UNAMBIGUOUS DISCRIMINATION OF TWO NONORTHOGONAL MULTIPARTITE STATES USING LOCAL MEASUREMENTS AND CLASSICAL COMMUNICATION

By

Jihane Mimih

A dissertation submitted to the Graduate Faculty in Physics in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

at

THE CITY UNIVERSITY OF NEW YORK

2006

This manuscript has been read and accepted for the Graduate Faculty in Physics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

Date	Professor Mark Hillery Chair of Examining Committee
Date	Professor Sultan Catto Executive Officer
Professor Janŏs Bergou	
Professor Christopher Gerry	
Professor Greg Foster	Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

UNAMBIGUOUS DISCRIMINATION OF TWO NONORTHOGONAL MULTIPARTITE STATES USING LOCAL MEASUREMENTS AND CLASSICAL COMMUNICATION

by

Jihane Mimih

Advisor: Mark Hillery

The problem of unambiguous state discrimination consists of determining to which member of a set of known quantum states the state of a particular quantum system corresponds. We are allowed to fail to determine the state of the quantum system, but if we succeed, we are not allowed to make an error. The optimal procedure is the one with the lowest failure probability. In this dissertation, we consider a quantum system of two nonorthogonal bipartite states, $|\Psi_0\rangle$ and$|\Psi_1\rangle$. We distribute the qubits between two parties, Alice and Bob. They each perform local measurements on their qubits and then, they compare their measurement outcomes to determine which of the two possible two-particle states they have been given. We first examine the effect of restricting the classical communication between the parties, either allowing none or with some communication eliminating the possibility that one party's measurement depends on the result of the other party's. We found that in some cases the restrictions cause an increase in the failure probability, but in other cases they do not. Applications of these procedures to secret sharing are discussed. In the second part of this dissertation, we consider the cases in which, should a failure occur, both parties receive a failure signal or only one does. In the latter case, if the two states share the same Schmidt basis, the states can be discriminated with the same failure probability as would be obtained if the qubits were measured together.

This scheme is sufficiently simple that it can be generalized to multipartite qubit and qudit states. Applications to quantum secret sharing are discussed. Furthermore, we will present a scheme that demonstrates how the protocol for the case of two qubits can be experimentally realized.

Acknowledgements

I would like to take this opportunity to extend my deepest gratitude to my advisor, Professor Mark Hillery whose analytical skills and constant guidance have been very instrumental in the success of this dissertation project. I am also grateful to him for teaching me the quantum mechanics courses and making me appreciate this subject so much that I decided to pursue my Ph.D research in quantum information. I would also like to thank him for all his understanding and patience while working with him.
I would like to thank Professor Janŏs Bergou for his invaluable comments and suggestions he shared with me while attending conferences and for teaching me quantum optics. I would like to thank Professor Christopher Gerry for teaching me quantum optics and for his encouragements. I would also like to thank Professor Greg Foster for being a member of my thesis committee.
Special acknowledgment is given to AGEP and to the MAGNET Dissertation Fellowship for funding this dissertation project.
My gratitude goes to my grandmother for taking care of me and encouraging me throughout my life and to my dad for his concern about my progress and well being. I also want to thank my husband for all his support and help. Last but not least, I am greatly indebted to my mother who brought me to the United States and supported me in every step of my undergraduate and graduate studies with a lot of enthusiasm and patience.

Table of Contents

List of Figures

Chapter 1

Introduction

The earth and everything on it is in motion. Newton, in his Principia, explained the motion of objects by deriving the mathematical equations of motion, which depend on the forces acting on the object as well as the mass of the object. In these derivations, Newton has treated objects as large and tangible. However, if we look at nature on its finest scale, those large objects are not continuous, but instead they are made up of atoms, where each atom is in turn, made up of other particles. Similarly, Maxwell treated light as a wave made of a combination of oscillating electric and magnetic fields. In 1899, Max Planck when trying to solve the problem of black body radiation, gave the first indication that light is quantized when he assumed that the exchange of energy between light and matter happens in discrete amounts. Max Planck at that time was not sure whether the quantization should be attributed to light or matter. Later on, Albert Einstein confirmed the quantization of light through his interpretation the photoelectric effect in 1905. In this experiment, Einstein found

that when an atom absorbs or emits light, energy is transferred in discrete amounts. These particles of light are called photons. So understanding the interaction of light and matter was the start for the development of the quantum theory.

Quantum mechanics is a mathematical model of the physical world which embraces all areas of physics. In fact, there is no discontinuity between quantum and classical physics. Classical physics is a special case of quantum mechanics. In fact, the discreteness of matter becomes less noticeable as we move from the physical description of small objects such as atoms to large objects such as trucks and planets. A physical system in quantum mechanics is described by a quantum state, which is a vector in a Hilbert space. During the mid 1920's, Heisenberg, Dirac and Schrodinger gave the mathematical formulation of quantum mechanics [1]. In 1925, Schrodinger gave a mathematical description of the time evolution of a quantum state. This evolution is unitary and is generated by the Hamiltonian of the system. In 1927, Heisenberg and Bohr formulated their famous Copenhagen interpretation which provides explanations to questions related to the wave-particle duality. In 1928, Dirac formulated a relativistic quantum mechanical equation which describes elementary spin-$\frac{1}{2}$ particles. Unlike Schrodinger's equation, Dirac's equation is based on relativistic quantum mechanics which describes particles moving at relativistic velocities and accounts for phenomena such as the beta decay [2].

In 1935, Schrodinger introduced the concept of entanglement, which he referred

to as "an essential mystery of quantum mechanics, to describe composite systems" [3]. In fact, Einstein along with Boris Podolsky and Nathan Rosen published a famous paper in 1935, called the "EPR paper". The purpose of this paper was to show that quantum theory is not a complete physical theory, because it lacked some essential "elements of reality" [4]. Twenty nine years later, John Bell derived inequalities demonstrating that quantum particles show stronger correlations than we would expect from the laws of physics which describe particles in terms of classical variables instead of quantum states.

Recently, the unusual features of quantum mechanics have come to be viewed as resources rather than as curiosities. This change was brought about at the beginning of the nineties, by the advent of the field of quantum information, which considers entanglement, not just a mystery, but rather as an essential resource for communication and computation. Scientists have realized that entangled quantum states provide a powerful means of computation, a secure mean of communication and can also be used to reduce the communication complexity beyond the limits allowed by classical physics [5]. In order to see how this has been achieved, we need to look at the fundamental particles of both classical and quantum information.

The smallest entity in classical information is the bit. The classical bit is generally prepared in two distinguishable states that correspond to two distinct values, "0" and "1", "True" and "False" or, "yes" and "No". The classical bit is physically realized

through a macroscopic physical system. Examples include the charge on a capacitor or an electrical switch.

On the other hand, the quantum bit, known as the "qubit", is the fundamental particle in quantum information. Similar to the classical bit, the qubit exists in two states $|0\rangle$ and $|1\rangle$ corresponding to the "0" and "1" states of the classical bit. However, an important difference between the classical and the quantum bit is that the latter can exist in a coherent superposition of those two states. This means that there is always a basis in which the qubit is well defined [6]. For example, if we consider the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, there is a 50 percent chance that the qubit is either in the state "0" or in the state "1" given that our measurement basis is $\{|0\rangle, |1\rangle\}$. However, if we consider the rotated basis $\{(|+x\rangle, |-x\rangle\}$ where $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, we find that the qubit is well defined. This superposition property is purely quantum mechanical and has no classical analogue. It just means that the qubit represents both states, "0" and "1" at the same time. From a mathematical point of view, if our quantum system is represented by two states $|a\rangle$ and $|b\rangle$, then the state $|\Psi\rangle = \alpha|a\rangle + \beta|b\rangle$ is also an allowed state for our quantum system, given that $|\alpha|^2 + |\beta|^2 = 1$. Physically, a qubit can be represented by the state of an atom. An electron for example in the ground state can jump to its first excited state if we shine light with enough energy and for the appropriate time for the transition to happen. However, if we reduce the time we shine the light, the electron can exist in the $|+x\rangle$ state which is a superposition of

the ground state and the first excited state [7].

When I first started studying quantum mechanics, I found it hard to digest the fact that a qubit can exist in two different states at the same time. However, I always find that the double slit experiment is a marvellous demonstration of this superposition phenomena. Feynman said that the double slit experiment "has in it the heart of quantum mechanics" [8]. In this experiment, we consider a weak light source emitting photons one by one passing through a screen which contains two slits S_1 and S_2. On a second screen, we observe the interference fringes. The existence of these fringes implies that what happens is that each photon interferes with itself since only one photon is emitted at a time. One might wonder about which slit the photon really goes through. Unfortunately, there is no way of finding out the path the photon takes. If we were to perform an experiment to find out which slit the photon goes through, we would interact with the particle and consequently loose the interference pattern. In fact the principle of superposition means that it is impossible to determine which of the situations forming the superposition of the quantum system physically happens. The experimental set up for this experiment is shown in figure 1.1.

The Young double slit experiment was originally done using photons, but other particles such electrons and neutrons have been used as well. The interference pattern obtained in this experiment is a manifestation of the fact that each photon interacts

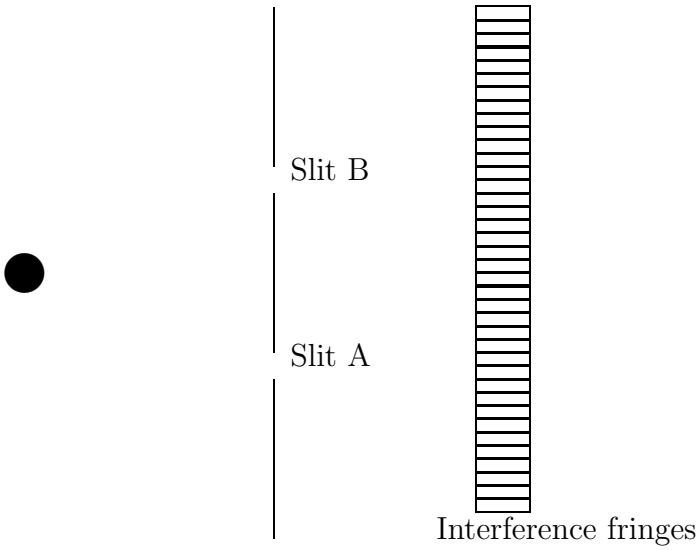

Figure 1.1: Youngs'double slit experiment

with itself, and the total state of the quantum system is a superposition of the quantum states of the system corresponding to only slit A being open and to only slit B being open.

In general, the state of a qubit can be represented by

$$|\Psi\rangle = a|0\rangle + b|1\rangle \tag{1.0.1}$$

where a and b are two complex numbers. The probability of finding the qubit in state $|0\rangle$ upon measurement is $p(0) = |a|^2$, and the probability of finding the qubit in state $|1\rangle$ is $p(1) = |b|^2$ where $|a|^2 + |b|^2 = 1$ since the probabilities have to add up to one. Geometrically, it is useful to visualize the qubit as a point on a three-dimensional sphere, called the Bloch sphere as shown in figure 1.2. The state of the qubit can

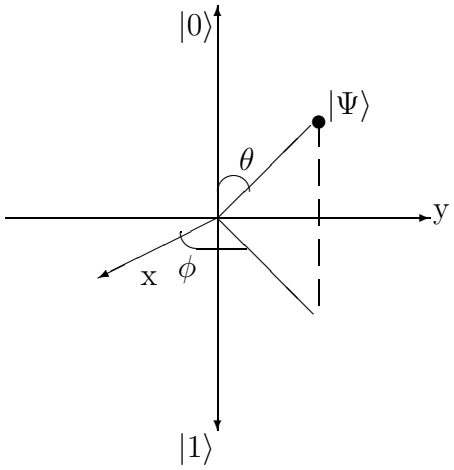

Figure 1.2: Geometrical representation of the qubit on the Bloch sphere

now be expressed as

$$|\Psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle \tag{1.0.2}$$

Hence, the complex numbers a and b describe now the orientation of the qubit in a three dimensional space by determining the polar angle θ and the azimuthal angle ϕ. A natural question that arises, is how much information a qubit represents? Well, if we measure the qubit and find 0 for example with a probability $|a^2|$, then the post measurement state is $|0\rangle$. Therefore, the state of the qubit collapses to a state which corresponds to the measurement outcome upon a measurement. Hence, from a single measurement, we learn one bit of information about the qubit at hand at the expense of changing the state.

1.1 Entanglement

Entanglement is a purely quantum mechanical resource that has no analogue in the classical world. Entangled states are a very useful resource in building communication

schemes such as quantum cryptography and quantum teleportation. Entanglement is also responsible for the power of quantum computers that perform some calculations exponentially faster than classical computers. An example of a state of a two particle system that is entangled is given by,

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2 \tag{1.1.1}$$

If $|0\rangle$ represents a horizontally polarized photon and $|1\rangle$ represents a vertically polarized photon, then the entanglement between the two photon states tells us that if the first particle is found to be horizontally polarized, then the second particle is always vertically polarized. The interesting feature here is that none of the qubits has a well defined polarization. However, as soon as one of the two qubits is measured, given that the result is completely random, the other qubit will be found to carry the opposite value. This property is independent of the distance between the qubits. In other words, the two particles can be located very far from each other, but yet, the correlations will still be observed when we perform our measurements.

The two particles in this state do not possess physical properties independent of observation. Only after we perform a measurement on the system can we say what the value of a physical property is. The rules of quantum mechanics enable us to determine the probabilities for the measurement outcomes. This of course violates the classical view that states that physical properties have well defined values independent of measurement. This discussion leads us to the conclusion that entangled states are

states that violate Bell inequalities, as the quantum world is not locally realistic. We shall see that entanglement is a valuable resource , similar in importance to energy, information and entropy, whose manipulation enables us to do major tasks of quantum information and quantum computation. In the following sections, I will discuss some useful applications of entanglement.

1.1.1 Superdense coding

Among the applications of entanglement is quantum dense coding, which was first been proposed by Bennett and Wiesner [9]. In this scheme, we consider two parties, Alice and Bob, who share two qubits in an entangled EPR state. Each qubit exists in the state $|0\rangle$ or in the state $|1\rangle$. Therefore, classical mechanics tells us that there are four possible combinations of these particles: $\{0,0\}$, $\{1,1\}$, $\{0,1\}$ or $\{1,0\}$, assuming that the first entry belongs to Alice and the second one to Bob. In this case, two bits of information can be encoded by manipulating both particles, but each particle carries only one bit. Let us see what happens if we want to use quantum mechanics to encode the two information bits. Well, quantum mechanics allows us to use the superposition of classical information. The Bell states are entangled orthogonal states which are useful to represent the two particle states.

$$|\Phi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$
$$|\Phi_-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$

$$|\Psi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$
$$|\Psi_-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$

It can be seen that we can assign each state of the four Bell states with different information. What is more interesting is, as shown on figure 1.3, two bits of classical information can be transferred from Alice to Bob by manipulating only one qubit. To see how this is achieved, we assume that Alice and Bob initially share two qubits in the entangled state $|\Phi_+\rangle_{AB}$. Alice performs one of the four following unitary transformations on her particle before she sends it to Bob:

1. Apply identity operator; this keeps the state $|\Phi_+\rangle_{AB}$ unchanged

2. Apply σ_x; which rotates the initial state around the x-axis. This changes the state to $|\Psi_+\rangle_{AB}$

3. Apply σ_y; which rotates the initial state around the y-axis. This changes the state to $|\Phi_-\rangle_{AB}$

4. Apply σ_z; which rotates the initial state around the z-axis. This changes the state to $|\Psi_-\rangle_{AB}$

1.1.2 Quantum teleportation

When Bob has both qubits in hand, he can determine which of the four Bell states his particles belong to, and hence determine which operation Alice performed. In sum,

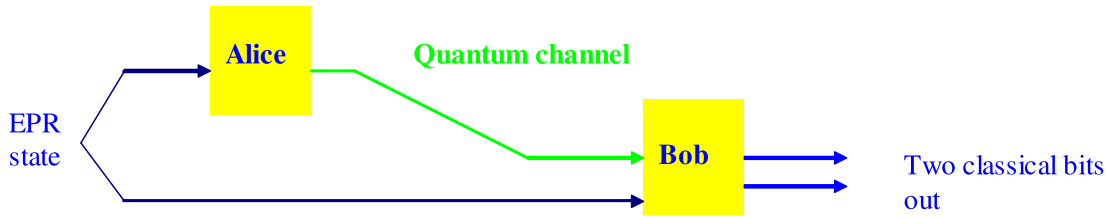

Figure 1.3: Quantum dense coding: Two classical bits are communicated through manipulation of one qubit

Alice communicates to Bob two bits of classical information by interacting only with the qubit in her possession. No interaction with Bob's qubit was needed. This task would have been impossible if Alice had transmitted only a classical bit.

In addition, it is worth mentioning that an eavesdropper who tries to capture Alice's particle, cannot learn the classical bit that Alice wants to communicate to Bob. This is due to the fact that information exists in the correlation between Alice and Bob's particles.

Quantum teleportation is a simple example that shows how useful entanglement is in communication schemes. Let us see how this protocol works. We assume that Alice has a qubit in the state $|\Psi\rangle_{A1} = a|0\rangle_{A1} + b|1\rangle_{A1}$, where a and b are two complex numbers with $|a|^2 + |b|^2 = 1$. Alice does not know the state of her qubit but she wants to send her qubit to Bob. The problem Alice has is that she cannot perform a measurement of her qubit because this will destroy the state without acquiring enough information for Bob to reconstruct the state. In addition, we assume that

Alice cannot hand her qubit directly to Bob.

This problem is solved if Alice and Bob share an entangled state, a Bell state in particular. For example, if the Bell state Alice and Bob share is $|\Psi_-\rangle_{A2,B} = \frac{1}{\sqrt{2}}(|0\rangle_{A2}|1\rangle_B - |1\rangle_{A2}|0\rangle_B)$, the total state of the system consists then of two particles in Alice's hand and one particle in Bob's possession.

$$\begin{aligned} |\Psi\rangle_{A1,A2,B} = |\Psi\rangle_{A1} \otimes |\Psi_-\rangle_{A2,B} &= \frac{1}{2}[|\Phi_+\rangle_{A_2,A_1}(a|1\rangle_B - b|0\rangle_B) \\ &+ |\Phi_-\rangle_{A_2,A_1}(a|1\rangle_B + b|0\rangle_B) \\ &+ |\Psi_+\rangle_{A_2,A_1}(-a|0\rangle_B + b|1\rangle_B) \\ &+ |\Psi_-\rangle_{A_2,A_1}(-a|0\rangle_B - b|1\rangle_B) \end{aligned}$$

As soon as Alice measures her particles by projecting them onto the four possible Bell states, Bob's particle will be found in one of the following states

$$\begin{aligned} |\Phi_+\rangle_{A1,A2} &\rightarrow a|1\rangle_B - b|0\rangle_B \\ |\Phi_-\rangle_{A1,A2} &\rightarrow a|1\rangle_B + b|0\rangle_B \\ |\Psi_+\rangle_{A1,A2} &\rightarrow -a|0\rangle_B + b|1\rangle_B \\ |\Psi_-\rangle_{A1,A2} &\rightarrow -a|0\rangle_B - b|1\rangle_B \end{aligned}$$

Once Alice tells Bob the outcome of her measurement, Bob can reconstruct his state by applying the appropriate unitary transformation. For example, if Alice's qubits exist in the state $|\Psi_+\rangle_{A1,A2}$, Bob will have to apply σ_z to recover the original state which is $a|0\rangle_B + b|1\rangle_B$.

Chapter 2

Measurements in quantum mechanics

2.1 Von Neumann measurements

Von Neumann measurements, also known as projective measurements, are described by hermitian operators acting on the state space of the quantum system. A Hermitian operator M can be expressed in its spectral decomposition as follows $M = \sum_m \lambda_m P_m$, where P_m are projectors onto the eigenspace of M . These projectors satisfy the completeness relation $\sum_m P_m = I$ as well as the orthogonality and repeatability condition $P_m P_{m'} = \delta_{m,m'} P_m$. λ_m are the eigenvalues of the operator M. If our quantum system is in a pure state $|\Psi\rangle$, then the probability of getting an outcome m is given by $p_m = \langle\Psi|P_m|\Psi\rangle$ and the post measurement state is

$$\frac{P_m|\Psi\rangle}{\sqrt{\langle\Psi|P_m|\Psi\rangle}} \tag{2.1.1}$$

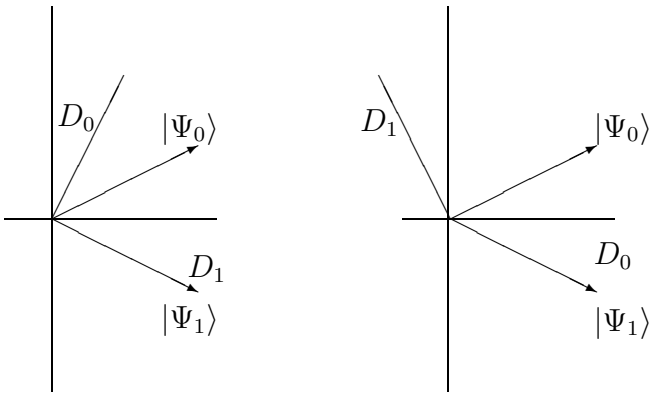

Figure 2.1: Von Neumann measurements to discriminate between two nonorthogonal states $|\Psi_0\rangle$ and $|\Psi_1\rangle$

A limitation of this type of measurements is that the measurement outcomes cannot exceed the dimensionality of the system's Hilbert space, so there is very little flexibility in the measurement. For example, suppose $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are two nonorthogonal quantum states, and we wish to discriminate between these two states using projective measurements. The best we can do, given that only projective measurements are allowed, is to choose two detectors, D_0 and D_1 respectively corresponding to the state $|\Psi_0\rangle$ and the state $|\Psi_1\rangle$. Here is the schematic illustration of such measurements[10];

As can be seen from figure 2.1, when we choose D_1 along $|\Psi_1\rangle$ and we choose D_0 along the orthogonal direction to D_1, then a click in detector D_0 means that $|\Psi_0\rangle$ is sent. However a click in D_1 is inconclusive since $|\Psi_0\rangle$ has a component along $|\Psi_1\rangle$ as well. Similarly, if we choose D_0 along $|\Psi_0\rangle$ and we choose D_1 along the orthogonal direction to D_0, then a click in detector D_1 means that $|\Psi_1\rangle$ is sent. However a click in D_0 is inconclusive since $|\Psi_1\rangle$ has a component along $|\Psi_0\rangle$ as well. Therefore, most of

the time, we detect one state at the expense of missing the other state. For this reason, we need some measurements that are more general than projective measurements.

2.2 Generalized measurements

There is an increased need when doing computations and experiments to some more flexible measurements than Von Neumann measurements due to their limitations. In fact, generalized measurements allow the number of measurement outcomes to exceed the dimensionality of the Hilbert space. This is possible because if we wish to do Generalized measurement on a system A, we choose a larger system that includes system A, we let both systems evolve through a unitary operator, then we perform orthogonal measurements on the larger system which will transform the state of the quantum system to the original Hilbert space. Let us see how this works. We assume we have our system A whose Hilbert space is $\mathcal{H}_A$ coupled to an ancillary system B, with Hilbert space $\mathcal{H}_B$. Therefore, our Hilbert space is part of a larger Hilbert space defined by the tensor product $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. We consider $\{|m_A\rangle\}$ an orthogonal basis for system A, which is initially in the state $|\Psi_A\rangle$ and $\{|m_B\rangle\}$ an orthogonal basis for system B, which is initially in the state $|\Psi_B\rangle$. If we let both systems evolve through a unitary operator U_{AB} defined as follows $U_{AB}|\Psi_A\rangle|\Psi_B\rangle \equiv \sum_m M_m|\Psi_A\rangle|m_B\rangle$, where M_m are measurement operators on quantum system A. When we perform a projective measurement P on the whole system where $P \equiv I_A \otimes |m_B\rangle\langle m_B|$. We find that the

probability that outcome m occurs is given by

$$\begin{aligned} p(m) &= \langle\Psi_A|\langle|\Psi_B U^\dagger P U|\Psi_A\rangle|\Psi_B\rangle \\ &= \langle\Psi_A|M_m^\dagger M_m|\Psi_A\rangle \end{aligned}$$

If we define $M_m^\dagger M_m = E_m$, we find that $\sum_m E_m = I$ and $E_m \geq 0$. The set E_m defines what is known as Positive Operator-Valued Measure or POVM. In this context, the probability of obtaining a measurement outcome m is given by $p(m) = \langle\Psi|E_m|\Psi\rangle$. The procedure discussed in this section is an instance of the well known Neumark theorem.

Chapter 3

State Discrimination

The problem of distinguishing between quantum states consists of determining which of a set of known quantum states the system belongs to. We assume we have two quantum states $|\Psi_0\rangle$ and $|\Psi_1\rangle$. If $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are orthogonal, then we can perfectly distinguish between the states using global measurements [11]. There exists some states, even though orthogonal, cannot be distinguished by means of local measurements. For example, let us consider the maximally entangled EPR states;

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$
$$|\Phi_-\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB})$$

When we consider the state $|\Phi_+\rangle$, the reduced density matrix of subsystem A is given by;

$$\begin{aligned}\rho_A^+ &= Tr_B(|\Phi_+\rangle|\langle\Phi_+|) = \sum_{m_B=0}^{1} \langle m_B|\frac{1}{2}(|00\rangle_{AB} + |11\rangle_{AB})(\langle 00|_{AB} + \langle 11|_{AB})|m_B\rangle \\ &= \frac{1}{2}I_A\end{aligned}$$

Similarly, the reduced density matrix for subsystem B is given by;

$$\begin{aligned}\rho_B^+ &= Tr_A(|\Phi_+\rangle|\langle\Phi_+|) = \sum_{m_A=0}^{1}\langle m_A|\frac{1}{2}(|00\rangle_{AB}+|11\rangle_{AB})(\langle 00|_{AB}+\langle 11|_{AB})|m_A\rangle \\ &= \frac{1}{2}I_B\end{aligned}$$

Similarly, for the state $|\Phi_-\rangle$, we find that the reduced density matrices for subsystems A and B respectively are;

$$\begin{aligned}\rho_A^- &= Tr_B(|\Phi_-\rangle|\langle\Phi_-|) \\ &= \frac{1}{2}I_A\end{aligned}$$

$$\begin{aligned}\rho_B^- &= Tr_A(|\Phi_-\rangle|\langle\Phi_-|) \\ &= \frac{1}{2}I_B\end{aligned}$$

Note that $\rho_A^+ = \rho_A^-$ and $\rho_B^+ = \rho_B^-$. Since the reduced density matrices are identical, the states are locally indistinguishable.

On the other hand, nonorthogonal states can never be perfectly distinguished if only one copy is provided [11]. The basic idea behind this is that each state has a component along the direction of the other state.

Since it is not possible to invent a device which can perform a measurement that will perfectly distinguish between nonorthogonal states, tremendous efforts were done to find strategies that will achieve optimal state discrimination. Minimum error state discrimination is one of the strategies used to distinguish between nonorthogonal

states and relies on minimizing the probability of errors. The second strategy is unambiguous state discrimination which gives error free measurement outcomes at the expense of obtaining some inconclusive results. Determining which method to follow depends on the problem at hand. Minimum-error discrimination always gives an answer, but can be wrong. Unambiguous state discrimination is never wrong but can fail to give an answer.

3.1 Minimum error state discrimination

There might be situations when we need to get a conclusive answer as to what the state of the quantum system is. We assume that we know that the state belongs to either $|\Psi_0\rangle$ or $|\Psi_1\rangle$, which are not orthogonal. after we perform our measurement, we obtain a conclusive answer as to what the state of the system is, but it might be wrong. Minimum error state discrimination consists in minimizing the probability of making errors. We consider two detection operators, E_0 for detecting the state $|\Psi_0\rangle$, and E_1 for detecting the state $|\Psi_1\rangle$. The probability to detect $|\Psi_0\rangle$ is given by $p_0 = \langle\Psi_0|E_0|\Psi_0\rangle$ and the probability to detect $|\Psi_1\rangle$ is given by $p_1 = \langle\Psi_1|E_1|\Psi_1\rangle$. Since the probabilities p_0 and p_1 are positive and real numbers, the detection operators must be Hermitian and positive as well. In addition, the measurement operators must satisfy $E_0+E_1 = I$, where I is the identity operator in the Hilbert space of the system. The error probability is given by $P_E = 1-\eta_0 p_0-\eta_1 p_1$, where η_0 and η_1 are the a priori probabilities of $|\Psi_0\rangle$ and $|\Psi_1\rangle$ respectively. The problem here amounts in finding the

measurement operators that minimize the failure probability P_E. The minimum error probability to distinguish two states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ was derived by Helstrom [12] ;

$$P_{E_{min}} = \frac{1}{2}(1 - \sqrt{1 - 4\eta_0\eta_1|\langle\Psi_0|\Psi_1\rangle|}) \tag{3.1.1}$$

As can be seen from the formula, when the states are orthogonal, the error probability is 0, which means, just as expected, we can perfectly distinguish between such states.

3.2 Unambiguous state discrimination

Before we proceed to the discussion of unambiguous state discrimination of two qubit states, which is the subject of this dissertation, I briefly discuss unambiguous state discrimination for single qubit states. The problem is as follows; we have a qubit that has been prepared in two nonorthogonal states, $|\Psi_0\rangle$ or $|\Psi_1\rangle$. We need to determine the state that the qubit has been prepared in without making any errors. The only way this can be done, since we cannot perfectly discriminate between nonorthogonal states, is if we sometimes allow some measurement outcomes to be inconclusive. For this purpose, we use POVM measurements. Figure 3.1 shows how such measurements can achieve unambiguous state discrimination [13].

Since we have an extra degree of freedom by considering generalized measurements, we obtain three measurement outcomes at the end of our measurements. We suppose that a click in a detector along D_0 corresponds to detecting the state $|\Psi_0\rangle$,

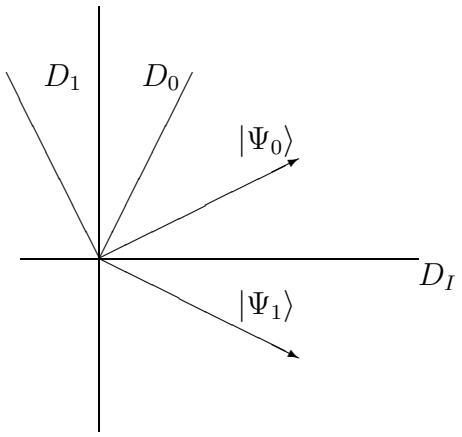

Figure 3.1: POVM measurements to discriminate with no error between two nonorthogonal states $|\Psi_0\rangle$ and $|\Psi_1\rangle$

a click in a detector along D_1 corresponds to detecting the state $|\Psi_1\rangle$ and a click in a detector along D_I simply indicates that we have failed to determine which state the quantum system belongs to. In fact, the direction of detector D_0 is chosen to be orthogonal to $|\Psi_1\rangle$, so that a click in this detector tells us that the state of the system is for sure $|\Psi_0\rangle$. Furthermore, because the direction of detector D_1 is orthogonal to $|\Psi_0\rangle$, a click in D_1 tells us that the state of the system is for sure $|\Psi_1\rangle$. However, a click in detector D_I tells us nothing about the state the system was prepared in because both states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ have components along this direction. These generalized measurements can be described by three detection operators; $A_0^\dagger A_0$ corresponds to detecting $|\Psi_0\rangle$, $A_1^\dagger A_1$ corresponds to detecting $|\Psi_1\rangle$, and $A_f^\dagger A_f$ corresponds to failing to detect either $|\Psi_0\rangle$ nor $|\Psi_1\rangle$. These detection operators satisfy the completeness relation;

$$A_0^\dagger A_0 + A_1^\dagger A_1 + A_I^\dagger A_I = I$$

The probabilities to correctly identify $|\Psi_0\rangle$ and $|\Psi_1\rangle$ respectively are given by

$$p_0 = \langle\Psi_0|A_0^\dagger A_0|\Psi_0\rangle$$

$$p_1 = \langle\Psi_1|A_1^\dagger A_1|\Psi_1\rangle$$

The probability that we want to minimize is the failure probability $q = \eta_0 q_0 + \eta_1 q_1$ where $q_0 = 1 - p_0$, $q_1 = 1 - p_1$ and η_0 and η_1 are the a priori probabilities of $|\Psi_0\rangle$ and $|\Psi_1\rangle$ respectively. When the states have equal a priori probabilities, it was found that the maximum probability to successfully distinguish between the states is given by,

$$P_{idp} = 1 - |\langle\Psi_0|\Psi_1\rangle| \tag{3.2.1}$$

This equation is the well known Ivanovic-Dieks-Peres limit, or the IDP limit[14, 15, 16]. The details of this derivation can be found in the appendix.

This procedure can be used as the basis for a quantum cryptography protocol[17]. In general, quantum cryptography is a method of generating a secure shared key between two or more parties. We assume we have two fictitious parties, Alice and Bob. Alice wants to send a message to Bob such that the message has to remain a secret. Alice uses a code to encrypt the message. The B92 protocol can be used to generate a secure key(see figure 3.2). Alice sends qubits to Bob prepared in one of

these two states

$$\begin{aligned} |\Psi_0\rangle &= |0\rangle \\ |\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \end{aligned}$$

If $|\Psi_0\rangle$ is sent, that key bit is recorded as "0" and if $|\Psi_1\rangle$ is sent, the corresponding bit is recorded as "1". Bob has to apply the unambiguous state discrimination procedure to the qubits he received from Alice. Bob will succeed with a probability $p_{idp} = 1 - |\langle\Psi_0|\Psi_1\rangle| = 1 - \frac{1}{\sqrt{2}}$. Bob then tells Alice over a public channel, over the phone for example, whether the procedure has succeeded or failed. Then, Alice and Bob keep the instances when the procedure has succeeded and they throw the instances when it has failed. In this manner, after repeating this procedure many times, Alice and Bob will be able to share a key, which in this case is a string of 0's and 1's. One might however wonder about the security of this key. We suppose an eavesdropper, Eve, has intercepted the particles. Her goal is to gain as much information as she can about the key bits. However, since both states are not orthogonal, there is no procedure that will allow Eve to determine with certainty whether the state sent is $|\Psi_0\rangle$ or $|\Psi_1\rangle$. The best Eve can do is to apply the optimal state discrimination procedure. Hence, she will fail with a probability of $|\langle\Psi_0|\Psi_1\rangle| = \frac{1}{\sqrt{2}}$. When Eve's measurement fails, she will not know what state the qubit belongs to and therefore, she will have to guess which state to send to Bob. As a result, Eve will send the wrong state to Bob with a probability $\frac{1}{2\sqrt{2}}$. This problem will be solved by having Alice and Bob compare some

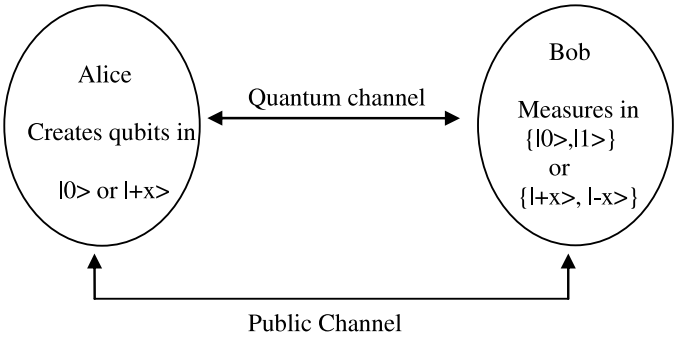

Figure 3.2: B92 protocol: Quantum key distribution using single qubits

of their key bits over a public channel. If they notice no discrepancies, they know that there is no eavesdropper and they keep the remaining key bits. However, if they find errors, they know that Eve is trying to learn the key and hence, they discard all the key bits and try the procedure again.

Another cryptography protocol that relies on the fact that nonorthogonal states cannot be perfectly discriminated is the BB84 protocol which is due to Bennett and Brassard. In this protocol, Alice sends random qubits to Bob. Each qubit can belong to one of the four following states;

$$|0\rangle \leftrightarrow 0$$

$$|1\rangle \leftrightarrow 1$$

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \leftrightarrow 0$$

$$|-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \leftrightarrow 1$$

Then, Bob measures randomly in one of the two bases; $\{|0\rangle, |1\rangle\}$ or $\{|+x\rangle, |-x\rangle\}$. After Bob is done with all his measurements, he communicates with Alice through a public channel. He tells Alice the basis in which he has performed each measurement. Therefore, if the measurement basis corresponds to the basis Alice sent the qubit in, they keep the key bit, otherwise, they discard the bit. At this point, Alice and Bob have already established a raw key where they have agreed on the preparation and on the measurement basis. However, there has been no communication regarding the state of the qubit yet. When Alice sends Bob the single qubits, an eavesdropper, Eve, can try to intercept some or all of the qubits in order to learn the key. When this happens, Eve does not know in which basis to do her measurements. Hence, if she chooses correctly her measurement basis, she will transmit the right state to Bob. However, if she chooses the incorrect basis, she will then send the wrong state to Bob. Eve will be detected when Alice and Bob publicly compare some of their bits. The presence of Eve will be revealed by the existence of errors.

Chapter 4

Effects of classical communication and of number of failure states on unambiguous state discrimination

We suppose we have a third party Charlie, who prepares a two-qubit state $|\Psi_0\rangle$ or $|\Psi_1\rangle$. Charlie sends one of the qubits to Alice and the other one to Bob. Charlie also tells Alice and Bob that the state he sends them is either $|\Psi_0\rangle$ or $|\Psi_1\rangle$ and provides them with the a priori probabilities for each state. By making local measurements and communicating through a classical channel, Alice and Bob want to determine which state they have. We are considering again here the case of unambiguous state discrimination, which means that the two parties, Alice and Bob, may fail to determine the state Charlie sends them, but if they succeed, they will not make an error. That is, they will never conclude that they have $|\Psi_0\rangle$ when they have been given $|\Psi_1\rangle$ or announce that they have $|\Psi_1\rangle$ while $|\Psi_0\rangle$ was actually sent. Our goal is to develop a procedure that Alice and Bob can use to discriminate between the states.

One aspect of this problem has already been solved. If each state is equally likely and both qubits can be measured together, then it is known that the states can be successfully unambiguously discriminated with a probability of $p_{idp} = 1 - |\langle\Psi_0|\Psi_1\rangle|$. It was recently shown that the states can be discriminated using only local operations and classical communication (LOCC) with the same success probability[18, 19]. Walgate, et al. proved that when the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are orthogonal , then they can be perfectly distinguished by means of LOCC [20] . However, the case when $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are not orthogonal was investigated numerically by Virmani, et al. [18], and they found that there is strong evidence that unambiguous state discrimination is possible for such states with a probability of p_{idp} using LOCC. In addition, they found a class of states for which they could prove that this was true. A proof that this is true for all bipartite states was provided by Chen and Yang [19].

One way to use LOCC to unambiguously discriminate between nonorthogonal quantum states is the following; Alice makes a projective measurement on her particle that gives her no information about whether the state is $|\Psi_0\rangle$ or $|\Psi_1\rangle$. Then, she communicates her measurement outcome to Bob who has not done anything to his particle at this point. Based on what Alice has told him, Bob chooses the appropriate measurement to make on his particle. In particular, he applies the procedure for the optimal unambiguous discrimination of single qubit states to his particle. The

drawback here is that this situation involves conditional measurement where a measurement made by Bob depend on Alice's measurement. This case is not of interest to us because while waiting for Alice's measurement outcome, Bob has to store his qubit and keep it safe from the effects of decoherence, which is a difficult thing to do. What we wish to examine here is the situation where Alice and Bob make their measurements independent of each other, then communicate to determine the state of their quantum system. This means that they each measure their qubit when they receive it and record the result of their measurement. In this case, only classical information needs to be stored, which is an easy task to do. More precisely, we would like to discuss in this section how restricting the classical communication between Alice and Bob can affect their abilities to discriminate between the quantum states. In a previous paper we discussed such a scheme [21]. In it, we first started by investigating the case where the classical communication between the parties is not allowed. Then, we looked at what happens when we relax the ban on the classical communication by allowing Alice and Bob to communicate their measurement results to each other.

4.1 No classical communication

In this case, each party has three possible measurement results, 0 corresponding to $|\Psi_0\rangle$, 1 corresponding to $|\Psi_1\rangle$, and f corresponding to failure to distinguish between either $|\Psi_0\rangle$ or $|\Psi_1\rangle$. Since Alice and Bob are not allowed to communicate, if $|\Psi_0\rangle$ is sent, then Alice and Bob both measure 0 or both measure f. In this manner,

both parties know, without communicating, that $|\Psi_0\rangle$ was sent or that the measurement failed. On the other hand, if $|\Psi_1\rangle$ is sent, then they both measure either 1 or f. Alice's measurements are characterized by the following POVM operators $\{A_0, A_1, A_f\}$. While Bob's measurements are characterized by the following POVM operators; $\{B_0, B_1, B_f\}$. These operators satisfy

$$I_A = \sum_{j=0,1,f} A_j^\dagger A_j \qquad I_B = \sum_{j=0,1,f} B_j^\dagger B_j, \tag{4.1.1}$$

where I_A is the identity on $\mathcal{H}_A$, the Hilbert space of Alice's qubit, and I_B is the identity on $\mathcal{H}_B$, the Hilbert space of Bob's qubit. Since we require that Alice and Bob only get the same measurement outcomes, we obtain the following conditions

$$A_j B_k |\Psi_n\rangle = 0, \tag{4.1.2}$$

where $j, k \in \{0, 1, f\}$ and $j \neq k$, and $n \in \{0, 1\}$. In addition, since we are considering unambiguous state discrimination, no errors are allowed in identifying the states which implies that

$$A_0 B_0 |\Psi_1\rangle \qquad A_1 B_1 |\Psi_0\rangle = 0. \tag{4.1.3}$$

When we act on the first equation with $B_0^\dagger$ and on the second equation with $B_1^\dagger$, then after adding, using the completeness relations for both Alice and Bob's Hilbert spaces, we find that

$$\begin{aligned} 0 &= A_0(I_B - B_f^\dagger B_f)|\Psi_1\rangle \\ &= A_0|\Psi_1\rangle, \end{aligned} \tag{4.1.4}$$

where, in going from the first to the second line, we noted that $A_0 B_f|\Psi_1\rangle = 0$. Similarly we find that

$$B_0|\Psi_1\rangle = 0 \quad A_1|\Psi_0\rangle = 0$$

$$B_1|\Psi_0\rangle = 0. \tag{4.1.5}$$

We now want to express $|\Psi_0\rangle$ and $|\Psi_1\rangle$ in their Schmidt bases‘

$$\begin{aligned} |\Psi_0\rangle &= \sum_{j=0}^{1} \sqrt{\lambda_{0j}}|u_{Aj}\rangle \otimes |u_{Bj}\rangle \\ |\Psi_1\rangle &= \sum_{j=0}^{1} \sqrt{\lambda_{1j}}|v_{Aj}\rangle \otimes |v_{Bj}\rangle. \end{aligned} \tag{4.1.6}$$

where $\{|u_{A0}\rangle, |u_{A1}\rangle\}$ and $\{|v_{A0}\rangle, |v_{A1}\rangle\}$ are orthonormal bases for Alice's space. Similarly $\{|u_{B0}\rangle, |u_{B1}\rangle\}$ and $\{|v_{B0}\rangle, |v_{B1}\rangle\}$ are orthonormal bases for Bob's space.

The two conditions on $|\Psi_1\rangle$ imply:

1. If $\lambda_{10} \neq 0$ and $\lambda_{11} \neq 0$, then $A_0|v_{Aj}\rangle = 0$, for $j = 0, 1$, and this implies that $A_0 = 0$. We also have that $B_0 = 0$.

2. If one of the λ_{1j}'s is zero, and we can assume, without loss of generality, that $\lambda_{11} = 0$, then we have that $A_0|v_{A0}\rangle = B_0|v_{B0}\rangle = 0$.

Similarly, the two conditions on $|\Psi_0\rangle$ imply:

3. If $\lambda_{00} \neq 0$ and $\lambda_{01} \neq 0$, then $A_1 = B_1 = 0$.

4. If $\lambda_{01} = 0$, then $A_1|u_{A0}\rangle = B_1|u_{B0}\rangle = 0$.

If conditions (1) and (3) are true, all the operators are zero except the failure operators. This implies that Alice and Bob always fail in determining the state of the quantum system. On the other hand, if conditions (2) and (4) are satisfied we have that the POVM operators A_j and B_j must be of the form

$$\begin{aligned} A_0 &= |\xi_A\rangle\langle v_{A1}| \quad B_0 = |\xi_B\rangle\langle v_{B1}| \\ A_1 &= |\eta_A\rangle\langle u_{A1}| \quad B_1 = |\eta_B\rangle\langle u_{B1}|, \end{aligned} \tag{4.1.7}$$

where the vectors $|\xi_A\rangle$, $|\xi_B\rangle$, $|\eta_A\rangle$, and $|\eta_B\rangle$ need to be determined.

We now examine the consequences of the conditions $A_0 B_f|\Psi_0\rangle = 0$ and $A_1 B_f|\Psi_1\rangle = 0$, or

$$\begin{aligned} A_0|u_{A0}\rangle \otimes B_f|u_{B0}\rangle &= 0 \\ A_1|v_{A0}\rangle \otimes B_f|v_{B0}\rangle &= 0. \end{aligned} \tag{4.1.8}$$

The first of these equations implies that either $\langle v_{A1}|u_{A0}\rangle = 0$, which further implies that $|v_{A0}\rangle$ is proportional to $|u_{A0}\rangle$, or that $B_f|u_{B0}\rangle = 0$. If the first alternative is true, then both A_0 and A_1 acting on either vector $|\Psi_j\rangle$ gives zero, and hence, the measurement always fails. In order to avoid this situation, we need to have $B_f|u_{B0}\rangle = 0$. However, the second equation tells us that, if the measurement does not always fail, that $B_f|v_{B0}\rangle = 0$. These conditions imply that (assuming that $|u_{B0}\rangle \neq |v_{B0}\rangle$; if this is not true the measurement always fails) $B_f = 0$. We then have that $I_B = B_0^\dagger B_0 + B_1^\dagger B_1$, which can only be true if $|v_{B1}\rangle = |u_{B0}\rangle$ or $|v_{B0}\rangle = |u_{B1}\rangle$, so

that $\langle\Psi_0|\Psi_1\rangle = 0$. Summarizing, we can say that if (2) and (4) are satisfied, which implies that $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are product states, then either they are orthogonal, or the measurement always fails.

Finally, let us look at the situation when (1) and (4) are true which is equivalent to the case where (2) and (3) are true. This implies that $A_0 = B_0 = 0$, so that $|\Psi_0\rangle$ is never detected, and that $|\Psi_0\rangle$ is a product state. After using similar techniques to those in the previous paragraphs, we find that

$$\begin{aligned} A_1 &= |\eta_A\rangle\langle u_{A1}| \quad B_1 = |\eta_B\rangle\langle u_{B1}| \\ A_f &= |\xi_A\rangle\langle u_{A0}| \quad B_f = |\xi_B\rangle\langle u_{B0}|, \end{aligned} \tag{4.1.9}$$

where the vectors $|\xi_A\rangle$, $|\xi_B\rangle$, $|\eta_A\rangle$, and $|\eta_B\rangle$ are undetermined unit vectors. The final conditions are given by using the above expressions in the equations $A_1 B_f|\Psi_1\rangle = 0$ and $A_f B_1|\Psi_1\rangle = 0$ to give

$$\begin{aligned} \langle u_{A1}| \otimes \langle u_{B0}|)|\Psi_1\rangle &= 0 \\ \langle u_{A0}| \otimes \langle u_{B1}|)|\Psi_1\rangle &= 0. \end{aligned} \tag{4.1.10}$$

Let us summarize our results. We found that the best we can do is to identify one of the states with a nonzero probability and fail the rest of the time. Let us look at an example. Let us consider the two nonorthogonal states given by

$$\begin{aligned} |\Psi_0\rangle &= |0\rangle|0\rangle \\ |\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \end{aligned} \tag{4.1.11}$$

where Alice's qubits are the first and Bob's qubit are in the second position. In addition, we have that $A_0 = B_0 = 0$, so that $|\Psi_0\rangle$ is never detected, and

$$A_1 = |1\rangle\langle 1| \quad B_1 = |1\rangle\langle 1|$$
$$A_f = |0\rangle\langle 0| \quad B_f = |0\rangle\langle 0|. \tag{4.1.12}$$

From this we see that, indeed, if $|\Psi_0\rangle$ is sent, then it will not be detected, but if $|\Psi_1\rangle$ is sent, then we will detect it with a probability of 1/2 and fail with a probability of 1/2. Thus, we are very limited in distinguishing two states without any classical communication between Alice and Bob.

4.2 Limited classical communication

The situation becomes more interesting if we allow Alice and Bob to communicate the results of their measurements to each other only after both measurements have been made. We now consider the following situation. Alice and Bob make measurements on their particles, and each of these measurements can have one of two outcomes, 0 or 1. Alice's measurement is described by the POVM $\{A_0, A_1\}$ and Bob's by $\{B_0, B_1\}$, where

$$I_A = A_0^\dagger A_0 + A_1^\dagger A_1 \qquad I_B = B_0^\dagger B_0 + B_1^\dagger B_1, \tag{4.2.1}$$

and I_A and I_B are the identity operators in Alice's and Bob's Hilbert spaces, respectively. The probability that Alice will obtain the result k if the two qubit-state is $|\Psi_j\rangle$ is given by $\langle\Psi_j|A_k^\dagger A_k|\Psi_j\rangle$. On the other hand, the probability that Bob obtains the

result l is given by $\langle\Psi_j|B_l^\dagger B_l|\Psi_j\rangle$. Note that A_0 and A_1 commute with B_0 and B_1.

Together, Alice and Bob have four possible sets of results (Alice's result is given first, Bob's second), $\{0,0\}$, $\{0,1\}$, $\{1,0\}$, $\{1,1\}$, and we have to decide which sets correspond to $|\Psi_0\rangle$, which to $|\Psi_1\rangle$, and which to failure to decide. Let us first consider what happens if we assume that none of the sets corresponds to failure. In particular, suppose that $\{0,0\}$ and $\{1,1\}$ correspond to $|\Psi_0\rangle$ and $\{0,1\}$ and $\{1,0\}$ correspond to $|\Psi_1\rangle$. This implies that if the state is $|\Psi_1\rangle$, then the probability of getting $\{0,0\}$ or $\{1,1\}$ is zero, and if the state is $|\Psi_0\rangle$, the probability of getting $\{0,1\}$ or $\{1,0\}$ is zero. Therefore, we have

$$\begin{aligned}\langle\Psi_0|A_0^\dagger A_0 B_1^\dagger B_1|\Psi_0\rangle &= \langle\Psi_0|A_1^\dagger A_1 B_0^\dagger B_0|\Psi_0\rangle &= 0\\ \langle\Psi_1|A_0^\dagger A_0 B_0^\dagger B_0|\Psi_1\rangle &= \langle\Psi_1|A_1^\dagger A_1 B_1^\dagger B_1|\Psi_1\rangle &= 0.\end{aligned} \tag{4.2.2}$$

These imply the simpler equations

$$\begin{aligned}A_0 B_1|\Psi_0\rangle &= A_1 B_0|\Psi_0\rangle &= 0\\ A_0 B_0|\Psi_1\rangle &= A_1 B_1|\Psi_1\rangle &= 0.\end{aligned} \tag{4.2.3}$$

If we now note that

$$\begin{aligned}\langle\Psi_1|\Psi_0\rangle &= \langle\Psi_1|I_A\otimes I_B|\Psi_0\rangle\\ &= \langle\Psi_1|(A_0^\dagger A_0 + A_1^\dagger A_1)\otimes(B_0^\dagger B_0 + B_1^\dagger B_1)\Psi_0\rangle,\end{aligned} \tag{4.2.4}$$

we see from the previous equation that $\langle\Psi_1|\Psi_0\rangle = 0$. Therefore, if we are able to distinguish the states every time without error, they must be orthogonal.

Now let us suppose that some of the measurement results correspond to a failure to distinguish the states. We will focus on two different cases. In the first we shall assume that two of the four alternatives correspond to failure, and in the second we shall assume that only one does.

4.2.1 Two failure states

Let us assume that $\{0,0\}$ corresponds to $|\Psi_0\rangle$, $\{1,1\}$ corresponds to $|\Psi_1\rangle$, and both $\{0,1\}$ and $\{1,0\}$ correspond to failure to distinguish. The condition of no errors implies that

$$A_0 B_0 |\Psi_1\rangle = 0 \qquad A_1 B_1 |\Psi_0\rangle = 0. \tag{4.2.5}$$

If we apply these conditions to Eq. (4.2.4), we find that

$$\langle \Psi_1 | \Psi_0 \rangle = \langle \Psi_1 | F | \Psi_0 \rangle, \tag{4.2.6}$$

where

$$F = A_0^\dagger A_0 B_1^\dagger B_1 + A_1^\dagger A_1 B_0^\dagger B_0. \tag{4.2.7}$$

Now let us examine the conditions in Eq. (4.2.5) in more detail. We first express $|\Psi_1\rangle$ in its Schmidt basis

$$|\Psi_1\rangle = \sum_{j=0}^{1} \sqrt{\lambda_{1j}} |v_{Aj}\rangle \otimes |v_{Bj}\rangle, \tag{4.2.8}$$

where $\{|v_{A0}\rangle, |v_{A1}\rangle\}$ and $\{|v_{B0}\rangle, |v_{B1}\rangle\}$ are orthonormal bases for Alice's and Bob's spaces, respectively, and λ_{1j} for $j = 0, 1$ are the eigenvalues of the reduced density

matrixes. The condition $A_0 B_0 |\Psi_1\rangle = 0$ then implies that

$$\sqrt{\lambda_{10}} A_0 |v_{A0}\rangle \otimes B_0 |v_{B0}\rangle = -\sqrt{\lambda_{11}} A_0 |v_{A1}\rangle \otimes B_0 |v_{B1}\rangle. \tag{4.2.9}$$

The only way this can be true is if $A_0|v_{A0}\rangle$ is parallel to $A_0|v_{A1}\rangle$ and $B_0|v_{B0}\rangle$ is parallel to $B_0|v_{B1}\rangle$. Therefore, we can write

$$\begin{aligned} A_0|v_{A0}\rangle = c_0|\eta_A\rangle \quad B_0|v_{B0}\rangle = d_0|\eta_B\rangle \\ A_0|v_{A1}\rangle = c_1|\eta_A\rangle \quad B_0|v_{B1}\rangle = d_1|\eta_B\rangle, \end{aligned} \tag{4.2.10}$$

where c_j and d_j are constants and $\|\eta_A\| = \|\eta_B\| = 1$. These equations imply that

$$\begin{aligned} A_0 &= \sum_{j=0}^{1} c_j |\eta_A\rangle\langle v_{Aj}| = |\eta_A\rangle\langle r_A| \\ B_0 &= \sum_{j=0}^{1} d_j |\eta_B\rangle\langle v_{Bj}| = |\eta_B\rangle\langle r_B|, \end{aligned} \tag{4.2.11}$$

where

$$|r_A\rangle = \sum_{j=0}^{1} c_j^* |v_{Aj}\rangle \qquad |r_B\rangle = \sum_{j=0}^{1} d_j^* |v_{Bj}\rangle. \tag{4.2.12}$$

The condition $A_0 B_0 |\Psi_1\rangle = 0$ can now be expressed as

$$(\langle r_A| \otimes \langle r_B|)|\Psi_1\rangle = 0. \tag{4.2.13}$$

We can now do the same thing with the condition that $A_1 B_1 |\Psi_0\rangle = 0$. Expressing $|\Psi_0\rangle$ in its Schmidt basis we have that

$$|\Psi_0\rangle = \sum_{j=0}^{1} \sqrt{\lambda_{0j}} |u_{Aj}\rangle \otimes |u_{Bj}\rangle, \tag{4.2.14}$$

where $\{|u_{A0}\rangle, |u_{A1}\rangle\}$ and $\{|u_{B0}\rangle, |u_{B1}\rangle\}$ are orthonormal bases for Alice's and Bob's spaces, respectively, and λ_{0j} for $j = 0, 1$ are the eigenvalues of the reduced density matrixes. Applying the same reasoning as before, we find that

$$A_1 = |\xi_A\rangle\langle s_A| \qquad B_1 = |\xi_B\rangle\langle s_B|, \tag{4.2.15}$$

where $\|\xi_A\| = \|\xi_B\| = 1$. We also have that

$$(\langle s_A| \otimes \langle s_B|)|\Psi_0\rangle = 0. \tag{4.2.16}$$

We can gain more information about the vectors $|r_A\rangle$, $|r_B\rangle$, $|s_A\rangle$, and $|s_B\rangle$ by substituting the results of the previous paragraphs into Eqs. (4.2.1). This gives us that

$$I_A = |r_A\rangle\langle r_A| + |s_A\rangle\langle s_A| \qquad I_B = |r_B\rangle\langle r_B| + |s_B\rangle\langle s_B|. \tag{4.2.17}$$

Now let both sides of the first of these equations act on the vector $|r_A\rangle$,

$$\|r_A\|^2|r_A\rangle + |s_A\rangle\langle s_A|r_A\rangle = |r_A\rangle. \tag{4.2.18}$$

The only way this can be true is if either $|r_A\rangle$ is parallel to $|s_A\rangle$ which violates Eq. (4.2.17), or if $\langle s_A|r_A\rangle = 0$ and $\|r_A\| = 1$. Therefore, $|s_A\rangle$ is orthogonal to $|r_A\rangle$, and both have norm 1. Henceforth, we shall denote $|s_A\rangle$ by $|r_A^\perp\rangle$, and we have that $\{|r_A\rangle, |r_A^\perp\rangle\}$ is an orthonormal basis for Alice's space. Similarly, we find that $\{|r_B\rangle, |r_B^\perp\rangle\}$, where $|r_B^\perp\rangle = |s_B\rangle$, is an orthonormal basis for Bob's space.

Now let us examine the failure probabilities. We first express the operator F, defined in Eq. (4.2.7) as

$$\begin{aligned} F &= (|r_A\rangle \otimes |r_B^\perp\rangle)(\langle r_A| \otimes \langle r_B^\perp|) + (|r_A^\perp\rangle \otimes |r_B\rangle)(\langle r_A^\perp| \otimes \langle r_B|) \\ &= I - (|r_A\rangle \otimes |r_B\rangle)(\langle r_A| \otimes \langle r_B|) \\ &\quad -(|r_A^\perp\rangle \otimes |r_B^\perp\rangle)(\langle r_A^\perp| \otimes \langle r_B^\perp|). \end{aligned} \tag{4.2.19}$$

We first note that if Eqs. (4.2.13) and (4.2.16) are satisfied, then the condition in Eq. (4.2.6) is also satisfied. The failure probability if Charlie sends the state $|\Psi_0\rangle$ is $\langle\Psi_0|F|\Psi_0\rangle$, and if he sends the state $|\Psi_1\rangle$, it is $\langle\Psi_1|F|\Psi_1\rangle$. These probabilities can be expressed as

$$\begin{aligned} \langle\Psi_0|F|\Psi_0\rangle &= 1 - |(\langle r_A| \otimes \langle r_B|)|\Psi_0\rangle|^2 \\ \langle\Psi_1|F|\Psi_1\rangle &= 1 - |(\langle r_A^\perp| \otimes \langle r_B^\perp|)|\Psi_1\rangle|^2. \end{aligned} \tag{4.2.20}$$

If each of the states is equally likely, then the total failure probability, p_f, is given by

$$p_f = \frac{1}{2}(\langle\Psi_0|F|\Psi_0\rangle + \langle\Psi_1|F|\Psi_1\rangle). \tag{4.2.21}$$

We want to minimize this overall failure probability.

Note that the failure probabilities are unaffected by the choice of the vectors $|\xi_A\rangle, |\xi_B\rangle, |\eta_A\rangle$, and $|\eta_B\rangle$. If we make the choices

$$\begin{aligned} |\xi_A\rangle = |r_A^\perp\rangle \quad |\xi_B\rangle = |r_B^\perp\rangle \\ |\eta_A\rangle = |r_A\rangle \quad |\eta_B\rangle = |r_B\rangle, \end{aligned} \tag{4.2.22}$$

then the operators A_j and B_j, where $j = 1, 2$, are projections and the generalized measurement becomes a von Neumann measurement.

Our problem is the following. We want to find a basis for Alice's space, $\{|r_A\rangle, |r_A^\perp\rangle\}$, and one for Bob's space, $\{|r_B\rangle, |r_B^\perp\rangle\}$, that satisfy the conditions

$$\begin{aligned}(\langle r_A^\perp| \otimes \langle r_B^\perp|)|\Psi_0\rangle &= 0 \\ (\langle r_A| \otimes \langle r_B|)|\Psi_1\rangle &= 0.\end{aligned} \tag{4.2.23}$$

We can reduce these conditions to the solution of several simple equations. First, expanding $|r_A^\perp\rangle$ and $|r_B^\perp\rangle$ in terms of $|u_{Aj}\rangle$ and $|u_{Bj}\rangle$, respectively, we have

$$|r_A^\perp\rangle = \sum_{j=0}^{1} e_j^*|u_{Aj}\rangle \qquad |r_B^\perp\rangle = \sum_{j=0}^{1} f_j^*|u_{Bj}\rangle. \tag{4.2.24}$$

The equations in the previous paragraph become

$$\sum_{j=0}^{1} \sqrt{\lambda_{0j}} e_j f_j = 0 \qquad \sum_{j=0}^{1} \sqrt{\lambda_{1j}} c_j d_j = 0, \tag{4.2.25}$$

while the conditions $\langle r_A^\perp|r_A\rangle = 0$ and $\langle r_B^\perp|r_B\rangle = 0$ become

$$\begin{aligned}\sum_{j_1,j_2=0}^{1} c_{j_1} e_{j_2}^* \langle v_{Aj_1}|u_{Aj_2}\rangle = 0 \\ \sum_{j_1,j_2=0}^{1} d_{j_1} f_{j_2}^* \langle v_{Bj_1}|u_{Bj_2}\rangle = 0.\end{aligned} \tag{4.2.26}$$

Now define the ratios

$$\begin{aligned}z_1 = \frac{c_1^*}{c_0^*} \quad z_2 = \frac{d_1^*}{d_0^*} \\ z_3 = \frac{e_1^*}{e_0^*} \quad z_4 = \frac{f_1^*}{f_0^*}.\end{aligned} \tag{4.2.27}$$

If we now divide Eqs. (4.2.25) and (4.2.26) by the appropriate product of expansion coefficients, e.g. the first of Eqs. (4.2.25) is divided by $e_0 f_0$ and the first of Eqs. (4.2.26) is divided by $c_0 e_0^*$, we find

$$\begin{aligned}
\sqrt{\lambda_{00}} + \sqrt{\lambda_{01}} z_3 z_4 &= 0 \\
\sqrt{\lambda_{10}} + \sqrt{\lambda_{11}} z_1 z_2 &= 0 \\
\langle v_{A0}|u_{A0}\rangle + \langle v_{A0}|u_{A1}\rangle z_3 & \\
+\langle v_{A1}|u_{A0}\rangle z_1^* + \langle v_{A1}|u_{A1}\rangle z_1^* z_3 &= 0 \\
\langle v_{B0}|u_{B0}\rangle + \langle v_{B0}|u_{B1}\rangle z_4 & \\
+\langle v_{B1}|u_{B0}\rangle z_2^* + \langle v_{B1}|u_{B1}\rangle z_2^* z_4 &= 0. \qquad (4.2.28)
\end{aligned}$$

Given two specific states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, these equations can be solved to find the vectors $|r_A\rangle$, $|r_A^\perp\rangle$, $|r_B\rangle$, and $|r_B^\perp\rangle$.

We want to look at the solution for two different examples. In the first we shall suppose that $|\Psi_0\rangle$ and $|\Psi_1\rangle$ have the same Schmidt bases while in the second example the Schmidt bases of the two states will be different.

We begin by assuming that our two states are given by

$$\begin{aligned}
|\Psi_0\rangle &= \cos\theta_0|00\rangle + \sin\theta_0|11\rangle \\
|\Psi_1\rangle &= \cos\theta_1|00\rangle + \sin\theta_1|11\rangle, \qquad (4.2.29)
\end{aligned}$$

where θ_0 and θ_1 are both between 0 and $\pi/2$. Solving Eqs. (4.2.28) for these states, we first find the condition $\tan\theta_0 \tan\theta_1 = 1$, which implies that $\theta_1 = (\pi/2) - \theta_0$. We

also find explicit expressions for the vectors

$$\begin{aligned} |r_A\rangle &= c_0^*(|0\rangle + z_1|1\rangle) \\ |r_B\rangle &= d_0^*\left(|0\rangle - \frac{\cot\theta_1}{z_1}|1\rangle\right) \\ |r_A^\perp\rangle &= e_0^*\left(|0\rangle - \frac{1}{z_1}|1\rangle\right) \\ |r_B^\perp\rangle &= f_0^*(|0\rangle + \cot\theta_0 z_1^*|1\rangle), \end{aligned} \tag{4.2.30}$$

where the normalization constants are given by

$$\begin{aligned} |c_0|^2 &= \frac{1}{1+|z_1|^2} \\ |d_0|^2 &= \frac{|z_1|^2}{|z_1|^2 + (\cot\theta_1)^2} \\ |e_0|^2 &= \frac{|z_1|^2}{1+|z_1|^2} \\ |f_0|^2 &= \frac{1}{1+(\cot\theta_1)^2|z_1|^2}. \end{aligned} \tag{4.2.31}$$

The quantity z_1 is at the moment undetermined, but it will be fixed by requiring the failure probability to be a minimum. This probability is now given by

$$p_f = 1 - \frac{|z_1|^2}{2+2|z_1|^2}\,\frac{(1-(\cot\theta_1)^2)^2}{1+(|z_1|\cot\theta_1)^2}\,\frac{(1-(\tan\theta_1)^2)^2}{1+(|z_1|\tan\theta_1)^2}, \tag{4.2.32}$$

where the condition $\theta_0 = (\pi/2) - \theta_1$ has been used to eliminate θ_0. Setting the derivative of p_f with respect to $|z_1|^2$ equal to zero, we find an equation that has only one positive solution, $|z_1|^2 = \cot\theta_1$. Substituting this value into Eq. (4.2.32), we find

$$p_f = \sin(2\theta_1) \tag{4.2.33}$$

This failure probability should be compared to that when a single joint measurement can be performed on both qubits of the two-qubit states. In that case, if each of the states is equally likely, then the probability of failing to distinguish between the states is given by the IDP limit

$$p_{fidp} = |\langle\Psi_0|\Psi_1\rangle| = \sin(2\theta_1). \tag{4.2.34}$$

Note that this expression is identical to that given in the previous paragraph. Therefore, in this example we can conclude that the failure probability that is achieved by measuring the qubits separately is the same as that when the qubits are measured together.

Now let us see what happens if the states have different Schmidt bases. We shall keep $|\Psi_0\rangle$ the same as in the previous example. However, we choose $|\Psi_1\rangle$ differently,

$$\begin{aligned} |\Psi_0\rangle &= \cos\theta_0|00\rangle + \sin\theta_0|11\rangle \\ |\Psi_1\rangle &= \cos\theta_1|+x\rangle|+x\rangle + \sin\theta_1|-x\rangle|-x\rangle, \end{aligned} \tag{4.2.35}$$

where $|\pm x\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)$. Solving Eqs. (4.2.28) for these states, we first find a quadratic equation for z_1

$$(1-\cot\theta_0)z_1^2 - (1-\cot\theta_1)(1+\cot\theta_0)z_1 - (1-\cot\theta_0)\cot\theta_1 = 0. \tag{4.2.36}$$

The vectors making up the POVM are given by

$$\begin{aligned}
|r_A\rangle &= c_0^*(|+x\rangle + z_1|-x\rangle) \\
|r_B\rangle &= d_0^*\left(|+x\rangle - \frac{\cot\theta_1}{z_1}|-x\rangle\right) \\
|r_A^\perp\rangle &= e_0^*(|0\rangle + z_3|1\rangle) \\
|r_B\rangle &= f_0^*\left(|0\rangle - \frac{\cot\theta_0}{z_3}|1\rangle\right).
\end{aligned} \tag{4.2.37}$$

The normalization constants are given by

$$\begin{aligned}
|c_0|^2 = \frac{1}{1+|z_1|^2} \qquad |e_0|^2 = \tfrac{1}{1+|z_3|^2} \\
|d_0|^2 = \frac{|z_1|^2}{|z_1|^2+\cot^2\theta_1} \quad |f_0|^2 = \tfrac{|z_3|^2}{|z_3|^2+\cot^2\theta_0},
\end{aligned} \tag{4.2.38}$$

where

$$z_3 = -\frac{1-\cot\theta_0\cot\theta_1+(1-\cot\theta_0)z_1^*}{1-\cot\theta_1}. \tag{4.2.39}$$

The failure probability is given by Eqs. (4.2.20) and (4.2.21), where

$$\begin{aligned}
|(\langle r_A|\otimes\langle r_B|)\Psi_0\rangle|^2 = \frac{|z_1|^2\sin^2\theta_0}{4(1+|z_1|^2)(|z_1|^2+\cot^2\theta_1)} \\
\left|(1+\cot\theta_0)(1-\cot\theta_1)+(\cot\theta_0-1)\left(z_1^*-\frac{\cot\theta_1}{z_1^*}\right)\right|^2 \\
|(\langle r_A^\perp|\otimes\langle r_B^\perp|)\Psi_1\rangle|^2 = \frac{|z_3|^2\sin^2\theta_1}{4(1+|z_3|^2)(|z_1|^3+\cot^2\theta_0)} \\
\left|(1+\cot\theta_1)(1-\cot\theta_0)+(\cot\theta_1-1)\left(z_3-\frac{\cot\theta_0}{z_3}\right)\right|^2.
\end{aligned} \tag{4.2.40}$$

Specializing to the case $\theta_0 = \pi/2$ we find that there are two sets of values for $z_1, \ldots z_4$. One set is obtained from the other simply by reversing the roles of $|r_A\rangle$ and

$|r_B\rangle$, and both give the same failure probability, so that we need only consider one of them. Doing so we have that

$$\begin{aligned} z_1 &= \cot\theta_1 & z_2 &= -1 \\ z_3 &= \frac{1+\cot\theta_1}{\cot\theta_1 - 1} & z_4 &= 0. \end{aligned} \tag{4.2.41}$$

This gives a value for the failure probability of

$$p_f = 1 - \frac{(1-\cot\theta_1)^2 + (\cos\theta_1\cot\theta_1 - \sin\theta_1)^2}{4(1+\cot^2\theta_1)}. \tag{4.2.42}$$

This can be compared to the failure probability when both qubits are measured together, which corresponds to the case considered by Ivanovic, Dieks and Peres

$$p_{fidp} = |\langle\Psi_0|\Psi_1\rangle| = \frac{1}{2}(\sin\theta_1 + \cos\theta_1). \tag{4.2.43}$$

These probabilities are plotted as a function of θ_1 as shown in Figure4.1, where p_f and p_{fidp} are represented by a continuous line and a dotted line respectively.

It can be seen that, as expected, $p_f \geq p_{fidp}$. The probabilities are equal at some isolated points. However, in general, there is a cost that we pay , which manifests itself as a higher failure probability, associated with determining the state by performing independent measurements on the two particles. This example differs from our previous one in that here there is a difference between p_f and p_{fidp}, whereas there is none when the two states we are trying to distinguish share the same Schmidt basis.

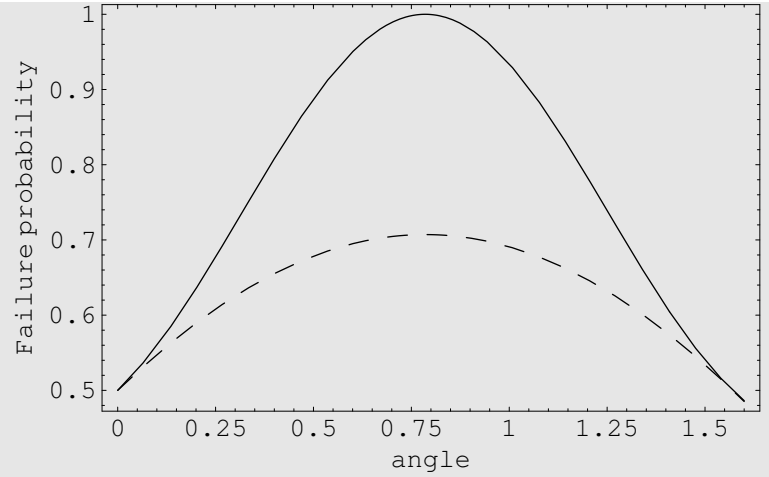

Figure 4.1: Failure probabilities as a function of the angle θ_1

4.2.2 One failure state

Let us now consider the case in which only one of the four measurement alternatives corresponds to failure. In particular, suppose that $\{0,0\}$ and $\{1,1\}$ correspond to $|\Psi_0\rangle$, $\{1,0\}$ corresponds to $|\Psi_1\rangle$, and $\{0,1\}$ corresponds to failure. We now have the conditions for our POVM operators

$$A_0 B_0 |\Psi_1\rangle = 0 \qquad A_1 B_1 |\Psi_1\rangle = 0$$
$$A_1 B_0 |\Psi_0\rangle = 0. \tag{4.2.44}$$

Using the same methods as before, we find that

$$A_0 = |r_A\rangle\langle r_A| \quad A_1 = |r_A^\perp\rangle\langle r_A^\perp|$$
$$B_0 = |r_B\rangle\langle r_B| \quad B_1 = |r_B^\perp\rangle\langle r_B^\perp|. \tag{4.2.45}$$

Where we previously had two conditions on the orthonormal bases $\{|r_A\rangle, |r_A^\perp\rangle\}$ and $\{|r_B\rangle, |r_B^\perp\rangle\}$, we now have three

$$(\langle r_A| \otimes \langle r_B|)\Psi_1\rangle = 0 \quad (\langle r_A^\perp| \otimes \langle r_B^\perp|)\Psi_1\rangle = 0$$
$$(\langle r_A^\perp| \otimes \langle r_B|)\Psi_0\rangle = 0. \tag{4.2.46}$$

Let us now consider an example. Let us assume that the states we are trying to distinguish have the same Schmidt basis and are given by

$$|\Psi_0\rangle = \cos\theta_0|00\rangle + \sin\theta_0|11\rangle$$
$$|\Psi_1\rangle = \cos\theta_1|00\rangle + \sin\theta_1|11\rangle,$$

Employing the same methods and notation as before, we find first that $\theta_1 = -\pi/4$, and that

$$z_1 = -z_4^* = \sqrt{\tan\theta_0}$$
$$z_2 = -z_3^* = \sqrt{\cot\theta_0} \tag{4.2.47}$$

The failure operator, F can be expressed as

$$F = A_0^\dagger A_0 B_1^\dagger B_1 = |r_A\rangle\langle r_A| \otimes |r_B^\perp\rangle\langle r_B^\perp|, \tag{4.2.48}$$

where

$$|r_A\rangle = \left(\frac{1}{1+\tan\theta_0}\right)^{1/2} (|0\rangle + \sqrt{\tan\theta_0}|1\rangle)$$
$$|r_B^\perp\rangle = \left(\frac{1}{1+\tan\theta_0}\right)^{1/2} (|0\rangle - \sqrt{\tan\theta_0}|1\rangle). \tag{4.2.49}$$

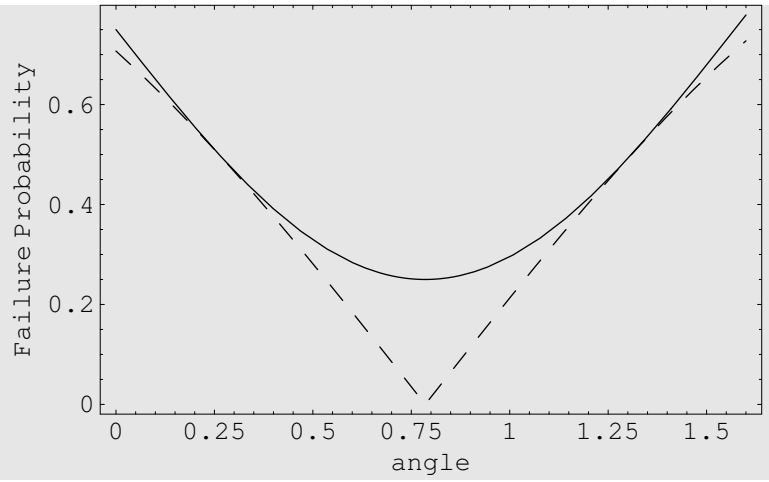

Figure 4.2: Failure probabilities as a function of the angle θ_0

If both states are equally probable, then the failure probability for this procedure is given by

$$\begin{aligned} p_f &= \frac{1}{2}(\langle\Psi_0|F|\Psi_0\rangle + \langle\Psi_1|F|\Psi_1\rangle) \\ &= \frac{1}{2}(\cos\theta_0 - \sin\theta_0)^2 + \frac{1}{4}. \end{aligned} \tag{4.2.50}$$

This probability and p_{fidp} are plotted as a function of θ_0 (θ_1 has been set equal to $-\pi/4$) as shown in Figure 4.2. Similar to the previous figure, we have p_f and p_{fidp} are represented by a continuous line and a dotted line respectively.

4.3 Secret sharing

An important application to state discrimination is secret sharing where two or more parties share a secret. Scientists have come up with several proposals for this problem

and only one experimental demonstration. There are two categories of the theoretical proposals. The first category uses quantum mechanics in order to securely distribute a classical shared key. One of these protocols is based on the use of GHZ states [22] and another makes use of pairs of Bell states in different bases [23]. An experiment based on the GHZ state protocol was carried out by Tittel, Zbinden and Gisin [24]. The second category consists of protocols in which the secret information that is split among several parties is quantum information [26]. The procedure we are considering here is of the first type.

Let us suppose that Charlie, sends one of two states to Alice and Bob, one qubit to Alice and one to Bob,

$$\begin{aligned} |\Psi_0\rangle &= \sin\theta|00\rangle + \cos\theta|11\rangle \\ |\Psi_1\rangle &= \cos\theta|00\rangle + \sin\theta|11\rangle. \end{aligned} \tag{4.3.1}$$

The procedure we are discussing here is based on the previous example in the preceding section. We first suppose that Alice makes a measurement of her state in the basis given by

$$\begin{aligned} |r_A\rangle &= \frac{1}{(1+\cot\theta)^{1/2}}(|0\rangle + \sqrt{\cot\theta}|1\rangle) \\ |r_A^{\perp}\rangle &= \frac{1}{(1+\tan\theta)^{1/2}}(|0\rangle - \sqrt{\tan\theta}|1\rangle), \end{aligned} \tag{4.3.2}$$

Bob on the other hand, makes a measurement on his particle in the basis

$$\begin{aligned} |r_B\rangle &= \frac{1}{(1+\cot\theta)^{1/2}}(|0\rangle - \sqrt{\cot\theta}|1\rangle) \\ |r_B^{\perp}\rangle &= \frac{1}{(1+\tan\theta)^{1/2}}(|0\rangle + \sqrt{\tan\theta}|1\rangle). \end{aligned} \tag{4.3.3}$$

Upon communicating their measurement outcomes, Alice and Bob can either determine the state that Charlie sent, or they will find out that their measurements have failed and they cannot infer the state of the system. The main point here is that,individually, Alice and Bob will not be able to make this determination. Hence, only together that they can share a key with Charlie. However, neither Alice nor Bob can individually learn the key .

Let us now examine the security of this scheme with regard to eavesdropping, and we will demonstrate that a simple changes have to be included to the procedure described above. The reason is that an eavesdropper, Eve, has a perfect cheating strategy. Eve simply captures the particles, and performs the same measurement on them that Alice and Bob would perform. She then sends particles to Alice and Bob consistent with her measurement results. For example, if she finds $|r_A\rangle$ and $|r_B\rangle$, she knows the state is $|\Psi_0\rangle$, and she sends a particle in $|r_A\rangle$ to Alice and a particle in $|r_B\rangle$ to Bob. Using this approach, Eve will know the key and Alice, Bob, and Charlie will not be aware of her presence.

This strategy of Eve's can be eliminated if Alice and Bob sometimes measure in the $\{|0\rangle, |1\rangle\}$ basis. Each of them chooses randomly, with some predetermined

probability, in which basis to measure. When they compare their results, they look at the instances in which they both measured in the $\{|0\rangle, |1\rangle\}$ basis, to see if their results were ever different. If they were, they can conclude that an eavesdropper was present. This defeats the attack proposed for Eve in the previous paragraph, because while the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ have no components along the vectors $|01\rangle$ and $|10\rangle$, states such as $|r_A\rangle|r_B\rangle$ do. That means that in order to avoid detection, Eve must send states lying in the subspace spanned by $|00\rangle$ and $|11\rangle$, which also means that she will not be able to control the results that Alice and Bob get. This leads to her detection. When she measures the state she receives from Charlie and fails, then she has to guess which state to send on to Alice and Bob. Sometimes she will guess incorrectly, and if Alice, Bob and Charlie publicly compare some fraction of their data, they will notice discrepancies, e.g. Charlie will have sent $|\Psi_0\rangle$, but Alice and Bob will have detected $|\Psi_1\rangle$. These discrepancies would not exist if Eve were not present, and their presence gives her away.

Now, let us see whether this procedure protects against cheating. Suppose that Bob is able to capture both qubits sent by Charlie. He first chooses a basis. If it is $\{|0\rangle, |1\rangle\}$, he sends a particle to Alice in one of these two states, and throws out the two-qubit state from Charlie (because of his basis choice the results from this state will not contribute to the key). When it comes time to compare results with Alice, if Alice measured the particle Bob sent in the other basis, the results are thrown

out, and if she also measured in the $\{|0\rangle, |1\rangle\}$ basis, Bob simply announces the result corresponding to the particle he sent her. If Bob chose to measure in the $\{|r_A\rangle, |r_A^{\perp}\rangle\}$ and $\{|r_B\rangle, |r_B^{\perp}\rangle\}$ bases, then, if he finds $|\Psi_0\rangle$ he send Alice $|r_A\rangle$, if $|\Psi_1\rangle$, he sends $|r_A^{\perp}\rangle$, and if he fails he sends either $|r_A\rangle$ or $|r_A^{\perp}\rangle$. If this is one of the results that is publicly compared, then if Bob's measurement succeeded, he announces the same state as the one he sent to Alice, and if it failed, the opposite state. Using this method, he knows the key bits, and Alice and Charlie do not know that he knows.

It is possible to fix this somewhat if instead of sending the particles to Alice and Bob simultaneously, Charlie first sends one particle to one party, who measures it and tells Charlie over a public channel that he or she has received and measured the particle. Charlie alternates sending the first particle to Alice and Bob. Now, supposing as before that Bob is the cheater, let us see what happens when the particle is sent to Alice first. Bob grabs the particle that has been sent to Alice, but then he must send her a substitute. If he sends her a particle in one of the states $|0\rangle$ or $|1\rangle$, there is no problem, but he cannot do this all of the time, because then no key bits would be generated. If he sends her a particle in either $|r_A\rangle$ or $|r_A^{\perp}\rangle$, he can run into a difficulty. Suppose he sent her $|r_A\rangle$, and when he receives the second particle from Charlie, he finds that the state Charlie sent was $|\Psi_1\rangle$, which should correspond to Alice measuring $|r_A^{\perp}\rangle$. If he is to avoid creating a detectable error, he must claim, if this is one of the bits which is publicly revealed, that he measured $|r_B^{\perp}\rangle$, which

corresponds to failure to distinguish. This, however, means that there will be more cases of failure to distinguish than there should be, and Alice and Charlie would be alerted to the fact that the security of the key is questionable.

Instead of sending Alice a single particle in a specific state, Bob can send Alice one of two particles in a singlet state. This, however, does not help him. From the particle remaining in his possession, he cannot determine which measurement Alice made, because his particle could be in one of four possible states, and these cannot all be orthogonal.

In summary, the procedure outlined here provides protection against eavesdropping, and some protection against cheating. The presence of an eavesdropper leads to errors (misidentification of states) while the presence of a cheater leads to an increased failure rate.

4.4 Qutrits

Higher dimensional quantum systems lead to more dense data recording in comparison with the two-dimensional systems. This means that within the cryptography domain, there will be a faster rate of data exchange and more security against eavesdropping.

The qutrit is the simplest multilevel system after the qubit. We want to develop a procedure to unambiguously discriminate between two-qutrit states given that there will be restricted communication between the parties. Similar to the previous section, Alice and Bob perform local measurements on their particles and will each obtain the

outcomes 0 or 1. Therefore, the POVM describing the measurements are: $\{A_0, A_1\}$ for Alice and $\{B_0, B_1\}$ for Bob.

These operators satisfy

$$I_A = A_0^\dagger A_0 + A_1^\dagger A_1 \quad I_B = B_0^\dagger B_0 + B_1^\dagger B_1 \tag{4.4.1}$$

Suppose$\{0,0\}$ corresponds to $|\Psi_0\rangle$, and we have to decide which sets correspond to $|\Psi_0\rangle$,$\{1,1\}$ corresponds to $|\Psi_1\rangle$ and $\{0,1\}$, $\{1,0\}$ correspond failure to distinguish. The failure operator is:

$$F = A_0^\dagger A_0 B_1^\dagger B_1 + A_1^\dagger A_1 B_0^\dagger B_0 \tag{4.4.2}$$

$|\Psi_0\rangle$ and $|\Psi_1\rangle$ expressed in their Schmidt basis are:

$$\begin{aligned} |\Psi_0\rangle &= \sum_{j=0}^{2} \sqrt{\lambda_{0j}} |u_{Aj}\rangle \otimes |u_{Bj}\rangle \\ |\Psi_1\rangle &= \sum_{j=0}^{2} \sqrt{\lambda_{1j}} |v_{Aj}\rangle \otimes |v_{Bj}\rangle \end{aligned} \tag{4.4.3}$$

Where $\{|u_{A0}\rangle, |u_{A1}\rangle, |u_{A2}\rangle\}$ and $\{|v_{A0}\rangle, |v_{A1}\rangle, |v_{A2}\rangle\}$ are orthonormal basis for Alice's space.

$\{|u_{B0}\rangle, |u_{B1}\rangle, |u_{B2}\rangle\}$ and $\{|v_{B0}\rangle, |v_{B1}\rangle, |v_{B2}\rangle\}$ are orthonormal basis for Bob's space.

Since no errors are allowed, we need to have:

$$\begin{aligned} A_0 B_0 |\Psi_1\rangle &= 0 \\ A_1 B_1 |\Psi_0\rangle &= 0 \end{aligned} \tag{4.4.4}$$

Now, we need to find expressions for the operators A_0, A_1, B_0 and B_1 that will satisfy the error free conditions expressed in equations 4.4.3 as well as the conditions in Eq.4.4.2.

We find that

$$A_0^\dagger A_0 = |w_0\rangle\langle w_0| \quad A_1^\dagger A_1 = I_A - |w_0\rangle\langle w_0|$$

$$B_1^\dagger B_1 = |w_1\rangle\langle w_1| \quad B_0^\dagger B_0 = I_B - |w_1\rangle\langle w_1|$$

where;

$$\begin{aligned} |w_1\rangle &= d_0^*|v_{B0}\rangle + d_1^*|v_{B1}\rangle + |v_{B2}\rangle \\ |w_0\rangle &= \sqrt{x_0}d_0|v_{B0}\rangle + \sqrt{x_1}d_1|v_{B1}\rangle + |v_{B2}\rangle. \end{aligned} \tag{4.4.5}$$

and we also defined

$$x_0 = \frac{\lambda_{00}}{\lambda_{02}} \qquad x_1 = \frac{\lambda_{01}}{\lambda_{02}}. \tag{4.4.6}$$

In terms of these quantities, $|\Psi_0\rangle$ can now be expressed as follows;

$$|\Psi_0\rangle = \frac{1}{(1+x_0+x_1)^{1/2}}(\sqrt{x_0}|v_{A0}\rangle\otimes|v_{B0}\rangle + \sqrt{x_1}|v_{A1}\rangle\otimes|v_{B1}\rangle + |v_{A2}\rangle\otimes|v_{B2}\rangle), \tag{4.4.7}$$

Putting all of this together we find that

$$\begin{aligned} \langle\Psi_0|F|\Psi_0\rangle &= 1 - \frac{1}{(1+x_0+x_1)}\left[\frac{x_0|d_0|^2 + x_1|d_1|^2 + 1}{|d_0|^2+|d_1|^2+1} + \frac{x_0^2|d_0|^2 + x_1^2|d_1|^2 + 1}{x_0|d_0|^2 + x_1|d_1|^2 + 1}\right. \\ &\quad \left. - \frac{2(x_0|d_0|^2 + x_1|d_1|^2 + 1)^2}{(|d_0|^2+|d_1|^2+1)(x_0|d_0|^2 + x_1|d_1|^2 + 1)}\right] \end{aligned} \tag{4.4.8}$$

We found that when we put all of the Schmidt coefficients for $|\Psi_0\rangle$ equal to 1/3, the failure probability is found to be equal to 1. What happens is that the conditions

on the Schmidt coefficients guarantee that $|\Psi_0\rangle = |\Psi_1\rangle$, so that the states cannot be distinguished.

Chapter 5

Unambiguous discrimination with LOCC with failure signal shared among the parties

The schemes discussed in the previous sections have the following drawback. The key bits for which the measurement failed, and which, therefore, must be discarded, are only identified after Alice and Bob have compared their bit strings. It would be much better if the bits that must be discarded could be identified immediately. The previous procedure requires that Alice and Bob get together and then tell Charlie which bits are good and which are not. He can then send them a message. A procedure in which the failed bits are immediately identified, allows Charlie to send Alice and Bob the two-qubit states from which the key bits can be extracted, discard the failed bits, and then immediately send them the message. At some later time, Alice and Bob can get together, combine their bit strings to get the key, and then read the message, without further input from Charlie [25]. This latter scheme is much more flexible.

Now, we will show that this can be accomplished by adding a third measurement result for one or both of the parties. If this added result is obtained, the measurement then has failed to distinguish between the two bipartite quantum states. As discussed in a previous section, the case where the measurements of both Alice and Bob yield three three possible outcomes, 0, 1, and f, which denotes failure to distinguish is not possible. it was found that there are too many restrictions on the POVM elements and they cannot all be satisfied. Therefore, we cannot construct a POVM that is error-free, and for which Alice and Bob receive simultaneous failure signals, when the procedure fails. If this was possible, it would have been interesting since no classical communication would be needed. For this reason, we now would like to consider the situation in which only one party receives a failure indication when the measurement fails. We consider a special case, that in which $|\Psi_0\rangle$ and $|\Psi_1\rangle$ have the same Schmidt bases and are given by

$$\begin{aligned} |\Psi_0\rangle &= \cos\theta_0|00\rangle + \sin\theta_0|11\rangle \\ |\Psi_1\rangle &= \cos\theta_1|00\rangle + \sin\theta_1|11\rangle. \end{aligned} \tag{5.0.1}$$

The conditions that no errors are allowed are given by

$$\begin{aligned} A_0B_0|\Psi_0\rangle = 0 \qquad & A_1B_1|\Psi_0\rangle = 0 \\ A_0B_1|\Psi_1\rangle = 0 \qquad & A_1B_0|\Psi_1\rangle = 0. \end{aligned} \tag{5.0.2}$$

These conditions imply that for $j = 0, 1$ we have

$$A_j = x_j|\eta_{Aj}\rangle\langle r_j| \qquad B_j = y_j|\eta_{Bj}\rangle\langle s_j|, \tag{5.0.3}$$

and we shall express the vectors $|r_j\rangle$ and $|s_j\rangle$ in the basis $\{|0\rangle, |1\rangle\}$ as

$$\begin{aligned} |r_0\rangle &= a_0|0\rangle + a_1|1\rangle \qquad |s_0\rangle = c_0|0\rangle + c_1|1\rangle \\ |r_1\rangle &= b_0|0\rangle + b_1|1\rangle \qquad |s_1\rangle = d_0|0\rangle + d_1|1\rangle \end{aligned} \tag{5.0.4}$$

The no-error conditions can now be expressed as

$$\begin{aligned} \langle r_0|\langle s_0|\Psi_0\rangle = 0 \qquad \langle r_1|\langle s_1|\Psi_0\rangle = 0 \\ \langle r_0|\langle s_1|\Psi_1\rangle = 0 \qquad \langle r_1|\langle s_{10}|\Psi_1\rangle = 0. \end{aligned} \tag{5.0.5}$$

if we define the ratios

$$z_0 = \frac{a_1}{a_0} \quad z_1 = \tfrac{b_1}{b_0} \tag{5.0.6}$$

$$z_2 = \frac{c_1}{c_0} \quad z_3 = \tfrac{d_1}{d_0}, \tag{5.0.7}$$

Equations (5.0.5) become

$$\begin{aligned} 1 + z_0^* z_2^* \tan\theta_0 = 0 \qquad 1 + z_1^* z_3^* \tan\theta_0 = 0 \\ 1 + z_0^* z_3^* \tan\theta_1 = 0 \qquad 1 + z_1^* z_2^* \tan\theta_1 = 0 \end{aligned} \tag{5.0.8}$$

A necessary condition for these equations to have a solution is that $\tan\theta_0 = \pm\tan\theta_1$. We are not interested in the case where $\tan\theta_0 = \tan\theta_1$, since this implies

that our states are identical. We wish to examine the case where $\tan\theta_0 = -\tan\theta_1$, which implies that $\theta_1 = -\theta_0$. Hence, our two states can be expressed as

$$|\Psi_0\rangle = \cos\theta_0|00\rangle + \sin\theta_0|11\rangle$$
$$|\Psi_1\rangle = \cos\theta_0|00\rangle - \sin\theta_0|11\rangle \tag{5.0.9}$$

In this case, we find

$$z_2 = -\frac{1}{z_0}\cot\theta_0 \qquad z_3 = -\frac{1}{z_1}\cot\theta_0 \qquad z_1 = -z_0. \tag{5.0.10}$$

We can now express the vectors $|r_j\rangle$ and $|s_j\rangle$ as

$$|r_0\rangle = \frac{1}{\sqrt{1+|z_0|^2}}(|0\rangle + z_0|1\rangle)$$
$$|r_1\rangle = \frac{1}{\sqrt{1+|z_0|^2}}(|0\rangle - z_0|1\rangle)$$
$$|s_0\rangle = \sqrt{\frac{|z_0|^2}{|z_0|^2+\cot{\theta_0}^2}}(|0\rangle - \frac{\cot\theta_0}{z_0}|1\rangle)$$
$$|s_1\rangle = \sqrt{\frac{|z_0|^2}{|z_0|^2+\cot{\theta_0}^2}}(|0\rangle + \frac{\cot\theta_0}{z_0}|1\rangle).$$

The parameter z_0 is yet to be determined. The failure operators for Alice and Bob can be expressed as

$$A_f^\dagger A_f = I_A - |x_0|^2|r_0\rangle\langle r_0| - |x_1|^2|r_1\rangle\langle r_1| \tag{5.0.11}$$

$$B_f^\dagger B_f = I_B - |y_0|^2|s_0\rangle\langle s_0| - |y_1|^2|s_1\rangle\langle s_1|, \tag{5.0.12}$$

where x_j, y_j, and z_0, where $j = 0, 1$, must be chosen so that these are positive

operators. The condition $A_f^\dagger A_f \geq 0$ implies that

$$I_A - \frac{|x_0|^2}{1+|z_0|^2}(|0\rangle + z_0|1\rangle)(\langle 0| + z_0^*\langle 1|) - \frac{|x_1|^2}{1+|z_0|^2}(|0\rangle - z_0|1\rangle)(\langle 0| - z_0^*\langle 1|) \geq 0, \quad (5.0.13)$$

or, in matrix form

$$M_A = \begin{pmatrix} 1 - \frac{|x_0|^2+|x_1|^2}{1+|z_0|^2} & -\frac{z_0^*(|x_0|^2-|x_1|^2)}{1+|z_0|^2} \\ -\frac{z_0(|x_0|^2-|x_1|^2)}{1+|z_0|^2} & 1 - \frac{|z_0|^2(|x_0|^2+|x_1|^2)}{1+|z_0|^2} \end{pmatrix} \geq 0. \quad (5.0.14)$$

This matrix will be positive if both $\mathrm{T}rM_A \geq 0$, which implies that

$$2 - (|x_0|^2 - |x_1|^2) \geq 0, \quad (5.0.15)$$

and $\det M_A \geq 0$, which implies

$$(1+|z_0|^2)^2(1 - (|x_0|^2 - |x_1|^2)) + 4|z_0|^2|x_0|^2|x_1|^2 \geq 0. \quad (5.0.16)$$

Similar conditions are found from the requirement that $B_f^\dagger B_f \geq 0$.

Our goal is to minimize the total failure probability, p_f, which is given by

$$p_f = \frac{1}{2}\sum_{k=0}^{1}\langle \Psi_k | A_f^\dagger A_f \otimes I_B + I_A \otimes B_f^\dagger B_f | \Psi_k \rangle. \quad (5.0.17)$$

We have assumed that the probability of receiving either $|\Psi_0\rangle$ or $|\Psi_1\rangle$ is the same, i.e. 1/2. We shall specialize to the case $x_0 = x_1$ and $y_0 = y_1$. As we shall see, this will still allow us to obtain the minimum achievable failure probability. Doing so we find that

$$\begin{aligned} A_f^\dagger A_f &= I_A - \frac{2|x_0|^2}{1+|z_0|^2}(|0\rangle\langle 0| + |z_0|^2|1\rangle\langle 1|) \\ B_f^\dagger B_f &= I_B - \frac{2|y_0|^2|z_0|^2}{|z_0|^2 + \cot^2\theta_0}\left(|0\rangle\langle 0| + \frac{\cot^2\theta_0}{|z_0|^2}|1\rangle\langle 1|\right). \end{aligned} \quad (5.0.18)$$

It is clear from Eq. (5.0.17) that the failure probability will be a minimum when $|x_0|$ and $|y_0|$ are as large as possible, subject to the constraint that the operators $A_f^\dagger A_f$ and $B_f^\dagger B_f$ are positive. From the above equations, we see that this implies that if $|z_0| \leq 1$, then $|x_0|^2 = (1 + |z_0|^2)/2$ and

$$A_f^\dagger A_f = (1 - |z_0|^2)|1\rangle\langle 1|, \tag{5.0.19}$$

and if $|z_0| \geq 1$, then $|x_0|^2 = [1 + (1/|z_0|^2)]/2$, and

$$A_f^\dagger A_f = \left(1 - \frac{1}{|z_0|^2}\right)|0\rangle\langle 0|. \tag{5.0.20}$$

We also have that if $\cot^2\theta_0 \leq |z_0|^2$, then $|y_0|^2 = [1 + (\cot\theta_0/|z_0|)^2]/2$ and

$$B_f^\dagger B_f = \left(1 - \frac{\cot^2\theta_0}{|z_0|^2}\right)|1\rangle\langle 1|, \tag{5.0.21}$$

and if $\cot^2\theta_0 \geq |z_0|^2$, then $|y_0|^2 = [1 + (|z_0|/\cot\theta_0)^2]/2$ and

$$B_f^\dagger B_f = \left(1 - \frac{|z_0|^2}{\cot^2\theta_0}\right)|1\rangle\langle 1|. \tag{5.0.22}$$

Let us consider the case when $|z_0| \leq 1$ and $0 \leq \theta \leq \pi/4$, which implies that Eqs. (5.0.19) and (5.0.21) apply. We then have that the failure probability is given by

$$p_f = 1 - 2|z_0|^2 \sin^2\theta_0, \tag{5.0.23}$$

and it is clear that this is minimized by choosing $|z_0| = 1$. This gives us

$$p_f = \cos(2\theta_0), \tag{5.0.24}$$

which is just the IDP limit for the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, with the optimal failure probability for these states being given by

$$1 - p_{idp} = |\langle\Psi_1|\Psi_0\rangle| = \cos(2\theta_0). \tag{5.0.25}$$

This implies that by using this procedure, we can distinguish the states just as well by measuring the qubits separately and comparing the results as we can by performing a joint measurement on both of them.

Let us now summarize the results of the preceding calculations. The states we are distinguishing are given in Eq. (5.0.9), with $0 \leq \theta \leq \pi/4$. Alice's POVM elements are $|r_j\rangle\langle r_j|$, for $j = 0, 1$, with

$$\begin{aligned} |r_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |r_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \end{aligned} \tag{5.0.26}$$

and $A_f = 0$. This implies that Alice will only obtain the results 0 or 1 for her measurement, she will never receive a failure result. In fact, she simply performs a projective measurement. Bob's POVM elements are

$$B_j^\dagger B_j = \frac{1}{2}(1 + \tan^2\theta_0)|s_j\rangle\langle s_j| \tag{5.0.27}$$

for $j = 0, 1$, with

$$\begin{aligned} |s_0\rangle &= \sin\theta_0|0\rangle - \cos\theta_0|1\rangle \\ |s_1\rangle &= \sin\theta_0|0\rangle + \cos\theta_0|1\rangle, \end{aligned} \tag{5.0.28}$$

and, corresponding to the failure result,

$$B_f^\dagger B_f = (1 - \tan^2\theta_0)|0\rangle\langle 0| \tag{5.0.29}$$

.

Examining these results, we can now see, in a simple way, how this procedure works. Define the single qubit states $|\psi_j\rangle$, for $j = 0, 1$ as

$$|\psi_j\rangle = \cos\theta_0|0\rangle + (-1)^j \sin\theta_0|1\rangle. \tag{5.0.30}$$

When Alice performs her measurement, she obtains either 0 or 1. If she obtains 0, then Bob is left with the state $|\psi_0\rangle$ if $|\Psi_0\rangle$ was sent, and $|\psi_1\rangle$ if $|\Psi_1\rangle$ was sent. If she obtains 1, then Bob is left with the state $|\psi_1\rangle$ if $|\Psi_0\rangle$ was sent, and $|\psi_0\rangle$ if $|\Psi_1\rangle$ was sent. In either case, Bob is faced with discriminating between the non-orthogonal states $|\psi_0\rangle$ and $|\psi_1\rangle$. He then applies the optimal POVM to distinguish between these states, and if he succeeds, he knows which of the two states he has. What he does not know, is which of his single-qubit states corresponds to $|\Psi_0\rangle$, and which to $|\Psi_1\rangle$. It is this bit of information that the result of Alice's measurement contains. Only by combining the results of their measurements can Alice and Bob deduce which state was sent.

The analysis in the preceding paragraph immediately allows us to see that there is another solution to the problem of finding a POVM in which one of the parties can receive a failure signal, and that is the one in which the roles of Alice and Bob are

interchanged. It that case, Bob makes a projective measurement, and Alice makes a measurement whose results are described by a three-outcome POVM.

5.1 Optical realization

We now want to show how this measurement can be realized optically. The states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are two-photon states with the information encoded in the polarization of the photons. We suppose that $|0\rangle$ corresponds to the horizontal polarization and $|1\rangle$ corresponds to the vertical polarization. Since Alice's states are orthogonal, her measurement is then straightforward (Figure 5.1). She sends her photon through a polarization beam splitter. A horizontally polarized photon incident on this device will continue in a straight line while a vertically polarized photon will be deflected by ninety degrees. Alice can use a quarter wave plate so that a photon in the polarization state $|+x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ is transmitted and one in the polarization state $|-x\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ is deflected. She has detectors in both paths, and she simply observes which one clicks. when detector D_0 clicks, Alice knows that her qubit exists in the state $|+x\rangle$, but when detector D_1 clicks, she knows that her qubit is in the state $|-x\rangle$.

Bob's measurement is more complicated, but it has been worked out by Huttner, *et al.* [28]. They presented two implementations of the POVM, one in which the failure signal can be detected explicitly and one in which it cannot, and demonstrated the second experimentally. We shall describe their first scheme. It makes use of two

polarization beam splitters, and one standard, polarization-insensitive beam splitter. The input state, which is either $|\psi_0\rangle$ or $|\psi_1\rangle$, is sent into the first polarization beam splitter PBS_1, in mode a. The vertically polarized part of the state is deflected into mode b, while the horizontally polarized part continues in mode a. If the input state is given by $|\phi_{in}\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a$, where the subscripts on the states denote the mode, we have that just after the first polarization beam splitter

$$|\phi_{in}\rangle_A \rightarrow \alpha|0\rangle_a + \beta|1\rangle_b. \tag{5.1.1}$$

The beam splitter,BS, transmits a photon with transmissivity t and reflects it with reflectivity r. This implies that after passing through the beam splitter the state $|0\rangle_a$ becomes $t|0\rangle_a + r|0\rangle_c$. Finally, after the second polarization beam splitter,PBS_2, the output state, $|\phi_{out}\rangle$ is

$$|\phi_{out}\rangle = \alpha t|0\rangle_a + \beta|1\rangle_a + \alpha r|0\rangle_c. \tag{5.1.2}$$

Choosing $t = \tan\theta_0$, we have that if the input state is $|\psi_0\rangle$, then

$$|\phi_{out}\rangle = \sin\theta_0(|0\rangle_a + |1\rangle_a) + \sqrt{\cos 2\theta_0}|0\rangle_c, \tag{5.1.3}$$

and if the input state is $|\psi_1\rangle$, then

$$|\phi_{out}\rangle = \sin\theta_0(|0\rangle_a - |1\rangle_a) + \sqrt{\cos 2\theta_0}|0\rangle_c. \tag{5.1.4}$$

Note that the parts of the two output states in the a mode have orthogonal polarizations, and can be distinguished by orienting a third polarization beam splitter PBS_3,

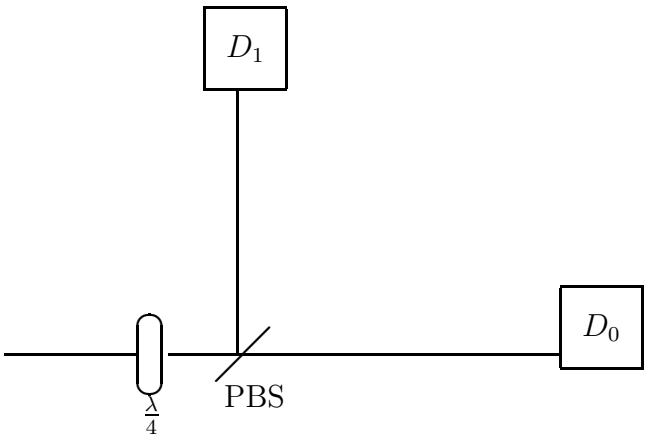

Figure 5.1: Apparatus to distinguish two orthogonal states.

so that $(|0\rangle_a + |1\rangle_a)/\sqrt{2}$ is transmitted and $(|0\rangle_a - |1\rangle_a)/\sqrt{2}$ is deflected. If the photon is detected in mode c, the procedure has failed. Bob's experimental set up is clearly more complicated than Alice's set up. Figure 5.2 shows how Bob's set up can be implemented.

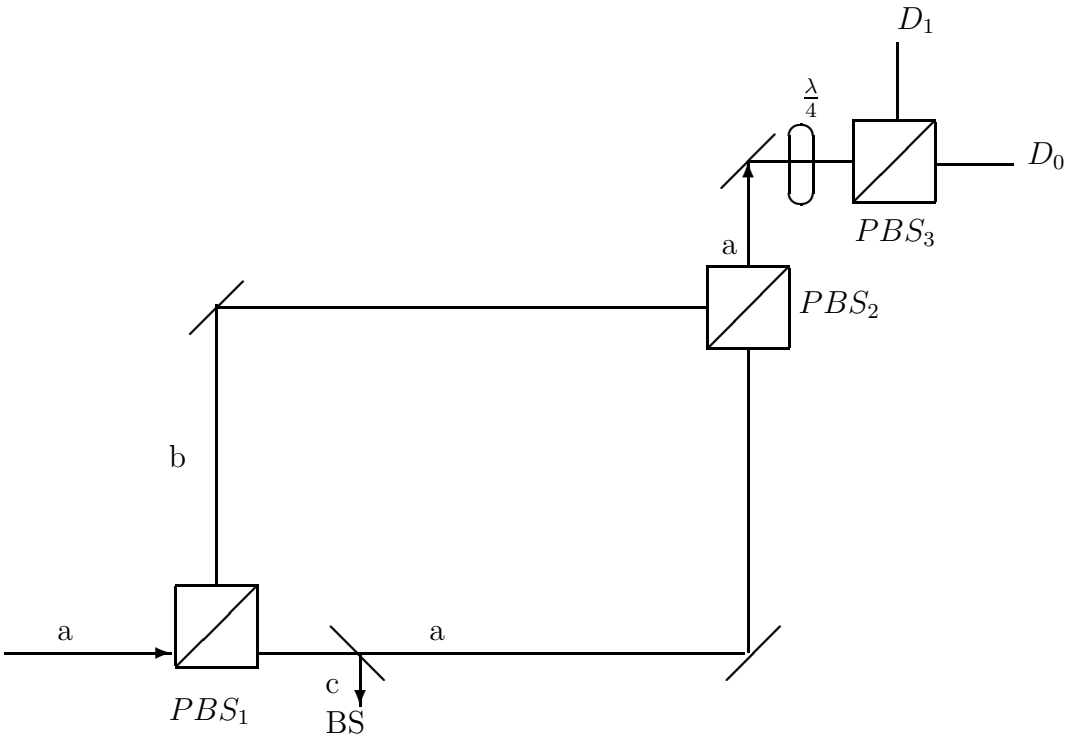

Figure 5.2: Experimental set up to distinguish nonorthogonal states. An incoming photon either in $|\psi_0\rangle$ or in $|\psi_1\rangle$ goes through PBS_1 which transmits a horizontally polarized photon into mode a and deflects a vertically polarized one into mode b. The transmitted photon passes through a beam splitter that transmits with a transmissivity t and reflects with a reflectivity r into mode c. The photon will also encounter PBS_2 while going trough the device. If the photon emerges in mode a, the measurement succeeds. However, a click in mode c means that the measurement has failed.

5.2 More than two parties

It is relatively easy to generalize the procedure in section 3 to divide the information about which of two states was sent among any number of parties. We shall show how to do this for both qubits and for qutrits.

Let us start with two N-qubit states

$$\begin{aligned} |\Psi_0\rangle &= \cos\theta_0|00\ldots0\rangle + \sin\theta_0|11\ldots1\rangle \\ |\Psi_1\rangle &= \cos\theta_0|00\ldots0\rangle - \sin\theta_0|11\ldots1\rangle, \end{aligned} \tag{5.2.1}$$

where $0 \leq \theta_0 \leq \pi/4$. Each of the qubits is sent to one of N parties, $A_1, \ldots A_N$. Each of the parties, A_1 through A_{N-1} measures their qubit in the $\{|r_0\rangle, |r_1\rangle\}$ basis (see Eq. (5.0.26)), and A_N performs the unambiguous-state discrimination procedure for the states $|\psi_0\rangle$ and $|\psi_1\rangle$ (see Eq. (5.0.30)). If parties A_1 through A_{N-1} obtained n_0 results of $|r_0\rangle$ and n_1 results of $|r_1\rangle$, then the states that A_N is distinguishing between are

$$\begin{aligned} |\psi_{0N}\rangle &= \cos\theta_0|0\rangle + (-1)^{n_1}\sin\theta_0|1\rangle \\ |\psi_{1N}\rangle &= \cos\theta_0|0\rangle - (-1)^{n_1}\sin\theta_0|1\rangle, \end{aligned} \tag{5.2.2}$$

i.e. A_N's qubit will be in the state $|\psi_{0N}\rangle$ if the state $|\Psi_0\rangle$ was sent and $|\psi_{1N}\rangle$ if the state $|\Psi_1\rangle$ was sent. In order to ascertain which of the two N-qubit states was sent, all of the parties will have to combine their information. If the measurement made by A_N succeeds, then she will have obtained either $|\psi_0\rangle$ or $|\psi_1\rangle$, but she will not,

without knowing the measurement results of all of the other parties, know which of these results corresponds to $|\Psi_0\rangle$ and which corresponds to $|\Psi_1\rangle$.

The procedure can be generalized to particles with more than two internal states, and to demonstrate this we shall consider the case of qutrits. Consider the three N-qutrit states

$$\begin{aligned} |\Psi_0\rangle &= c_0|0\ldots0\rangle + c_1|1\ldots1\rangle + c_2|2\ldots2\rangle \\ |\Psi_1\rangle &= c_0|0\ldots0\rangle + c_1\omega|1\ldots1\rangle + c_2\omega^*|2\ldots2\rangle \\ |\Psi_2\rangle &= c_0|0\ldots0\rangle + c_1\omega^*|1\ldots1\rangle + c_2\omega|2\ldots2\rangle, \end{aligned} \tag{5.2.3}$$

where $\omega = \exp(2\pi i/3)$. Define the single qutrit orthonormal basis

$$\begin{aligned} |\eta_0\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle) \\ |\eta_1\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \omega|1\rangle + \omega^*|2\rangle) \\ |\eta_2\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + \omega^*|1\rangle + \omega|2\rangle). \end{aligned} \tag{5.2.4}$$

Each of the N qutrits is sent to one of the parties $A_1, \ldots A_N$. Now, parties A_1 through A_{N-1} perform projective measurements in the basis $\{|\eta_0\rangle, |\eta_1\rangle, |\eta_2\rangle\}$, and suppose that m_j of them find their qutrit in the state $|\eta_j\rangle$, $j = 0, 1, 2$. The party A_N performs the optimal POVM to unambiguously distinguish the states [29, 30]

$$\begin{aligned} |\psi_0\rangle &= c_0|0\rangle + c_1|1\rangle + c_2|2\rangle \\ |\psi_1\rangle &= c_0|0\rangle + c_1\omega|1\rangle + c_2\omega^*|2\rangle \\ |\psi_2\rangle &= c_0|0\rangle + c_1\omega^*|1\rangle + c_2\omega|2\rangle. \end{aligned} \tag{5.2.5}$$

After the parties A_1 through A_{N-1} have performed their measurements, the qutrit belonging to A_N is in one of the three states

$$\begin{aligned} |\psi_{0N}\rangle &= c_0|0\rangle + c_1\omega^{(m_2-m_1)}|1\rangle + c_2\omega^{-(m_2-m_1)}|2\rangle \\ |\psi_{1N}\rangle &= c_0|0\rangle + c_1\omega^{(m_2-m_1+1)}|1\rangle + c_2\omega^{-(m_2-m_1+1)}|2\rangle \\ |\psi_{2N}\rangle &= c_0|0\rangle + c_1\omega^{(m_2-m_1-1)}|1\rangle + c_2\omega^{-(m_2-m_1-1)}|2\rangle. \end{aligned} \tag{5.2.6}$$

The qutrit is in the state ψ_{jN} if the original N-qutrit state was Ψ_j, for $j = 0, 1, 2$.

If the measurement made by A_N succeeds, she will have found her qutrit in one of the states $|\psi_j\rangle$, $j = 0, 1, 2$. She will not know to which of the original N-qutrit states it corresponds, however, without knowing the measurement results of all of the other parties. In particular, we have the correspondence

$$|\Psi_j\rangle \leftrightarrow |\psi_{[j+m_2-m_1\rangle \ \mathrm{mod}3]}. \tag{5.2.7}$$

Therefore, all of the parties must combine their information in order to determine which of the three N-qutrit states was originally sent.

Note that in both the case of N qubits and N qutrits, only one party will receive a failure signal if the measurement fails. In addition, the probability of failure is the same as if the best possible, i.e. it is the same as it would be if all of the qubits or qutrits were measured together. Consequently, we have not lost anything by measuring the particles separately.

5.3 secret sharing

So far, we have demonstrated how it is possible to distinguish between two non-orthogonal two-qubit states by means of local measurements and classical communication without making any errors and with one of the parties receiving a failure signal if the procedure fails. Both of parties, Alice and Bob make independent and local measurements. If the procedure succeeds, each party obtains either a 0 or a 1. However, they are not able to obtain enough information that will enable them to individually identify the state. It only after combining their measurement outcomes that the parties can identify the state.

This procedure should be useful as a basis for a quantum secret sharing protocol. An eavesdropper, Eve, who intercepts the two-qubit state cannot identify it with certainty. The best she can do is to apply the two-state unambiguous state discrimination procedure, which will sometimes fail. When it does, she does not know which state to send on to Alice and Bob, and will, consequently, introduce errors, e.g. Alice and Bob will have detected $|\Psi_0\rangle$ when $|\Psi_1\rangle$ was sent. These errors can be detected if Alice and Bob publicly compare a subset of their measurements with information provided by the person who sent the states.

There is also some protection against cheating. If Alice cheats by obtaining both qubits, then the best she can do is to apply two-state unambiguous state discrimination to them. Her measurement will sometimes fail, and then she has a problem.

She must send a qubit to Bob, but there is no state for this qubit that will make Bob's measurement fail with certainty. That means that Bob will sometimes obtain incorrect results, i.e. when he and Alice combine their results, they will find that the state they detected was not the one that was sent. Therefore, cheating by Alice will introduce errors. If Bob has obtained both particles, then he also can apply two-state unambiguous state discrimination to the two-qubit state. If his measurement succeeds, he can just send a qubit in the appropriate state to Alice, and if it fails, he can simply state that it failed. That means that cheating by Bob cannot be detected. However, a modification of the protocol will solve this problem. When the two-qubit state is sent, the person sending the state can announce over a public channel, which of the parties is to make the projective measurement and which is to make the three-outcome POVM. This means that part of the time, Bob will be assigned to make the projective measurement, and then his cheating will be detected. He can, however, not cheat if he is assigned to make the projective measurement, and in that case he will gain partial information about the key and not be detected. One way to address this problem is to combine several received bits into a block, the parity of which is a single key bit. In order for Bob to ascertain the key bit, he would have to know all of the received bits in the block, but the probability that he would can be made very low by choosing the block size sufficiently large.

Chapter 6

Conclusion

In the first part of this dissertation, we have examined the problem of distinguishing between two two-qubit states without error by using local measurements and either no or limited classical communication. In the first case we found that only one of the two states can be identified, the other generates a failure indication. In the second case, for some pairs of states it is possible to identify the states with the lowest possible failure probability. However, for other states, the failure probability with limited classical communication is higher than the optimal value. In addition, We proposed a secret sharing scheme based on limited classical communication scenario.

In the second part of the dissertation, we have shown that it is possible to distinguish unambiguously between two non-orthogonal two-qubit states by means of LOCC with one of the parties receiving a failure signal when the procedure fails. We found that for states sharing the same Schmidt basis, it is possible to distinguish between the states with the lowest failure probability. We showed how this can be

used as a basis for a quantum secret sharing protocol. We also, presented an experimental demonstration of how this procedure can be implemented. Furthermore, we generalized the problem to N-qubit and N-qutrit states.

Chapter 7

Appendix

The IDP limit is the optimum success probability to unambiguously discriminate between two nonorthogonal states, $|\Psi_0\rangle$ and $|\Psi_1\rangle$. These two states are linearly independent and assumed to be prepared with the same probabilities. $|\Psi_0\rangle$ and $|\Psi_1\rangle$ belong to the Hilbert space $\mathcal{H}$. We introduce an auxiliary space $\mathcal{A}$, which we call our failure space. The total Hilbert space of both subsystems is H where $H = \mathcal{H} \oplus A$. Therefore, $|\Psi_0\rangle$ and $|\Psi_1\rangle$ belong also to the larger system with Hilbert space H.

We now apply a unitary transformation which acts on the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ resulting in the states $|\Psi_0\rangle_{out}$ and $|\Psi_1\rangle_{out}$.

$$U|\Psi_0\rangle = |\Psi_0\rangle' + |\Phi_0\rangle = |\Psi_0\rangle_{out}$$

$$U|\Psi_1\rangle = |\Psi_1\rangle' + |\Phi_1\rangle = |\Psi_1\rangle_{out}$$

Where the states $|\Phi_i\rangle$ belong to the auxiliary system and the states $|\Psi_i\rangle'$ belong to the system with Hilbert space $\mathcal{H}$, where $i = 0, 1$. A measurement is now performed on $|\Psi_i\rangle_{out}$ that projects this state either on $|\Phi_i\rangle$ or on $|\Psi_i\rangle'$.

If the state of the system is projected onto $|\Psi_i^{'}\rangle$, the procedure succeeds, but if it is projected onto $|\Phi_i\rangle$, then the procedure fails.

Since we are considering unambiguous state discrimination, we need to have $\langle\Psi_1^{'}|\Psi_0\rangle^{'} = 0$. This means that when the procedure succeeds, we must distinguish between the states without making any errors.

In addition, because we require the procedure to be optimum, we must have $|\Phi_0\rangle$ and $|\Phi_1\rangle$ linearly dependent. This insures that no further unambiguous discrimination can be performed on those failure states. Therefore, we must have,

$$|\Phi_0\rangle = \sqrt{q_0}|e\rangle$$

$$|\Phi_1\rangle = e^{i\chi}\sqrt{q_1}|e\rangle$$

where q_0 and q_1 are real numbers and χ is the phase factor.

Because we consider unitary transformations, we must have,

$$\langle\Psi_0|U^{\dagger}U|\Psi_0\rangle = 1 \Rightarrow p_0 + q_0 = 1$$

$$\langle\Psi_1|U^{\dagger}U|\Psi_1\rangle = 1 \Rightarrow p_1 + q_1 = 1$$

$p_0 = \langle\Psi_0^{'}|\Psi_0^{'}\langle$ is the probability that the state of the system is $|\Psi_0\rangle$ and $p_1 = \langle\Psi_1^{'}|\Psi_1^{'}\langle$ is the probability that the system is in the state $|\Psi_1\rangle$.

We also have

$$\langle\Psi_1|U^{\dagger}U|\Psi_0\rangle = \langle\Psi_1|\Psi_0\rangle = e^{i\chi}\sqrt{q_0 q_1} \tag{7.0.1}$$

We have then,

$$|\langle\Psi_1|\Psi_0\rangle|^2 = q_0 q_1 \Rightarrow q_1 = \frac{|\langle\Psi_1|\Psi_0\rangle|^2}{q_0} \tag{7.0.2}$$

The total failure probability is

$$Q = \frac{1}{2}q_0 + \frac{1}{2}q_1 = \frac{1}{2}q_0 + \frac{1}{2}\frac{|\langle\Psi_1|\Psi_0\rangle|^2}{q_0} \tag{7.0.3}$$

This equation is minimum when $q_0 = |\langle\Psi_1|\Psi_0\rangle|$ Therefore, the minimum failure probability to distinguish between $|\Psi_0\rangle$ and $|\Psi_1\rangle$ is given by

$$Q_{opt} = |\langle\Psi_1|\Psi_0\rangle| \tag{7.0.4}$$

Therefore the optimum success probability to distinguish between the states, also known as the IDP limit, is given by

$$P_{IDP} = 1 - Q_{opt} = 1 - |\langle\Psi_1|\Psi_0\rangle| \tag{7.0.5}$$

Bibliography

[1] C. C. Gerry, P. L. Knight, Introductory Quantum Optics,p. 3, Cambridge university press (2005).

[2] J. J. Sakurai, Advanced Quantum Mechanics, p. 1, Addison-Wesley Publishing Company, (1967).

[3] D. Bouwmeester, A. Ekert, A. Zeilinger, The Physics of Quantum Information, p. 7, Springer press (2000).

[4] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information,p. 114, Cambridge University Press (2000).

[5] C. Brukner, M. Zukowski, A. Zeilinger,Quantum communication complexity protocol with two entangled qutrits, lanl e-print server Quant-ph/0205080.

[6] D. Bouwmeester, A. Ekert, A. Zeilinger, The Physics of Quantum Information, p. 3, Springer press (2000).

[7] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information,p. 14, Cambridge university press (2000).

[8] D. Bouwmeester, A. Ekert, A. Zeilinger, The Physics of Quantum Information, p. 1, Springer press (2000).

[9] C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett., **69**,2881 (1992).

[10] J. A. Bergou, U. Hergoz, M. Hillery, Discrimination of Quantum States, Lect. Notes Phys. **649**,p. 424 (2004).

[11] Y. Chen, D. Yang, Optimally conclusive discrimination of non-orthogonal entangled states locally, lanl e-print server Quant-ph/0104068.

[12] C. W. Helsrom, Quantum Detection and Estimation Theory, Academic Press, New York, (1976).

[13] J. A. Bergou, U. Hergoz, M. Hillery, Discrimination of Quantum States, Lect. Notes Phys. **649**,p. 425 (2004).

[14] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[15] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[16] A. Peres, Phys. Lett. A **128**, 19 (1988).

[17] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[18] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, quant-ph/0102073.

[19] Yi-Xin Chen and Dong Yang, Phys. Rev. A **65**,022320 (2002).

[20] J. Walgate, A. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[21] M. Hillery and J. Mimih, Phys. Rev. A **67**,042304 (2003).

[22] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**,1829 (1999).

[23] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[24] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[25] M. Hillery and J. Mimih, Phys. Rev. A **71**,012329 (2005).

[26] R. Cleve, D. Gottesman, and H. -K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[27] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen(De), and U. Sen, Phys. Rev. A **65**, 062307 (2002).

[28] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996).

[29] A. Peres and D. Terno, J. Phys. A **31**, 7105 (1998).

[30] Y. Sun, M. Hillery, and J. A. Bergou, Phys. Rev. A **64**, 022311 (2001).