0602v2 (cit. on pp. xii, 58).

[9] Antony Milne. "Quantum steering ellipsoids: conditions for describing a two-qubit state". In: (20 September 2013) (cit. on pp. 24, 26).

[10] Arieh Ben Naim. *A Farewell To Entropy: Statistical Thermodynamics Based On Information*. Singapore: Scientific-World, 2008.

[11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2010 (cit. on pp. xi, xii, 57).

[12] Terry Rudolph. *Introduction to Quantum Information*. Imperial College London: Lectures, 2012 (cit. on p. 13).

[13] Terry Rudolph. "Quantum steering ellipsoids, extremal physical states and monogamy". In: (Mar. 2014). DOI: arXiv:1403.0418v1 (cit. on pp. 26–28).

[14] Terry Rudolph. "The Quantum Steering Ellipsoid". In: (20 March 2013). DOI: arXiv:1303.4724v1 (cit. on pp. 21, 22, 24, 29).

[15] H. Wiseman S. Jones and D. Pope. In: *Phys. Rev. A* 72 (2005), p. 022330 (cit. on p. 26).

[16] Peter W. Shor. "On the Number of Elements Needed in a POVM Attaining the Accessible Information". In: (19 september 2000). DOI: arXiv:quant-ph/0009077v1 (cit. on p. 15).

[17] G. Vidal W. Dur and J. Cirac. In: *Phys. Rev. A* 62 (2000), p. 062314 (cit. on p. 27).

[18] William K. Wootters. "Entanglement of formation and concurrence". In: *Quantum Information and Computation* 1 (1 2001), pp. 27–44 (cit. on p. 26).