Universidad de Concepción
Departamento de Física

APLICACIONES DE LA DISCRIMINACIÓN DE ESTADOS CUÁNTICOS

TESIS PARA OPTAR AL GRADO ACADÉMICO
DE DOCTOR EN CIENCIAS
CON MENCIÓN EN FÍSICA

por

Omar Alejandro Jiménez Henríquez

Universidad de Concepción
Facultad de Ciencias Físicas y Matemáticas
Departamento de Física
Concepción, Chile.

Agosto 2009

Director de Tesis	:	Dr. Aldo Delgado Hidalgo
Comisión	:	Dr. Luis Roa Oppliger
		Dr. Carlos Saavedra Rubilar
		Dr. Reinaldo Vianna

Dedicado a mi Madre y a mi Padre.

Agradecimientos

Primero, quiero dar gracias a la vida y a la oportunidad de conocer y admidar desde la Física la belleza del Universo. Quisiera agradecer a quienes han sido mis profesores. A Jose Aguirre, Jaime Araneda, Rolando Hernández, Patricio Salgado, Carlos Saavedra, Luis Roa, Aldo Delgado, Adelio Matamala, Guillermo Rubilar, Paul Minning. También deseo agradecer, al profesor Fernando Gutiérrez por su orientación durante mi primer año en Ciencias Físicas. En forma especial, agradezco al Profesor Carlos Saavedra por su disposición durante mis inicios en Física y también, a mi Tutor Aldo Delgado por confiar y trabajar junto a mi durante estos años. También, agradezco por compartir sus conocimientos junto a mi a los profesores en el extranjero, Andrei Klimov y Antonio Acín. También, quiero agradecer a mis amigos y compañeros de Física: Marcelo Alid, Leonardo Baez, Benjamin Burgos, Ronnie Burgos, Ignacia Calisto, Antollena Cid, Pablo Coelho, Maria Corona, Arturo Fernandez, Rodrigo Fuentes, Arturo Gomez, Nelson Merino, Patricio Mella, Rodrigo Navarro, Jazmina Olmos, Georgina Olivares, Carlos Paiva, Cristian Salas, Julio Oliva, Andres Anabalón, Cesar Sanchez, Javier Saez, Jose Luis Romero, Fabián Torres, Paola Utreras, Omar Valdivia, Marisol Zambrano y Abner Zapata por su amistad y discusiones siempre enriquecedoras. Mi más sincero agradecimiento para las secretarias del Departamento de Física; Marta Astudillo, Patricia Luarte, Marcela Sanhueza y Nubia Arancibia, y también para los auxiliares, Heraldo Manríquez y Víctor Mora.

Este trabajo no hubiera sido posible sin el apoyo y comprensión de mi familia; a mi Madre Maria Henríquez, mi Padre Victor Jiménez, mi dos hermanos Rodrigo Jiménez y Victor Jiménez y hermana Angélica Jiménez. También, agradezco a Karla Kauffmann por su compañia y comprensión.

Mi dedicación exclusiva al programa de Doctorado fue posible gracias a las Becas; de docencia de la Escuela de Graduados de la Universidad de Concepción y a las Becas de la Iniciativa Cientifica Milenio “Centro de Óptica e Información Cuántica” ICM N° P02-49-F y ICM N° P06-067-F. También, agradezco a las Becas MECESUP UCO-0209, CONICYT-PBCT, que me permitieron participar en congresos y realizar estadías en centros internacionales de investigación.

A todos los que han hecho posible la finalización de la tesis, les estoy realmente muy agradecido.

Resumen

En la tesis se estudia la discriminación de estados no ortogonales, junto con algunas de sus aplicaciones. Se propone un esquema experimental para la discriminación sin ambigüedad y la discriminación con mínimo error de cuatro estados puros que son simétricos. Mediante una modificación de los respectivos esquemas anteriores, es posible realizar la discriminación sin ambigüedad y la discriminación con mínimo error de dos operadores densidad llamados unitariamente equivalentes. El proceso de discriminación de los estados es probabilista y en los esquemas experimentales propuestos se obtiene la probabilidad óptima de discriminación para los estados considerados. También se propone un esquema para la distribución de claves criptográficas entre tres usuarios utilizando un estado maximalmente entrelazado como canal. Si el estado utilizado como canal cuántico está parcialmente entrelazado aún es posible realizar la distribución de la clave pero el protocolo es probabilista y debemos discriminar un conjunto de estados simétricos para finalizar el protocolo. Recientemente, se ha propuesto un nuevo conjunto de estados llamados igualmente separados, debido a que el producto interior entre los estados depende sólo de un parámetro α. Uno de los principales resultados de la tesis fue determinar la forma explícita de los estados igualmente separados en la base lógica. Además, se estudia la copia probabilista de un conjunto de n estados igualmente separados. Aquí, los estados se pueden copiar en forma determinista sólo si los estados son mutuamente ortogonales y en el caso de tener estados no ortogonales tenemos una probabilidad de copia que es menor que la unidad, lo cual está de acuerdo con el teorema de no copiado cuántico. Además, en el límite asintótico de infinitas copias, la probabilidad de copia de los estados es igual a la probabilidad de discriminar sin ambigüedad los estados igualmente separados.

Abstract

In this thesis, the discrimination of non-orthogonal states is studied, along with some of its applications. An experimental scheme is proposed for the unambiguous discrimination and for the minimum error discrimination of four pure symmetric states. A modification of the proposed schemes also allows us to discriminate without ambiguity and realize the minimum error discrimination of two unitary equivalent density matrices. The process of state discrimination is probabilistic. The experimental schemes achieve the maximal theoretical discrimination probability for the states considered. A theoretical scheme for quantum sharing of a cryptographic key among three users using a maximally entangled state as a channel is also proposed. If the state used as a quantum channel is partially entangled, it is still possible to distribute the key but the protocol is now probabilistic. This problem is overcome by resorting to the discrimination of a set of symmetric states. This process is a new stage in the key sharing scheme which supplement the usual protocol. Recently, a new set of states has been proposed, called equi-separated states, due to the fact that the inner product between two arbitrary states in this set depends only of a constant parameter. One of the main results of this thesis was to determine the explicit form of the equi-separated states in the logic base. Furthermore, the probabilistic cloning of a set of n equi-separated states is also studied. In this case, the states can be deterministically cloned only if the states are mutually orthogonal. In the case of non-orthogonal states, we have a cloning probability less than one, which is in agreement with the No Cloning Theorem. Moreover, in the asymptotic limit of infinite copies, the probability of state cloning is equal to the probability of unambiguous discrimination of equi-separated states.

Índice general

Índice de figuras

Capítulo 1

Introducción

Nuestra capacidad para transmitir y procesar la información esta limitada por las leyes que gobiernan los sistema físicos usados para tal propósito. En la Teoría Cuántica de la Información se utilizan sistemas cuánticos como portadores de la información. Esto permite que las propiedades que caracterizan a los sistemas cuánticos sean empleadas como un nuevo recurso, para realizar el procesamiento y transmisión de la información. Estas nuevas propiedades, tales como la superposición y el entrelazamiento de estados cuánticos, permiten realizar operaciones sobre los sistemas cuánticos que dan origen por ejemplo a: la teleportación de estados, la computación cuántica y la criptografía cuántica. Estas operaciones o procesos físicos tienen características que no son realizables por sistemas clásicos.

Actualmente, se utilizan protocolos de criptografía clásica para la distribución de la clave de encriptación y desencriptación de un mensaje. La seguridad en la distribución de la clave en la criptografía clásica se basa en la dificultad para resolver ciertos algoritmos matemáticos. Estos, sin embargo, no se ha demostrado que sean insolubles y por lo tanto, la criptografía clásica no provee de seguridad incondicional en la transmisión de un mensaje secreto. El principio de la criptografía cuántica consiste en la utilización de estados cuánticos no ortogonales. En este caso, la información (clave) que permite establecer una clave criptográfica es codificada en estados no ortogonales, los cuales no pueden ser identificados, copiados o divididos sin introducir perturbaciones detectables en el estado. El primer protocolo de distribución cuántica de claves fue propuesto por Bennett y Brassard en el año 1984, el cual es conocido como BB84. En el protocolo BB84 se utilizan estados bidimensionales y dos bases conjugadas para codificar el mensaje. En la criptografía cuántica tanto el receptor del estado cuántico como también un posible intruso en el canal de comunicación se enfrentan al problema de la identificación de estados. Sin embargo, el estado no es un observable en Mecánica Cuántica y por lo tanto, no podemos acceder directamente a la información codificada en el estado. Para lograr obtener la información es preciso determinar el estado cuántico. En el lenguaje de la Mecánica Cuántica, decimos que debemos determinar o discriminar el estado cuántico en el cual se encuentra el sistema.

Usualmente, la discriminación de estados cuánticos es introducida en el contexto de comunicaciones cuánticas. Un usuario dispone de un conjunto de estados cuánticos para transmitir información. De manera de acceder a esta información, el receptor procede a identificar los estados. Sin embargo, esto puede ser realizado deterministicamente sólo si el conjunto de estados

está compuesto por estados mutuamente ortogonales. En otro caso, la discriminación puede ser realizada con una cierta probabilidad de éxito. La optimización de la probabilidad de éxito se puede realizar por medio de dos estrategias distintas de discriminación, conocidas como discriminación con mínimo error y discriminación sin ambigüedad, esto es, sin error.

La estrategia óptima de discriminación con mínimo error de dos estados no ortogonales conduce al límite de Helstrom. En este caso, los estados siempre son discriminados pero no tenemos certeza y la medida tiene asociada una probabilidad de error. El límite de Helstrom determina la mínima probabilidad de error en el proceso de discriminación eligiendo apropiadamente los operadores de detección. Por otro lado, en la discriminación de estados sin ambigüedad, se impone la condición que los estados deben ser identificados con certeza, es decir, sin error. Esto es posible, a expensas de introducir un resultado inconclusivo, es decir que no permite discriminar sin error los estados. Al obtener un resultado inconclusivo, el proceso de discriminación falla y no obtenemos información del estado que está siendo discriminado. Sin embargo, si el proceso de discriminación tiene éxito hemos obtenido correctamente el estado en el cual fue preparado el sistema cuántico. La óptima discriminación sin ambigüedad para dos estados puros no ortogonales, denotados por $\{|\psi_+\rangle, |\psi_-\rangle\}$, con igual probabilidad de preparación, fue obtenida por Ivanovic-Dieks-Peres.

La posibilidad de utilizar un conjunto de más de dos estados no ortogonales permite por ejemplo mejorar el desempeño de los protocolos de criptografía cuántica. Por lo tanto, la discriminación de un número arbitrario de estados es uno de los problemas fundamentales en Teoría Cuántica de la Información. En este contexto, Chefles demostró que un requisito para la discriminación sin ambigüedad de un conjunto de N estados no ortogonales es que el conjunto de estados sean linealmente independientes. Si el conjunto de estados es simétrico es posible construir la estrategia para la discriminación sin error y también la estrategia sin ambigüedad. En particular, la probabilidad óptima de discriminar sin ambigüedad N estados simétricos fue encontrada por Chefles y Barnett. La discriminación sin ambigüedad de estados no ortogonales ha sido aplicada en la concentración del entrelazamiento, la teleportación cuántica de qudits, intercambio de entrelazamiento de qudits y en la codificación densa de la información.

1.1. Alcance y Organización de la Tesis

1.1.1. Discriminación de Estados Simétricos

Una etapa fundamental en los protocolos de comunicaciones cuánticas es la discriminación de estados. Bajo ciertas condiciones los estados no ortogonales a ser discriminados forman un conjunto de estados simétricos linealmente independientes. La discriminación conclusiva de esta clase de estados permite la teleportación de estados cuánticos desconocidos con fidelidad unitaria y con cierta probabilidad de éxito. Un resultado similar se obtiene en los casos del intercambio del entrelazamiento y de la codificación densa. Es por este motivo importante investigar la implementación experimental de los esquemas de discriminación óptimos, dado que permiten mejorar la capacidad de los protocolos de comunicación cuántica. En esta Tesis, proponemos un esquema experimental para discriminar estados simétricos no ortogonales linealmente independientes con una probabilidad óptima de discriminación. El esquema experimental utiliza óptica lineal y considera los procesos requeridos para generar, propagar y discriminar los estados. El esquema se puede configurar para implementar la discriminación sin ambigüedad y además, la discriminación con mínimo error de estados simétricos. Mediante una modificación del esquema experimental es posible discriminar con mínimo error y sin ambigüedad, dos estados mixtos no ortogonales construidos desde los estados simétricos utilizados.

1.1.2. Distribución de Estados Cuánticos

La criptografía cuántica provee de una forma segura para transmitir información entre dos o más usuarios. Los protocolos de criptografía cuántica son diseñados de manera que cualquier intruso en el canal de comunicación deje una marca en la llave usada para codificar la información clásica. Por medio de esto, es posible decidir si una llave puede ser usada en forma segura o se debe generar una nueva. La criptografía cuántica ha sido extendida al caso de distribución de secretos cuánticos. Esta generalización se origina cuando examinamos la versión clásica del problema de distribución de secretos, esto es, la distribución de información sensible entre muchas partes de manera que una parte deshonesta no puede tener acceso a la información completa. En el caso cuántico, el secreto a ser distribuido puede ser una clave clásica o un estado cuántico. En el capítulo 6 se analizó la distribución de estados cuánticos de dimensión d entre tres usuarios y caracterizamos el conjunto de estados maximalmente entrelazados que pueden ser usados como canal cuántico en el protocolo. También, se considera el uso de un canal no ideal, es decir, estados que están parcialmente entrelazados. En este caso, relacionamos los protocolos para distribuir un qudit con el problema de la discriminación de estados. Esto permite la formulación de un protocolo, donde la recuperación del estado se logra con una cierta probabilidad.

1.1.3. Copia Probabilista de Estados Cuánticos

La imposibilidad de copiar estados cuánticos no ortogonales desconocidos en forma perfecta y de manera determinista es una de las principales características de los sistemas físicos con propiedades cuánticas. Este resultado conocido como “no-cloning theorem” fue demostrado por Wooters y Zurek. Establece que debido a la linealidad de las operaciones cuánticas no es posible

duplicar un estado cuántico $|\psi\rangle$ arbitrario desconocido que pertenece a un conjunto de estados mutuamente no ortogonales. Sin embargo, no está prohibida la posibilidad de una copia imperfecta, es decir con una fidelidad menor que la unidad o bien con una fidelidad igual a la unidad pero es este caso la probabilidad del proceso es menor que la unidad. En el capítulo 7 de la Tesis se estudia una máquina de copiado probabilista que genera M copias de un estado que pertenece a un conjunto de n estados igualmente separados. Estos estados son puros, con igual probabilidad de preparación $1/n$, linealmente independientes y tienen la propiedad que el producto interior entre dos estados es un único número complejo α. Se determinó la forma explícita de los estados igualmente separados en la base lógica y la transformación unitaria que conecta los estados. En cuanto a la copia probabilista de estados, se analiza el efecto que posee la fase de α en la probabilidad de éxito en el proceso de copia de los estados igualmente separados.

1.1.4. Organización de la Tesis

En esta tesis se estudia la discriminación óptima de estados cuánticos que son no ortogonales y algunas de sus posibles aplicaciones. Esta tesis se organiza de la siguiente manera: En el Capítulo 2 se describe brevemente la teoría de la información clásica. En el Capítulo 3 se expone los principios de la Mecánica Cuántica y algunos de sus resultados más importantes. El Capítulo 4 trata sobre la discriminación de estados cuánticos, aquí se detallan las características y principales resultados sobre la discriminación sin error y la discriminación con mínimo error. En el Capítulo 5 se propone un esquema experimental para la discriminación de estados simétricos no ortogonales. La propuesta experimental es para estados puros y para dos estados mixtos, tanto para la discriminación sin ambigüedad y la discriminación sin error. En el Capítulo 6 se propone un protocolo para la distribución de estados cuánticos. Aquí, se emplea estados cuánticos maximalmente entrelazados como recurso para realizar el protocolo de distribución de estados. Si inicialmente se tiene un estado parcialmente entrelazado, aún es posible realizar el protocolo pero con cierta probabilidad. En el Capítulo 7 trata sobre la caracterización del conjunto de estados cuánticos denominados igualmente separados y la copia en forma probabilista de este tipo de estados. En este caso, hay una conección entre la copia probabilista y la discriminación sin ambigüedad de los estados. Finalmente, las conclusiones se exponen en el Capítulo 8, donde se resumen los resultados de la tesis.

Capítulo 2

Teoría Clásica de la Información

La Teoría Clásica de la Información consiste en la cuantificación de los recursos físicos necesarios para procesar, transmitir y almacenar la información clásica. Para ello se estudia los símbolos utilizados en la comunicación y el soporte o los medios de comunicación. Los símbolos con los cuales un emisor codifica un mensaje contienen una cierta cantidad de información a la que puede acceder un receptor al decodificar el mensaje. Al intercambio de información se le conoce con el nombre de comunicación. De esta manera, por ejemplo un lenguage común facilita la transmisión de información dado que la comunicación se hace más eficiente. Por otro lado, el soporte de comunicación permite conectar a dos o más usuarios a través de un canal de comunicación.

El elemento básico para procesar, almacenar y transmitir información clásica es el bit (dígito binario), que corresponde a un sistema clásico con sólo dos posibles valores, 0 ó 1. Cada bit puede ser físicamente representado o almacenado por ejemplo, mediante el estado de carga de un capacitor (0=descargado, 1=cargado). Estos constituyen dos estados macroscópicos distinguibles y son estables ante el ruido. La información no sólo es almacenada, también puede ser transmitida (comunicación) y procesada (computación). Para ello es posible utilizar n bits con lo cual tenemos acceso a 2^n valores o símbolos diferentes. Por ejemplo, con dos bit es posible generar los cuatro números siguientes, $0 = 00$, $1 = 01$, $2 = 10$, y $3 = 11$. De esta manera, es posible representar cualquier alfabeto o conjunto de símbolos por medio de bits.

La Teoría Clásica de la Información tiene origen en los trabajos realizados por C. Shannon [1, 2]. En los cuales, da respuesta a la siguiente pregunta: ¿Cuál es la cantidad mínima de recursos físicos, requeridos para almacenar la información producida por una fuente, de manera que posteriormente la información sea reconstruida por el receptor?. El concepto clave, en la teoría de la información clásica, resulta ser la entropía de Shannon.

2.1. Teoremas de Shannon

2.1.1. Primer Teorema de Shannon

La información $I(x_i)$ medida en bits [3], que aporta un determinado valor x_i, de una variable aleatoria $X = \{x_1, x_2, ..., x_n\}$ que posee un conjunto de n símbolos que permiten codificar un

mensaje, y que tiene una distribución de probabilidad $p_1, p_2, ..., p_n$, de aparición respectivamente, es definida por

$$I(x_i) = log_2 \frac{1}{p_i}. \tag{2.1}$$

La entropía de Shannon $H(X)$ cuantifica la cantidad de información obtenida en promedio cuando conocemos el valor de la variable aleatoria X, y es definida por

$$H(X) = -\sum_{i=1}^{n} p_i log_2 p_i. \tag{2.2}$$

Una interpretación alternativa, es que la entropía de Shannon $H(X)$ cuantifica la cantidad de incertidumbre de la variable X, antes de conocer su valor [4]. Por ejemplo, si consideramos el lanzamiento de una moneda, donde los dos posibles resultados son aleatorios, con probabilidad 1/2 de ocurrir. Entonces, la entropía de Shannon es igual a 1 y, por lo tanto, nuestra incerteza inicial es completa, dado que no tenemos información sobre cual será el resultado del lanzamiento de la moneda. Sin embargo, si el lanzamiento de la moneda no es del todo aleatorio, es decir, si lanzamos la moneda de manera que siempre aparece sólo una de las alternativas. Entonces, la entropía de Shannon es igual a cero, y nuestra información es completa, dado que ahora tenemos certeza sobre el resultado del lanzamiento.

La entropía de un alfabeto X (2.2) puede ser utilizada para determinar el número medio óptimo de bit necesarios para representar un símbolo de ese alfabeto. Por ejemplo, si enviamos información en uno de los cuatro símbolos, 1, 2, 3 ó 4. Sin compresión de la información, se requieren dos bits para almacenar los correspondientes cuatro posibles valores. Sin embargo, si la fuente genera los símbolos 1, 2, 3 y 4, con una distribución de probabilidad igual a $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}$ y $\frac{1}{8}$ respectivamente, es posible un esquema de compresión de la información. Una codificación óptima de los símbolos 1, 2, 3 y 4, está asociada con la siguiente secuencia de bit 0,10,110,111, respectivamente, y por lo tanto, el largo medio de la cadena de bit comprimida es $\frac{1}{2}1 + \frac{1}{4}2 + \frac{1}{8}3 + \frac{1}{8}3 = \frac{7}{4}$ bits de información al usar el canal de comunicación [4]. Por otro lado, la entropía de Shannon es $H(X) = -\frac{1}{2}log_2\frac{1}{2} - \frac{1}{4}log_2\frac{1}{4} - \frac{1}{8}log_2\frac{1}{8} - \frac{1}{8}log_2\frac{1}{8} = \frac{7}{4}$, por cuanto, la entropía cuantifica la óptima compresión que puede ser realizada. La entropía de Shannon (2.2) es el resultado conocido como teorema de codificación de un canal sin ruido.

2.1.2. Segundo Teorema de Shannon

Si el canal de transmisión de la información no es perfecto, se producirán errores en algunos bits, producto del ruido inherente del canal clásico y parte de la información se perderá. Para asegurar que el mensaje enviado sea reproducido por el receptor, utilizamos la redundancia de la información. Esto se realiza, codificando cada símbolo con más bits de los estrictamente necesarios, de manera que los errores puedan ser fácilmente detectados y corregidos. El costo de la redundancia de la información es que se requieren más bits, con lo cual la transmisión de la información se vuelve más lenta. El segundo teorema de Shannon [2], sobre la codificación de un canal que posee ruido, cuantifica la mínima redundancia posible que permite la transmisión fidedigna de la información. Para ello, es preciso primero definir el concepto de canal de informacion.

Definición: Canal de Información
Un canal de información[1] es determinado por un alfabeto de entrada $A = \{a_i\}$, con $i = 1, 2, ..., r$; un alfabeto de salida $B = \{b_j\}$, $j = 1, 2, ..., s$; y un conjunto de probabilidades condicionales $P(b_j|a_i)$. Donde, $P(b_j|a_i)$ es la probabilidad de recibir a la salida el símbolo b_j cuando se envía el símbolo de entrada a_i [3].

En particular, un canal de gran importancia teórica es el canal binario simétrico. Este canal posee dos símbolos de entrada ($a_1 = 0, a_2 = 1$) y dos símbolos de salida ($b_1 = 0, b_2 = 1$). Es simétrico dado que la probabilidad de error p es la misma al recibir un 0 o un 1 y por lo tanto, la probabilidad de recibir los símbolos 0 ó 1 sin error es igual a $1 - p$.

La elección del símbolo de entrada a_i, tiene asociada una probabilidad $P(a_i)$. Sin embargo, si el símbolo de salida es b_j, la probabilidad de que el símbolo de entrada correspondiente sea a_i es $P(a_i|b_j)$. Esta probabilidad condicional se determina, utilizando la ley de Bayes, por medio de la siguiente expresión

$$P(a_i|b_j) = \frac{P(b_j|a_i)P(a_i)}{P(b_j)}, \tag{2.3}$$

donde la probabilidad $P(b_j)$ es dada por

$$P(b_j) = \sum_{i=1}^{r} P(b_j|a_i)P(a_i). \tag{2.4}$$

La probabilidad que el símbolo de entrada sea a_i y el símbolo de salida sea b_j, se denomina probabilidad conjunta. Es denotada por $P(a_i, b_j)$ y es simétrica al intercambio de a_i por b_j. Esta probabilidad se calcula por medio de la siguiente expresión

$$P(a_i, b_j) = P(b_j|a_i)P(a_i) = P(a_i|b_j)P(b_j). \tag{2.5}$$

Ahora, se determina el cambio que sufre el valor de la probabilidad de los distintos símbolos de entrada, por el hecho de recibir a la salida el símbolo b_j. Se denomina $P(a_i)$ la probabilidad a priori de los símbolos de entrada, es decir, antes de recibir un símbolo de salida determinado. La probabilidad a posteriori $P(a_i|b_j)$, es la probabilidad después de la recepción de b_j. Luego, la entropía a priori de A es

$$H(A) = -\sum_{i=1}^{r} P(a_i) log_2 P(a_i), \tag{2.6}$$

y la entropía a posteriori de A, recibido b_j es

$$H(A|b_j) = -\sum_{i=1}^{r} P(a_i|b_j) log_2 P(a_i|b_j). \tag{2.7}$$

La interpretación de estas dos relaciones se realiza basándose en el primer teorema de Shannon. $H(A)$ es el número medio de bits necesarios para representar un símbolo de una fuente con una

[1] El canal definido de esta forma se denomina, canal de información sin memoria. En general, la probabilidad de una salida dada b_j puede depender de varios símbolos precedentes e incluso de los símbolos de salida. Los cuales, se conocen como canales con memoria.

probabilidad a priori $P(a_i)$, $i = 1, 2, ..., r$; $H(A|b_j)$ representa el número medio de bits necesarios para representar un símbolo de la fuente con una probabilidad a posteriori $P(a_i|b_j)$, $i = 1, 2, ..., r$. El valor medio de las entropías a posteriori, denotada por $H(A|B)$ es

$$H(A|B) = \sum_{j=1}^{s} P(b_j)H(A|b_j), \tag{2.8}$$

y recibe el nombre de equivocación de A con respecto a B, o equivocación del canal. La equivocación del canal en función de las probabilidades conjuntas y condicionales es

$$H(A|B) = -\sum_{A,B} P(a,b)log_2P(a|b). \tag{2.9}$$

Cabe destacar que los sucesivos símbolos de entrada a_i se codifican empleando códigos distintos para cada símbolo de salida b_j. Sin embargo, no es suficiente seleccionar un conjunto de códigos unívocos cuyas palabras tengan longitudes que satisfagan la relación (2.9), se requiere también, que los códigos sean instantáneos [3].

2.2. Información Mutua

El segundo teorema de Shannon es sobre la codificación de la información en un canal con ruido. Establece que aunque un canal ruidoso interfiere con la comunicación, es posible establecer una comunicación libre de error. La máxima tasa de transferencia de información del canal, para un cierto nivel de ruido se denomina capacidad.

La diferencia entre entropía a priori de A y la equivocación el canal, proporcionan en promedio $H(A) - H(A|B)$ bits de información por la observación de un símbolo de salida. Esta diferencia se denomina información mutua de A y B, o información mutua del canal, que se escribe

$$I(A;B) = H(A) - H(A|B). \tag{2.10}$$

Es posible expresar la información mutua de la forma,

$$I(A;B) = \sum_{A,B} P(a,b)log_2\frac{P(a,b)}{P(a)P(b)}, \tag{2.11}$$

por lo tanto, la información media recibida por un canal ha de ser siempre positiva [3]. Además, la condición para que la información mutua sea nula es que los símbolos de entrada y salida sean estadísticamente independientes, es decir

$$P(a_i, b_j) = P(a_i)P(b_j), \tag{2.12}$$

para cualquier i, j. Una propiedad importante de la información mutua $I(A;B)$, es que es simétrica respecto de las variables a_i y b_j, y por lo tanto,

$$I(A;B) = I(B;A), \tag{2.13}$$

lo que pone de manifiesto la reciprocidad de la información mutua. Finalmente, para cada canal sin memoria discreto, la capacidad del canal es

$$C = sup_{pa} I(A; B), \tag{2.14}$$

donde, *sup* representa la máxima información mutua para la distribución de probabilidad $Pa = p(a_i)$ del alfabeto A.

2.3. Criptografía Clásica

La criptografía clásica tiene como objetivo establecer un canal de comunicación secreto. En el esquema criptográfico más sencillo, un emisor desea transmitir un mensaje secreto a un receptor sin que sea interceptado por un agente externo. Actualmente, con el uso habitual de las comunicaciones electrónicas, se requiere de técnicas que permitan almacenar y transmitir datos en forma segura.

En 1917 G. Vernam propuso un sistema criptográfico inquebrantable llamado "cifrado Vernam", también conocido como "One-time pad". Su seguridad en el cifrado, contra adversarios con ilimitados recursos tecnológicos y computacionales, fue provado por C. Shannon en términos de la teoría clásica de la información en 1949 [2].

El cifrado de Vernam es un caso especial de cifrado por sustitución, y es un tipo de cifrado simétrico de claves secretas. El cifrado simétrico requiere el uso de la misma clave para encriptar y desencriptar el mensaje. El principio del cifrado está en que, si se agrega al mensaje una clave aleatoria, la cadena de bits resultante también es aleatoria y, por lo tanto, no contiene información del mensaje. Si usamos la lógica binaria, en vez de Vernam que trabajo con las 26 letras del alfabeto, el algoritmo de encriptación E puede ser escrito como [5]

$$E_K(M) = (M_1 + K_1, M_2 + K_2, ..., M_n + K_n) \text{mod } 2, \tag{2.15}$$

donde $M = (M_1, M_2, ..., M_n)$ es el mensaje del emisor a ser encriptado y la clave es $K = (K_1, K_2, ..., K_n)$ compuesta por bits aleatorios. El mensaje y la clave son sumadas en forma binaria, es decir, modulo 2. La desencriptación D del texto cifrado $C = E_K(M)$ es idéntica a la encriptación, ya que la doble adición modulo 2 resulta ser igual a la idéntidad, por lo tanto

$$M = D_K(C) = (C_1 + K_1, C_2 + K_2, ..., C_n + K_n) \text{mod } 2. \tag{2.16}$$

Las condiciones que debe cumplir la clave para que el cifrado sea incondicionalmente seguro, probado por C. Shannon [2], son:

(1) La clave debe ser del mismo largo que el mensaje.
(2) Debe ser generada aleatoriamente.
(3) Puede ser usada sólo una vez, motivo del nombre "One-time pad".

El emisor y el receptor en este esquema requieren conocer en forma previa a la comunicación la clave que se empleará para codificar y decodificar el mensaje. Por esta razón, el cifrado de Vernam es utilizado sólo en ciertos casos donde se requiere altos niveles de confiabilidad. En

aplicaciones más cotidianas, si el emisor y el receptor no conocen la clave, surge la interrogante, ¿como distribuir la clave en forma segura?. La seguridad del mensaje, de este modo se reduce a la seguridad en la distribución de la clave.

La solución al problema de la distribución de la clave, fue encontrada por W. Diffie y M. Hellman [6] al inventar la "criptografía de llave pública" en 1976. Este es un tipo de cifrado asimétrico, la clave para codificar el mensaje es distinta de la clave para decodificar el mensaje. Un usuario tiene dos claves criptográficas, una pública y otra privada. La clave privada se mantiene en secreto, mientras que la clave pública es ampliamente conocida.

La seguridad de la criptografía de clave pública se basa en varios problemas computacionales, los cuales son dificiles de resolver. De manera que un adversario puede acceder a la clave, si logra resolver el respectivo algoritmo. Los algoritmos de encriptación y desencriptación utilizan las llamadas funciones de una dirección. Las funciones de una dirección son funciones matemáticas fáciles de cálcular en una dirección, pero su inversión es muy difícil[2]. Estos algoritmos pueden ser; descomposición de números primos, factorización de números enteros o resolución de ecuaciones logarítmicas. Por ejemplo, es fácil multiplicar dos números primos, pero factorizar el producto de dos números primos grandes es una tarea difícil.

Sin embargo, la criptografía de clave pública no provee de seguridad incondicional en la transmisión de un mensaje secreto. Actualmente, se utiliza un sistema de criptografía de clave pública conocido como RSA. El sistema criptográfico RSA fue inventado en 1977 por R. Rivest, A. Shamir y L. Adleman [7], y emplea la dificultad para factorizar números grandes. Las claves RSA utilizan actualmente entre 1024-2048 bits de longitud [8], pero se cree que pronto estas claves serán vulnerables. Esto se debe a que los permanentes avances en los algoritmos de desencriptación y en las capacidades computacionales, permiten reducir los tiempos de cálculo de los algoritmos.

2.4. Computación Clásica

La noción abstracta de un computador programable fue desarrollada por Alan Turing en 1936 [9] y el esquema de computación propuesto se conoce como máquina de Turing [4]. Una máquina de Turing consiste de una cinta de longitud infinita y una cabeza de lectura de la cinta (cabezal). La cinta está dividida en espacios cuyos posibles estados son descritos por símbolos de un alfabeto finito $\Sigma_{cinta} = \{t_i\}$. El cabezal de la cinta tiene estados internos representados por un alfabeto finito $\Sigma_{cabezal} = \{h_i\}$. El cabezal puede determinar el estado de un espacio particular de la cinta y modificarlo de acuerdo a las siguientes reglas de operación,

(1) Cambiar el símbolo del espacio de la cinta por otro símbolo en Σ_{cinta}.
(2) Mover un espacio de la cinta hacia atrás o adelante y
(3) Cambiar su estado por otro símbolo en $\Sigma_{cabezal}$.

[2]Difícil significa que el número de operaciones elementales requeridas para resolver el problema matemático crece exponencialmente con el número de bits de la clave.

La relación entre los símbolos Σ_{cinta}, $\Sigma_{cabezal}$ y el movimiento de la cinta son denotadas por d y la máquina de Turing por M_d. Un particular computo sobre la máquina de Turing consiste en suministrar a la máquina con un valor de entrada t, que corresponden a símbolos en la Σ_{cinta} de largo n. Posteriormente, la máquina preparada en un estado inicial t_{ini}, procesa la entrada t de acuerdo a las reglas (1), (2) y (3) hasta que se detiene en el estado final h_{fin}. El conjunto de valores (h, t, p) con $h \in \Sigma_{cabezal}$, $t \in \Sigma_{cinta}$, y p la posición de la cinta, es llamado una configuración de la máquina de Turing y d es la función de transición la cual relaciona dos configuraciones consecutivas. Una función f dada es computable en la máquina de Turing si esta eventualmente se detiene para todos los posibles caracteres de entrada t de largo finito. Uno de los resultados de Turing fue mostrar la existencia de una máquina universal de Turing U. Esto es, una máquina de Turing que puede emular cualquier otra máquina de Turing M_d cuando los caracteres de entrada también contienen el conjunto de relaciones d la cuales especifican M, es decir

$$U(d, t) = M_d(t) \ \forall \ d, t, \tag{2.17}$$

donde el número de operaciones básicas de U necesarias para simular una operación de M_d es sólo una función polinómica de d. Por lo tanto, cualquier proceso algoritmico puede ser eficientemente simulado usando una máquina de Turing, esta afirmación es conocida como tesis Church-Turing [10].

Una máquina de Turing probabilista es una máquina de Turing cuyas funciones de transición asignan una probabilidad a cualquier posible par configuraciones consecutivas. Esta transición de probabilidad obedece la condición de normalización, por cuanto la suma de todas las probabilidades de transición para una configuración inicial dada debe ser igual a la unidad [11].

Capítulo 3

Teoría Cuántica de la Información

En la Teoría Cuántica de la Información se utilizan sistemas cuánticos como portadores de la información clásica. Esto permite que las propiedades que caracterizan a los sistemas cuánticos sean empleadas como un nuevo recurso, para realizar el procesamiento y transmisión de la información. Estas nuevas propiedades, tales como la superposición y el entrelazamiento de estados cuánticos, permiten realizar operaciones sobre los sistemas cuánticos que dan origen por ejemplo a: la teleportación de estados cuánticos, la computación cuántica y la criptografía cuántica.

En Teoría Clásica de la Información el elemento básico para codificar la información es el bit. Para generalizar el bit clásico al caso cuántico, asociamos los estados ortogonales $\{|0\rangle, |1\rangle\}$ de un sistema cuántico bidimensional con los dos valores que puede asumir el bit clásico $\{0, 1\}$, respectivamente. Como una extensión del caso clásico, el sistema cuántico puede estar en una superposición de los dos estados base. Esta superposición de estados es conocida como bit cuántico ("quantum bit"), o bien como "qubit"[12]. El estado más general de un qubit aislado puede ser representado de la siguiente forma

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle, \tag{3.1}$$

donde los números reales θ y φ definen un punto sobre una esfera unitaria tridimensional, conocida como esfera de Bloch. Si el estado cuántico está compuesto por una superposición de d estados de la forma

$$|\psi\rangle = \sum_{k=0}^{d-1} c_k |k\rangle, \tag{3.2}$$

entonces se denomina "qudit", el cual es una generalización del "qubit".

La posibilidad de representar la información por medio de sistemas cuánticos da origen a que por ejemplo, no sea posible copiar un estado cuántico desconocido. Otra propiedad de los sistemas cuánticos empleada en la Teoría Cuántica de la Información es el entrelazamiento. El entrelazamiento es ampliamente utilizado en la teoría cuántica de la información, ya que permite realizar las siguientes aplicaciones: teleportación de estados, codificación densa de la información, intercambio del entrelazamiento y criptografía cuántica. Todas estas nuevas propiedades y aplicaciones se pueden describir con el formalismo de la Mecánica Cuántica. En este capítulo se exponen los axiomas y el formalismo de la Mecánica Cuántica para describir las propiedades de

los sistemas cuánticos. Además, se expone como el formalismo de la Mecánica Cuántica permite describir sus aplicaciones más importantes.

3.1. Axiomas de la Mecánica Cuántica

La teoría cuántica es un modelo matemático que, junto con conceptos físicos, nos permite describir los fenómenos físicos a escala microscópica. Para caracterizar el comportamiento de los sistemas cuánticos se requiere conocer: el estado, la evolución del estado y las mediciones realizadas sobre el sistema cuántico. Estos conceptos toman forma con los cuatro postulados de la Mecánica Cuántica [4], que se detallan a continuación.

- **Postulado 1:** Estado del sistema

Asociado a cada sistema cuántico aislado se tiene un espacio de Hilbert conocido como el espacio de estados del sistema. Todas las predicciones posibles del sistema cuántico son descritas por un vector unitario $|\psi\rangle$, llamado el vector de estado, en el espacio de estados del sistema.

Un espacio de Hilbert $\mathcal{H}$ es un espacio vectorial sobre el campo de los complejos $\mathcal{C}$, el cual está dotado de una norma $\|\psi\|$ que proviene de un producto interior. El producto interior, entre dos estados $|\psi\rangle \in \mathcal{H}$ y $|\phi\rangle \in \mathcal{H}$ es un mapeo de vectores a números complejos, el cual es denotado por $\langle\psi|\phi\rangle$ y posee las siguientes propiedades:

(a) Linealidad: $\langle\psi|\left(a\,|\phi_1\rangle + b\,|\phi_2\rangle\right) = a\,\langle\psi|\phi_1\rangle + b\,\langle\psi|\phi_2\rangle$.
(b) Simetría: $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$, donde $*$ denota el complejo conjugado.
(c) Positividad: $\langle\psi|\psi\rangle \geq 0$, la igualdad se tiene para el vector nulo $|\psi\rangle = 0$.

Además, el espacio de Hilbert es completo en la norma $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$, lo que en el caso de espacios de dimensión infinita asegura la convergencia de las expanciones en funciones propias. Esto nos garantiza que sea posible expandir los estados en términos de una base ortonormal de estados. Esto también es válido para espacios de Hilbert de dimensión finita. Por ejemplo, en un espacio de Hilbert bidimensional, el estado del sistema se puede expandir en términos de la base ortonormal $\{|0\rangle, |1\rangle\}$. Por lo tanto, el estado del sistema es una combinación lineal de estados, conocida como superposición de estados,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{3.3}$$

Si la norma de los estados es $\|\,|\psi\rangle\,\| = 1$, los coeficientes α y β cumplen con la condición de normalización, $|\alpha|^2 + |\beta|^2 = 1$. Esto permite interpretar a los coeficientes α y β, como las amplitudes de probabilidad y a $|\alpha|^2$, $|\beta|^2$ como las probabilidades de encontrar al sistema en el estado $|0\rangle$, $|1\rangle$, respectivamente. Si los estados no están normalizados, es conveniente normalizarlos dividiendo por su norma, $|\psi\rangle \,/\, \|\,|\psi\rangle\,\|$, de manera de asegurar que las probabilidades, de los posibles resultados de las mediciones, sumadas sean iguales a la unidad.

Los estados $|\psi\rangle$ y $e^{i\varphi}\,|\psi\rangle$ describen el mismo estado físico, ya que la fase $e^{i\varphi}$ no tiene efectos observables. Sin embargo, la fase relativa en la superposición es fisicamente importante, los estados $\alpha\,|0\rangle + \beta\,|1\rangle$ y $e^{i\varphi}(\alpha\,|0\rangle + \beta\,|1\rangle)$ son equivalentes, pero diferentes al estado $\alpha\,|0\rangle + e^{i\varphi}\beta\,|1\rangle$.

- **Postulado 2:** Evolución del estado

La evolución del estado de un sistema cuántico, describe los cambios que se producen en el estado con el tiempo. En particular, la evolución de un sistema cuántico aislado que no interactúa con otro sistema, que relaciona el estado inicial $|\psi\rangle$ en el instante t_1 y estado final $|\psi'\rangle$ en el instante t_2, es descrita por una transformación unitaria U que depende sólo de los tiempos t_1 y t_2

$$\left|\psi'\right\rangle = U\left|\psi\right\rangle. \tag{3.4}$$

La transformación unitaria U es generada por un operador hermítico llamado Hamiltoniano H. La dinámica temporal del vector de estado del sistema, cuando el Hamiltoniano es independiente del tiempo, es gobernada por la ecuación de Schrödinger

$$i\hbar\frac{d}{dt}\left|\psi\right\rangle = H\left|\psi\right\rangle, \tag{3.5}$$

donde, $\hbar$ es la constante de Planck. De manera que, si conocemos el Hamiltoniano del sistema, es posible en principio, determinar completamente el estado en función del tiempo. El Hamiltoniano es un operador hermítico que tiene una descomposición espectral de la forma,

$$H = \sum_E E\left|E\right\rangle\left\langle E\right|, \tag{3.6}$$

con autovalores E, y con los correspondientes autovectores normalizados $|E\rangle$. Los estados $|E\rangle$ son conocidos como los autovalores de energía y E es la energía del estado $|E\rangle$. El estado de más baja energía es conocido como el estado base y su energía asociada, se denomina energía del estado base.

La transformación unitaria U de la ecuación (3.4), está relacionada con el Hamiltoniano H del sistema por medio de la siguiente expresión,

$$U(t_1, t_2) = exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]. \tag{3.7}$$

- **Postulado 3:** Mediciones cuánticas

Una medición es descrita por un conjunto de operadores de medida $\{M_m\}$. Estos operadores actúan en el espacio Hilbert del sistema. El subíndice m nos indica el resultado de la medición que ocurre en el experimento. Si el estado del sistema inmediatamente antes de la medida es $|\psi\rangle$ entonces, la probabilidad de obtener el resultado m es

$$p(m) = \left\langle\psi\right| M_m^\dagger M_m\left|\psi\right\rangle, \tag{3.8}$$

y el estado inmediatamente después de la medida es

$$\frac{M_m\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m\left|\psi\right\rangle}}. \tag{3.9}$$

Los operadores de medida satisfacen la condición de completitud,

$$\sum_m M_m^\dagger M_m = \mathbf{1}. \tag{3.10}$$

La condición de completitud expresa el hecho que las probabilidades deben sumar uno,

$$1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle . \tag{3.11}$$

- **Postulado 4:** Sistemas compuestos

El espacio de Hilbert de un sistema cuántico compuesto[1], es el producto tensorial de los espacios de Hilbert de las componentes del sistema cuántico. Es decir, si tenemos numerados los sistemas desde 1 hasta n, y el sistema número i está preparado en el estado $|\psi_i\rangle$, entonces el estado conjunto del sistema total es $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$.

La Teoría Cuántica es por construcción probabilística, lo que se pone de manifiesto con la aleatoriedad del resultado obtenido en la medida de un observable. Sin embargo, la ecuación de Schrödinger nos entrega una descripción determinista de la evolución del estado. Por lo tanto, tenemos una evolución unitaria del estado en función del tiempo la cual es interrumpida al realizar una medida del estado. Luego de la cual, el estado del sistema nuevamente evoluciona con una transformación unitaria. Además, en Mecánica Cuántica no se puede medir simultáneamente dos observables incompatibles, lo cual es conocido como el principio de incertidumbre de W. Heisenberg [13]. Dos observables A y B que no conmutan, es decir $AB \neq BA$, se denominan observables incompatibles. Por ejemplo, la posición y el momentum de una partícula en Mecánica Cuántica son observables incompatibles. Esto contrasta con la Mecánica Clásica, donde es posible medir simultáneamente y en forma determinista, la posición y el momentum de una partícula.

3.2. Ensamble de Estados y Operador Densidad

En la sección anterior hemos considerado que el estado del sistema cuántico se describe por medio de un estado $|\psi\rangle$ en un espacio de Hilbert. En general, el estado inicial del sistema cuántico no es un estado puro $|\psi\rangle$. Sin embargo, se asume que el sistema está en uno de los estados $|\psi_i\rangle$ del conjunto de estados $\{|\psi_i\rangle\}$, con una probabilidad p_i, respectivamente. Por lo tanto, nuestro conocimiento del sistema cuántico es descrito por un ensamble de estados puros, $\{|\psi_i\rangle, p_i\}$. Si el ensamble del sistema está compuesto de sólo un estado, entonces el estado es puro. En otro caso, tenemos un estado mixto, es decir, una mezcla de estados puros. Para describir un estado mixto, usamos un operador en vez de un vector estado. Este operador se denomina operador densidad, que es denotado por ρ, y tiene la siguiente forma

$$\rho = \sum_i^n p_i |\psi_i\rangle \langle\psi_i| . \tag{3.12}$$

El operador densidad, también denoninado como matriz densidad, posee las siguientes propiedades,

(a) Condición de normalización, $Tr(\rho) = 1$, es decir, la suma de los elementos diagonales son iguales a uno.
(b) Es semidefinida positiva, es decir $\langle\varphi| \rho |\varphi\rangle \geq 0$, para cualquier vector $|\varphi\rangle$ en el espacio de

[1] Un sistema es compuesto si utilizamos una partícula con a lo menos dos grados de libertad, o bien dos o más partículas.

estados.

Si se cumplen las dos condiciones anteriores, el operador densidad tiene una descomposición espectral, de la forma

$$\rho = \sum_j \lambda_j \left|j\right\rangle \left\langle j\right|, \tag{3.13}$$

donde los vectores $|j\rangle$ son mutuamente ortogonales y los valores propios de ρ, denotados por λ_j son reales no negativos. En general, $Tr(\rho^2) \leq 1$, la igualdad se tiene sólo para estados puros. Además, el operador densidad es hermítico, es decir $\rho = \rho^\dagger$ y sus términos matriciales fuera de la diagonal son llamados términos de coherencia, $\rho_{nm} = \langle n| \rho |m\rangle$ y sus términos diagonales $\rho_{nn} = \langle n| \rho |n\rangle$ son llamados poblaciones. Los términos de coherencia y las poblaciones, cumplen con la desigualdad triangular, es decir, $\langle n| \rho |n\rangle \langle m| \rho |m\rangle \geq |\langle n| \rho |m\rangle|^2$.

Ahora, los postulados de la Mecánica Cuántica en términos del operador densidad quedan de la siguiente forma:

- **Postulado 1:** Estado del sistema

Asociado a cada sistema cuántico se tiene un espacio de Hilbert conocido como el espacio de estado del sistema. El sistema es completamente descrito por su operador densidad, el cual es un operador positivo con traza igual a uno, actuando sobre el espacio de estado del sistema. Si el sistema cuántico está en el estado ρ_i, con probabilidad p_i, entonces el operador densidad para el sistema es $\sum_i p_i \rho_i$.

- **Postulado 2:** Evolución del estado

La evolución de un sistema cuántico cerrado es descrita por una transformación unitaria U. Esto implica, que el estado inicial ρ en el instante t_1 y estado final ρ' en el instante t_2, están relacionados a través del operador unitario U que depende sólo de los tiempos t_1 y t_2,

$$\rho' = U \rho U^\dagger. \tag{3.14}$$

- **Postulado 3:** Mediciones cuánticas

Una medición es descrita por un conjunto de operadores de medida $\{M_m\}$. Estos operadores actúan en el espacio de Hilbert del sistema. El subíndice m nos indica el resultado de la medición que ocurre en el experimento. Si el estado del sistema inmediatamente antes de la medida es ρ entonces, la probabilidad de obtener el resultado m es

$$p(m) = Tr(M_m^\dagger M_m \rho), \tag{3.15}$$

y el estado inmediatamente después de la medida es

$$\frac{M_m \rho M_m^\dagger}{Tr(M_m^\dagger M_m \rho)}. \tag{3.16}$$

Los operadores de medida satisfacen la condición de completitud,

$$\sum_m M_m^\dagger M_m = \mathbf{1}. \tag{3.17}$$

- **Postulado 4:** Sistemas compuestos

El espacio de Hilbert de un sistema cuántico compuesto, es el producto tensorial de los espacios de Hilbert de las componentes del sistema cuántico. Es decir, si tenemos numerados los sistemas desde 1 hasta n, y el sistema número i está preparado en el estado ρ_i, entonces el estado conjunto del sistema total es $\rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n$.

3.3. Entrelazamiento de Estados Cuánticos

El entrelazamiento es una propiedad de los sistemas cuánticos compuestos de dos o más partículas, o bien sistemas cuánticos individuales de dos o más grados de libertad. Esta propiedad da origen a un recurso físico que puede ser utilizado en aplicaciones de computación e información cuántica, tales como: teleportación de estados cuánticos [14], codificación densa [15], computación cuántica [16] y criptografía cuántica [17], que son imposibles de realizar con sistemas clásicos.

En el año 1935 E. Schrödinger [18] introduce el concepto de entrelazamiento de la siguiente forma: Cuando dos sistemas separados, de los cuales conocemos los estados de sus respectivas representaciones, entran en una interacción física temporal debido a fuerzas conocidas que actúan sobre ellos, y después de un tiempo de influencia mutua los sistemas se separan, entonces los sistemas no pueden ser descritos de la misma forma inicial dotando a cada uno de los sistemas con su propia representación. No diría que es la única pero es la característica de la Mecánica Cuántica que genera un completo distanciamiento de las lineas del pensamiento clásico. Debido a la interacción las dos representaciones (los estados cuánticos) se habrán entrelazado.

En el mismo año y como crítica a la interpretación de Copenhagen de la Mecánica Cuántica, A. Einstein, B. Podolsky y N. Rosen publican un trabajo actualmente conocido como paradoja EPR [19]. En este trabajo se cuestiona si la Mecánica Cuántica puede ser considerada como una teoría completa de la realidad física. Según los autores, en una teoría completa, cada "elemento de realidad" física debe tener una contraparte en la teoría física. Esta teoría debería satisfacer el siguiente criterio: Si sin perturbar en ningún modo un sistema podemos predecir con certeza, es decir con probabilidad unitaria, el valor de una cantidad física, entonces existe un elemento de realidad física asociado a dicha cantidad. El argumento EPR señala que en Mecánica Cuántica, si los correspondientes operadores de dos cantidades físicas, decimos A y B no conmutan, es decir $AB \neq BA$, entonces el conocimiento preciso de una de las cantidades físicas excluye el conocimiento de la otra cantidad física. Por lo tanto, se concluye que: (1) la descripción de realidad de la Mecánica Cuántica entregada por la función de onda no es completa, ó (2) cuando los correspondientes operadores de dos cantidades físicas no conmutan no pueden tener realidad simultáneamente.

Posteriormente, en el mismo año 1935 N. Bohr [20] responde a la crítica realizada a la interpretación de Copenhagen de la Mecánica Cuántica. El argumento de Bohr fue que hay una ambigüedad en la implicancia de la expresión: "sin perturbar en ningún modo un sistema", dado que en Mecánica Cuántica es imposible controlar con certeza la reacción de un objeto ante el instrumento de medida. Lo cual es conocido como principio de incertidumbre. Por ejemplo, es imposible controlar la transferencia de momentum en el caso de la medida de la posición, y el

desplazamiento en el caso de la medida del momentum.

En el año 1952 D. Bohm introduce una nueva interpretación de la Mecánica Cuántica en términos de variables "ocultas" [21]. Con las cuales se puede determinar en forma precisa el resultado de cada proceso individual de medida. Señala que la Mecánica Cuántica puede ser generalizada, al considerar que las perturbaciones en el proceso de medida podrían ser eliminadas. Según esta interpretación es concebible que el principio de incertidumbre no sea válido.

En el año 1964 fue propuesta una prueba experimental por J. Bell [22], para determinar si los argumentos de EPR eran válidos. El resultado es conocido como la "desigualdad de Bell", la cual es completamente general y no depende de una teoría física en particular. Por medio de la desigualdad de Bell fue posible demostrar que al considerar estados maximalmente entrelazados no se cumple la desigualdad de Bell lo que está de acuerdo con las predicciones de la Mecánica Cuántica y en contradicción con las ideas de la paradoja EPR. Es el requisito de localidad, o más precisamente que el resultado de una medición sobre un sistema, no sea afectado por operaciones sobre sistemas distantes con los cuales ha interactuado en el pasado, el que crea la dificultad esencial. Por lo tanto, no existe una teoría física sobre variables ocultas que reproduzca todas las predecicciones de la Mecánica Cuántica.

3.3.1. Estados Separables y Entrelazados

Los estados cuánticos maximalmente entrelazados son el recurso principal para varios protocolos en el campo de las comunicaciones cuánticas, tales como teleportación cuántica [14], codificación densa [15], intercambio de entrelazamiento [23] y criptografía cuántica [24]. Sin embargo, si el estado cuántico está parcialmente entrelazado es aún posible utilizar este grado de entrelazamiento para realizar los protocolos mencionados anteriormente, pero con una menor eficiencia [25]. Dada la importancia de este nuevo recurso físico, se requiere conocer cuando un estado está entrelazado y cuantificar el grado de entrelazamiento del sistema cuántico en estudio.

Los estados compuestos de dos o más partículas que no están entrelazados se llaman separables y se caracterizan por que siempre satisfacen la desigualdad de Bell (3.32). Decimos que un estado $\rho_{ABC...}$ compuesto por los subsistemas A, B, C,..., es separable [26] si el estado puede ser escrito como

$$\rho_{ABC...} = \sum_i p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i \otimes ..., \tag{3.18}$$

donde ρ_A^i, ρ_B^i, ρ_C^i,..., son los operadores densidad de los subsistemas A, B, C,..., respectivamente, y $\sum_i p_i = 1$.

Como contraparte a los estados separables que no presentan correlaciones cuánticas, pero si correlaciones clásicas, tenemos los estados entrelazados. Un estado bipartito en un espacio de Hilbert $d \times d$ dimensional, está maximalmente entrelazado si puede ser escrito de la forma,

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i, i\rangle \,, \tag{3.19}$$

o es unitariamente equivalente a (3.19). Un estado maximalmente entrelazado $|\psi_{jk}\rangle$ puede ser construido a partir de una base separable, la cual es denotada por $|j\rangle \otimes |k\rangle$ con $j,k = 0,...,d-1$ que expande un espacio de Hilbert de dos qudit, de la siguiente forma

$$|\psi_{jk}\rangle_{12} = GXOR_{12}[(F\,|j\rangle_1) \otimes |k\rangle_2] = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} e^{i\frac{2\pi}{d}jn}\,|n\rangle_1 \otimes |n \ominus k\rangle_2\,, \tag{3.20}$$

donde F es la transformada discreta de Fourier que es de la forma

$$F\,|j\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{i\frac{2\pi}{d}jm}\,|m\rangle\,, \tag{3.21}$$

y la compuerta cuántica unitaria $GXOR$ [11] aplicada sobre dos partículas es,

$$GXOR_{12}\,|i\rangle_1\,|j\rangle_2 = |i\rangle_1\,|i \ominus j\rangle_2\,, \tag{3.22}$$

donde $i \ominus j$ denota la diferencia $i - j$ modulo d.

En particular, cuando la dimensión es igual a $d = 2$, los estados maximalmente entrelazados son los cuatro estados de Bell. Estos estados son ortogonales y forman una base para el espacio de Hilbert de las dos partículas. Por lo tanto, es posible expandir cualquier estado que pertenece a este espacio de Hilbert en la base de Bell. Los estados de Bell son:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle), \tag{3.23}$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle - |1\rangle\,|1\rangle), \tag{3.24}$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle), \tag{3.25}$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle). \tag{3.26}$$

3.3.2. Desigualdad de Bell

La desigualdad de Bell se obtiene asumiendo la existencia de un sistema físico compuesto por dos subsistemas A y B, el cual es descrito por un conjunto de variables ocultas λ. Se considera que el sistema está compuesto de dos partículas de spin 1/2 y que medimos en un experimento $\sigma_{\vec{a}}^{(A)}$ en el sistema A en la dirección $\vec{a}$ y $\sigma_{\vec{b}}^{(B)}$ en el sistema B en la dirección $\vec{b}$. Los posibles resultados serán:

$$\sigma_{\vec{a}}^{(A)} \to A(\vec{a},\lambda) \;=\; \pm 1, \tag{3.27}$$

$$\sigma_{\vec{b}}^{(B)} \to B(\vec{b},\lambda) \;=\; \pm 1, \tag{3.28}$$

donde $\vec{a}$ y $\vec{b}$ son vectores unitarios. Además, existe una anticorrelación perfecta si medimos en la misma dirección, es decir, $A(\vec{a},\lambda)B(\vec{a},\lambda) = -1$, lo que implica que las partículas de spin

estarán en sentidos opuestos. El resultado obtenido de cada subsistema lo multiplicamos entre sí y repetimos el experimento muchas veces, de esta forma el promedio de esas mediciones será

$$E(\vec{a},\vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a},\lambda) B(\vec{b},\lambda), \tag{3.29}$$

donde $\rho(\lambda) \geq 0$ es la distribución estadística de las variables ocultas que cumple con la relación $\int d\lambda \rho(\lambda) = 1$. Si la partícula B es medida en una dirección adicional $\vec{c}$ es posible establecer una diferencia entre las mediciones realizadas en las distintas direcciones, es decir

$$E(\vec{a},\vec{b}) - E(\vec{a},\vec{c}) = \int d\lambda \rho(\lambda) A(\vec{a},\lambda)(B(\vec{b},\lambda) - B(\vec{c},\lambda)). \tag{3.30}$$

Usando la propiedad de anticorrelación y el hecho que $A^2 = 1$, se obtiene

$$E(\vec{a},\vec{b}) - E(\vec{a},\vec{c}) = -\int d\lambda \rho(\lambda) A(\vec{a},\lambda) A(\vec{b},\lambda)(1 + A(\vec{b},\lambda) B(\vec{c},\lambda)), \tag{3.31}$$

donde notamos que el término $1 + A(\vec{b},\lambda)B(\vec{c},\lambda)$ es siempre positivo o nulo. En el caso que $A(\vec{a},\lambda)A(\vec{b},\lambda) = 1$, es decir, tome su máximo valor, se tiene

$$E(\vec{a},\vec{b}) - E(\vec{a},\vec{c}) \geq -\int d\lambda \rho(\lambda)(1 + A(\vec{b},\lambda) B(\vec{c},\lambda)) = -1 - E(\vec{b},\vec{c}),$$

en el caso que $A(\vec{a},\lambda)A(\vec{b},\lambda) = -1$, es decir, tome su mínimo valor, se tiene

$$E(\vec{a},\vec{b}) - E(\vec{a},\vec{c}) \leq \int d\lambda \rho(\lambda)(1 + A(\vec{b},\lambda) B(\vec{c},\lambda)) = 1 + E(\vec{b},\vec{c}).$$

Con lo cual se obtiene la desigualdad de Bell,

$$|E(\vec{a},\vec{b}) - E(\vec{a},\vec{c})| \leq 1 + E(\vec{b},\vec{c}), \tag{3.32}$$

que depende sólo de los ángulos de las distintas direcciones de medida y que debe ser satisfecha si la teoría de variables ocultas es válida. Sin embargo, si consideramos el estado singlete para dos partículas de spin 1/2

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A |\downarrow\rangle_B - |\downarrow\rangle_A |\uparrow\rangle_B), \tag{3.33}$$

el cual es un estado cuántico maximalmente entrelazado, no se satisface la desigualdad de Bell (3.32). Por lo tanto, existen estados cuánticos que no cumplen la desigualdad de Bell y en consecuencia, la teoría de las variables ocultas no puede ser correcta.

Si uno de los observadores puede medir en las direcciones $\vec{a}$ y $\vec{b}$ y el otro observador mide en las direcciones $\vec{c}$ y $\vec{d}$, se obtiene una desigualdad generalizada de Bell llamada de Clauser-Horne-Shimony-Holt (CHSH) [27], la cual tiene la siguiente forma

$$|S| = |\langle ac\rangle - \langle ad\rangle + \langle bc\rangle + \langle bd\rangle| \leq 2. \tag{3.34}$$

La desigualdad de CHSH fue comprobada experimentalmente [28] utilizando pares de fotones entrelazados en polarización. En el resultado experimental se obtuvo un valor de $S_{exp} = 2{,}697 \pm$

0,015, el cual está muy por sobre el valor predicho por la desigualdad de CHSH igual a $|S| \leq 2$ y se ajusta mucho mejor al valor $|S_{MC}| = 2\sqrt{2}$, predicho por la Mecánica Cuántica. También se han reportado correlaciones no locales en experimentos realizados con fotones entrelazados [29, 30] y con pares de átomos entrelazados [31]. Con lo cual los resultados experimentales se ajustan a los predichos por la Mecánica Cuántica y no a los predichos por una teoría de realismo local.

3.3.3. Medidas de Entrelazamiento

La generación experimental de los estados entrelazados no es perfecta, por lo que generalmente se cuenta con estados que están parcialmente entrelazados. Por ello es necesario cuantificar el grado de entrelazamiento de los estados parcialmente entrelazados. Un posible criterio para distinguir los estados separables de los estados entrelazados es la desigualdad de Bell. Sin embargo, existen estados entrelazados que no satisfacen la desigualdad. Por ejemplo, los estados de Werner [26] que se pueden parametrizar de la siguiente forma

$$\rho_w = \frac{1-\lambda}{d^2}\mathbf{1} + \lambda \left|\beta_{11}\right\rangle \left\langle\beta_{11}\right|, \tag{3.35}$$

están parcialmente entrelazados pero no violan de la desigualdad de Bell. Por lo tanto, la desigualdad de Bell no puede ser utilizada como una posible medida de entrelazamiento.

- **Entropía del entrelazamiento**

Para estados puros bipartitos $|\phi\rangle_{AB}$ una buena medida de entrelazamiento es la entropía de von Neumann de una de las operadores densidad reducida. Se define la *entropía del entrelazamiento* para un estado puro $|\phi\rangle_{AB}$ como

$$E(|\phi\rangle\langle\phi|) = S(Tr_A |\phi\rangle\langle\phi|) = S(Tr_B |\phi\rangle\langle\phi|), \tag{3.36}$$

donde S denota la entropía de von Neumann $S(\rho) = -Tr[\rho log_2 \rho]$, y Tr_B denota la traza parcial sobre el subsistema B.

- **Condiciones para una medida de entrelazamiento**

Para estados mixtos no hay una única medida de entrelazamiento. Sin embargo, una posible medida de entrelazamiento debería satisfacer las siguientes condiciones [32]:

(a) La medida de entrelazamiento para un sistema bipartito $E(\rho)$ debe ser un mapeo desde operadores densidad a números reales positivos $\rho \rightarrow E(\rho) \in \mathbb{R}^+$.
(b) La medida de entrelazamiento debe ser cero, si y sólo si, el estado es separable, es decir $E(\rho) = 0$, $\forall\rho$ separable.
(c) La medida de entrelazamiento $E(\rho)$ no debe en promedio aumentar bajo operaciones locales y comunicaciones clásicas (LOCC), es decir,

$$E(\rho) \geq \sum_i p_i E(\frac{A_i \rho A_i^\dagger}{Tr A_i \rho A_i^\dagger}), \tag{3.37}$$

donde los A_i son los operadores de Kraus describiendo algún protocolo LOCC y la probabilidad de obtener el resultado i es dado por $p_i = Tr(A_i \rho A_i^\dagger)$.
(d) Para estados puros la medida de entrelazamiento se debe reducir a la entropía del entrelazamiento [33], es decir a la relación de la ecuación (3.36). Para estados maximalmente entrelazados como el estado de la ecuación (3.19) la medida de entrelazamiento debería ser igual a $E(|\psi\rangle_{AB}) = logd$.

Junto con las condiciones básicas, expuestas anteriormente, que debe satisfacer una medida de entrelazamiento $E(\rho)$ algunos autores [32, 34] exigen otras propiedades que debe cumplir $E(\rho)$. Por ejemplo,

(e) *Continuidad*: El entrelazamiento debe converger a cero, en el límite cuando la distancia de dos operadores densidad distintos tiende a cero, es decir, $E(\rho) - E(\sigma) \to 0$ para $\|\rho - \sigma\| \to 0$.
(f) *Aditividad*: Un número n de copias idénticas del estado ρ debería contener n veces el entrelazamiento de una copia, es decir, $E(\rho^{\otimes n}) = nE(\rho)$.
(g) *Subaditividad*: El entrelazamiento del producto tensorial de dos estados ρ y σ no debería ser mayor que la suma de los entrelazamientos de cada subsistema, es decir, $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$.
(h) *Convexidad*: La medida del entrelazamiento debería ser una función convexa, es decir, $E(\lambda\rho + (1-\lambda)\sigma) \leq \lambda E(\rho) + (1-\lambda)E(\sigma)$ para $0 < \lambda < 1$.

- **Entrelazamiento de formación**

Una de las medidas de entrelazamiento que satisface las condiciones anteriores y que generaliza la entropía del entrelazamiento (3.36) para estados mixtos, es el entrelazamiento de formación E_f. Para un sistema bipartito ρ_{AB}, el entrelazamiento de formación es el mínimo sobre todas las descomposiciones del ensamble de ρ_{AB},

$$E_f(\rho_{AB}) = min \sum_i p_i E(\psi_i), \tag{3.38}$$

donde la minimización es realizada sobre todos los ensambles $\{p_i, \psi_i\}$ tal que $\rho_{AB} = \sum_i p_i |\psi_i\rangle \langle\psi_i|$. La minimización de la expresión (3.38) en el caso de dos qubit fue realizada por Wootters [35]. El entrelazamiento de formación de un estado ρ_{AB} de dos qubit es

$$E_f(\rho_{AB}) = h\left(\frac{1 + \sqrt{1 - C(\rho_{AB})^2}}{2}\right), \tag{3.39}$$

donde h es la entropía binaria $h(x) = -xlog_2x - (1-x)log_2(1-x)$, y $C(\rho_{AB})$ es la llamada concurrencia dada por la siguiente expresión

$$C(\rho_{AB}) = max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \tag{3.40}$$

donde λ_i, $i = 1, 2, 3, 4$, son los autovalores de $\sqrt{\sqrt{\rho_{AB}}\tilde{\rho}_{AB}\sqrt{\rho_{AB}}}$, donde

$$\tilde{\rho_{AB}} = (\sigma_y \otimes \sigma_y)\rho_{AB}^*(\sigma_y \otimes \sigma_y). \tag{3.41}$$

- **Negatividad**

En el caso de sistemas de 2×2 Peres [36] encontró un criterio de separabilidad conocido como la negatividad. Si la matriz transpuesta parcial de ρ tiene algún autovalor negativo entonces el estado ρ está entrelazado. La positividad de la matriz transpuesta parcial de ρ es una condición necesaria y suficiente para la separabilidad de estados de dimensión 2×2 y 2×3 [37]. Para dimensiones más altas el criterio de la transpuesta parcial positiva (PPT) es sólo una condición necesaria de separabilidad, ya que ha sido demostrada la existencia de estados entrelazados con transpuesta parcial positiva [38].

La transposición parcial de un estado ρ_{AB}

$$\rho_{AB} = \sum_{i,j,k,l} \rho_{ij,kl} \left|i\right\rangle_A \left\langle j\right| \otimes \left|k\right\rangle_B \left\langle l\right|, \tag{3.42}$$

con respecto al subsistema B, es definido como

$$\rho^{T_B} = \sum_{i,j,k,l} \rho_{ij,kl} \left|i\right\rangle_A \left\langle j\right| \otimes \left|l\right\rangle_B \left\langle k\right|. \tag{3.43}$$

La negatividad cuantifica que tan negativo es el espectro de la transpuesta parcial, la cual es definida como

$$N(\rho) = \frac{\|\rho^{T_B}\| - 1}{2}, \tag{3.44}$$

donde $\|X\| = Tr\sqrt{X^\dagger X}$ es la norma traza. Sin embargo, la negatividad no es aditiva, por lo que se utiliza como medida de entrelazamiento la llamada negatividad logarítmica, la cual es definida como

$$E_N(\rho) = log_2\|\rho^{T_B}\|. \tag{3.45}$$

La mayor ventaja práctica de E_N es que puede ser calculada fácilmente. Además, constituye un límite para la capacidad de la teleportación [39] y está relacionada con otras medidas de entrelazamiento (Anexo A).

3.4. Aplicaciones del Entrelazamiento

3.4.1. Codificación Densa

Una de las primeras aplicaciones de los estados maximalmente entrelazados a la transmisión de información clásica es la codificación densa, más conocida como "dense coding". Publicada el año 1992 por C. Bennett y S. Wiesner [15], consiste en la transmisión de dos bits de información clásica enviando sólo un qubit. Este proceso se basa en que por medio de operaciones locales, es decir operaciones unitarias que se aplican sólo sobre una de las partículas, es posible transformar un estado de Bell a otro estado de Bell.

Suponemos que una de las partes, "Alice" prepara un estado maximalmente entrelazado, el cual es uno de los estados de Bell, por ejemplo $|\beta_{00}\rangle_{AB}$,

$$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B), \tag{3.46}$$

y envía la partícula B a otro usuario llamado "Bob". Luego, Bob aplica una de las cuatro transformaciones unitarias U_{jk} sobre su partícula B. La información que desea transmitir Bob está codificada en los valores de los coeficientes (j,k) de la transformación unitaria U_{jk}, donde

$$\begin{aligned} U_{00} &= |0\rangle\langle 0| + |1\rangle\langle 1|, & (3.47)\\ U_{01} &= |0\rangle\langle 1| + |1\rangle\langle 0|, & (3.48)\\ U_{10} &= |0\rangle\langle 0| - |1\rangle\langle 1|, & (3.49)\\ U_{11} &= |0\rangle\langle 1| - |1\rangle\langle 0|. & (3.50) \end{aligned}$$

Después de lo cual, Bob cambia el estado conjunto inicial $|\beta_{00}\rangle_{AB}$ y le reenvía su partícula a Alice. Por lo tanto, el estado que posee Alice será uno de los cuatro de Bell,

$$\begin{aligned} |\beta_{00}\rangle_{AB} = U_{00}|\beta_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), & (3.51)\\ |\beta_{01}\rangle_{AB} = U_{01}|\beta_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle), & (3.52)\\ |\beta_{10}\rangle_{AB} = U_{10}|\beta_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle), & (3.53)\\ |\beta_{11}\rangle_{AB} = U_{11}|\beta_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). & (3.54) \end{aligned}$$

Ahora, Alice debe distinguir el estado que posee de manera de obtener los dos bit de información enviada por Bob. Esto se debe a la directa relación entre el estado de Bell que posee Alice y la transformación unitaria aplicada por Bob.

Los estados maximalmente entrelazados y, en particular los estados de Bell se pueden generar utilizando las transformaciones unitarias $GXOR$ y la transformada cuántica de Fourier[2] tal como aparece en la ecuación (3.20)

$$|\beta_{j,k}\rangle_{AB} = GXOR_{AB}[(F|j\rangle_A)|k\rangle_B]. \tag{3.55}$$

De manera de recuperar la información enviada por Bob, Alice debe aplicar las transformaciones unitarias inversas $GXOR^{-1}$ y F^{-1} sobre su estado de Bell, para obtener

$$|j\rangle_A |k\rangle_B = F_A^{-1}[GXOR_{AB}^{-1}|\beta_{j,k}\rangle_{AB}], \tag{3.56}$$

midiendo en la base lógica de las partículas A y B, Alice encuentra los valores de (j,k) que representan los 2 bits de información clásica enviados por el qubit de Bob.

Se debe destacar que Alice no tiene información si sólo posee un qubit, ya que cada qubit por separado se encuentra en un estado completamente mixto. Esto implica que los dos bits

[2]La transformada de Fourier para sistemas bidimensionales es idéntica a la compuerta cuántica Hadamard.

de información están codificados en las correlaciones cuánticas y, pueden ser obtenidos si Alice tiene acceso simultáneamente a los dos qubits. Por otro lado, Bob es capaz de enviar los dos bit de información clásica al enviar su qubit a Alice, sin interactuar directamente con el qubit de Alice. Este proceso es imposible de realizar si se utiliza sólo un bit clásico.

Además, la máxima información accesible, según el límite de Holevo [40], es 1 bit de información clásica por qubit. Por lo tanto, la codificación densa de la información no contradice el límite de Holevo, ya que se deben utilizar dos qubits para transmitir dos bit de información clásica. La codificación densa ha sido experimentalmente realizada utilizando: fotones [41], resonancia nuclear magnética [42] y estados de luz comprimidos [43]. Es posible generalizar la codificación densa al caso de estados maximalmente entrelazados de dimensión d, utilizando los estados de Bell que aparecen en (3.20). En este caso, los coeficientes (i, j) están entre $0, ..., d-1$ y, el proceso permite la transmisión de $2log_2 d$ bit de información clásica al enviar un qudit.

3.4.2. Teleportación de Estados Cuánticos

La teleportación de un estado cuántico es un proceso que permite la transferencia de un estado cuántico, desde un punto a otro espacialmente alejado. La transferencia del estado se realiza, entre el emisor y el receptor, utilizando un estado entrelazado (canal cuántico) junto con comunicación clásica.

El esquema de teleportación en una dimensión arbitraria, denotada por d, está basado en la siguiente identidad

$$|\chi\rangle_1 |\psi_{jk}\rangle_{23} = \frac{1}{d} \sum_{l,m=0}^{d-1} |\psi_{lm}\rangle_{12} e^{-i\frac{2\pi}{d}jm} U(l,m) |\chi\rangle_3 , \tag{3.57}$$

donde, la transformación unitaria $U(l, m)$ es de la forma,

$$U(l,m) = X^{k+m} Z^{j-l}, \tag{3.58}$$

y está compuesta de las siguientes transformaciones unitarias

$$X = \sum_{n=0}^{d-1} |n-1\rangle \langle n| , \tag{3.59}$$

$$Z = \sum_{n=0}^{d-1} e^{i\frac{2\pi}{d}n} |n\rangle \langle n| . \tag{3.60}$$

En el proceso de teleportación, inicialmente, el emisor llamada Alice y el receptor llamado Bob, establecen un canal de comunicación cuántico, al generar y compartir el estado maximalmente entrelazado $|\psi_{jk}\rangle_{23}$. Este corresponde a dos partículas de dimensión d. Luego, el emisor y el receptor se separan, quedando la partícula 2 en manos del emisor y la partícula 3, en manos del receptor. Esto permite la posibilidad de establecer correlaciones cuánticas entre Alice y Bob.

El estado cuántico a ser teleportado por Alice está en general descrito por una superposición de estados de la forma

$$|\chi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle , \tag{3.61}$$

donde la información a ser transmitida y que inicialmente son desconocidos para Alice y Bob son los coeficientes α_i del estado $|\chi\rangle$.

El emisor posee las partículas 1 y 2 del estado puro conjunto $|\chi\rangle_1 |\psi_{jk}\rangle_{23}$. El estado conjunto de las tres partículas está en una superposición de estados que puede ser expresada de la forma (3.57). Para ello utilizamos los estados $|\psi_{lm}\rangle_{12}$ que son maximalmente entrelazados como una base para el espacio de Hilbert de las partículas 1 y 2. Luego, el emisor realiza una medida de Bell generalizada sobre el estado $|\psi_{lm}\rangle_{12}$, obteniendo los valores de (l, m) y proyectando el estado de la partícula del receptor al estado $U(l, m) |\chi\rangle_3$. Los valores de (l, m) son enviados a Bob, que se encuentra en un lugar en principio desconocido para Alice, por un canal clásico de comunicación. Para finalizar el proceso de teleportación, el receptor debe realizar la transformación unitaria $U^{-1}(l, m)$ de manera que la partícula 3 quede en el estado $|\chi\rangle$.

Se debe descatar que el estado original de Alice $|\chi\rangle_1$ se destruye en el proceso, es decir, después de la teleportación el estado de Alice es $|\psi_{lm}\rangle_{12}$ con (l, m) bien definido. Para obtener información de la partícula 1, Alice debe trazar sobre la partícula 2. Dado que el estado $|\psi_{lm}\rangle_{12}$ es maximalmente entrelazado, la partícula 1 queda en un estado completamente mixto. Por lo tanto, se produce un intercambio del estado entre las partículas 1 y 3. Esto es consistente con el teorema de no copiado [44], dado que no se duplica o copia la información.

La teleportación cuántica fue descubierta en el año 1993 por Bennett, Brassard, Crépeau, Jozsa, Peres, y Wootters [14]. Posteriormente, se realizó experimentalmente la teleportación utilizando; fotones [30, 45], estados comprimidos de luz [46], resonancia nuclear magnética [47] y recientemente con iones [48].

3.4.3. Intercambio de Entrelazamiento

El intercambio del entrelazamiento, también conocido como "entanglement swapping", funciona de manera similar al proceso de teleportación cuántica. Sin embargo, en este caso para transmitir información, no se requiere que inicialmente los usuarios compartan un estado maximalmente entrelazado. El intercambio de entrelazamiento se realiza de la siguiente manera [11]:

Alice inicialmente tiene el estado maximalmente entrelazado $|\psi_{\alpha,\beta}\rangle_{12}$ y, en forma independiente Bob tiene otro estado maximalmente entrelazado $|\psi_{\mu,\nu}\rangle_{34}$, estos corresponden a estados de Bell (3.20) de dimensión d. Por lo tanto, el estado conjunto inicial $|\psi_{\alpha,\beta}\rangle_{12} \otimes |\psi_{\mu,\nu}\rangle_{34}$ está factorizado y no hay entrelazamiento entre las partículas 1 ó 2 con las partículas 3 ó 4. Sin embargo, si utilizamos la base de Bell de las partículas 23 y 14, el estado inicial corresponde a una super-

posición de d^2 estados de la forma,

$$|\psi_{\alpha,\beta}\rangle_{12} \otimes |\psi_{\mu,\nu}\rangle_{34} = \frac{1}{d} \sum_{l,\rho=0}^{d-1} e^{-i\frac{2\pi}{d}\mu(\rho+\beta)} |\psi_{l,\rho}\rangle_{23} \otimes U(l,\beta) |\psi_{\alpha+\mu,\beta+\rho+\nu}\rangle_{14} ,$$

donde la transformación unitaria $U(l,\beta)$ actúa sólo sobre el primer qudit y es definida por

$$U(l,\beta) = e^{i\frac{2\pi}{d}l\beta}(Z)^{-l}. \tag{3.62}$$

Si ahora, Alice envía la partícula 2 y Bob la partícula 3 a un tercer participante (Eva) para que realice una medida de Bell sobre las partículas 23. Entonces, Eva obtiene los valores de (l,ρ) y proyecta el estado inicial, al estado maximalmente entrelazado de las partículas 1 y 4, el cual es dado por

$$U(l,\beta) |\psi_{\alpha+\mu,\beta+\rho+\nu}\rangle_{14} . \tag{3.63}$$

Eva debe comunicar a Alice el resultado de su medida, es decir el par de valores (l,ρ), de manera que Alice pueda aplicar la transformación unitaria $U^{-1}(l,\beta)$ sobre la primera partícula. Finalmente, el estado de las partículas 1 y 4 será $|\psi_{\alpha+\mu,\beta+\rho+\nu}\rangle_{14}$, el cual está maximalmente entrelazado.

Se debe destacar que Alice necesita conocer sólo el valor de l, ya que ella conoce el valor de β. Además, no es necesaria la presencia de Eva, ya que las partículas 1, 2 y 3 pueden estar eventualmente en el poder de Alice. En el intercambio del entrelazamiento, dos partículas que inicialmente no poseen entrelazamiento, después de finalizado el proceso se encuentran maximalmente entrelazadas. Para ello se debe medir en la base de Bell dos de las partículas que inicialmente no estaban entrelazadas.

El intercambio de entrelazamiento fue publicado el año 1993 por M. Zukowski, A. Zeilinger, M. Horne y K. Ekert [23]. Fue realizado experimentalmente usando: fotones [49], resonancia nuclear magnética [50] y átomos neutros [51]. El intercambio de entrelazamiento se puede generalizar, al considerar la manipulación del entrelazamiento en sistemas multi-partícula [52].

3.5. Operaciones Cuánticas

El formalismo de las operaciones cuánticas nos permite describir la dinámica de los sistemas cuánticos, en una gran variedad de condiciones físicas. Por ejemplo, los sistemas cuánticos abiertos, los cuales se encuentran fuertemente acoplados con su medio ambiente, pueden ser descritos a través de las operaciones cuánticas. En el formalismo de las operaciones cuánticas, el estado del sistema se describe por medio del operador densidad ρ, el cual transforma de la siguiente manera

$$\rho' = \mathcal{E}(\rho). \tag{3.64}$$

Al mapeo $\mathcal{E}$ que transforma el operador densidad inicial ρ en el operador densidad final ρ' se le denomina "operación cuántica".

La operación cuántica $\mathcal{E}$ describe la dinámica del cambio del estado que ocurre como resultado de algún proceso físico; donde ρ es el estado inicial antes del proceso, y $\mathcal{E}(\rho)$ es el estado final después de ocurrido el proceso, donde el estado final debe estar normalizado. Algunos ejemplos de operaciones cuánticas son: las transformaciones unitarias, $\mathcal{E}(\rho) = U\rho U^\dagger$ y las mediciones cuánticas $\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$.

3.5.1. Operaciones Locales

Consideramos que un operador densidad ρ_{AB} describe el estado de un sistema cuántico compuesto de dos subsistemas. Cada uno de los subsistemas se encuentra en poder de un observador, a los cuales llamamos A y B. Los observadores A y B sólo pueden aplicar transformaciones sobre su respectivo sistema, lo cual es denotado por $\mathcal{A}\otimes\mathbf{1}$ y $\mathbf{1}\otimes\mathcal{B}$, respectivamente. Permitiremos que las transformaciones que un observador aplica sobre su sistema dependan de las transformaciones aplicadas por el otro observador sobre su sistema. Dado que permitimos esta condicionalidad en la aplicación de las transformaciones debe existir una coordinación entre los observadores, la cual se lleva a cabo por medio del intercambio de información clásica. Este tipo de operaciones se denominan *operaciones cuánticas locales y comunicaciones clásicas* (LOCC) [53].

Un mapeo local puede ser cualquier transformación local, incluyendo una medida promediada sobre todos los posibles resultados [54]. La aplicación de un mapeo local por una de las partes no es necesariamente conocida por su contraparte con quien comparte el estado ρ_{AB}. Por ejemplo, Alice puede elegir entre distintos mapeos locales para codificar el mensaje "m" que Alice desea transmitir. Ella codifica el mensaje al realizar la transformación $\mathcal{A}_m \otimes \mathbf{1}$ sobre su partícula. Por otro lado, Bob puede aplicar una transformación local $\mathbf{1}\otimes\mathcal{B}$ sobre su partícula y luego, una medida local $\mathbf{1}\otimes\Pi_r$ para decodificar el mensaje. Donde Π_r es un elemento de un operador de medida definido positivo (POVM).

Es posible descomponer una operación cuántica local arbitraria en términos de cuatro procesos más simples [53]. Estos son:

- **Transformación local unitaria**,

$$\rho_{AB} \to \rho'_{AB} = (U_A \otimes \mathbf{1}_B)\rho_{AB}(U_A^\dagger \otimes \mathbf{1}_B), \tag{3.65}$$

  donde U_A es una transformación unitaria que actúa sobre el sistema en poder del observador A. La transformación unitaria también puede ser aplicada por el observador B, en este caso tenemos el operador $\mathbf{1}_A \otimes U_B$ actuando sobre ρ_{AB}.

- **Mediciones locales tipo von Neumann**. El observador A mide alguna cantidad sobre su sistema. Dicho proceso está simulado por la aplicación de un proyector $P^k = P^k_{AB} \otimes \mathbf{1}_B$ local sobre la matriz densidad ρ_{AB}. El resultado de la medida se obtiene con probabilidad p_k y proyecta al sistema total al estado $\rho^k_{AB} = P^k\rho_{AB} = (P^k_{AB}\otimes\mathbf{1}_B)\rho_{AB}$. Como ya se ha analizado, los proyectores P^k son ortogonales y una resolución del operador identidad $\mathbf{1}_A$.

- **Adjuntar una ancilla**,

$$\rho_{AB} \to \rho_{ABC} = \rho_{AB} \otimes \rho_C. \tag{3.66}$$

  Esta operación consiste en que un observador aumenta la dimensión de su espacio de Hilbert por medio de la inclusión de un nuevo sistema físico. El estado de este sistema no está inicialmente correlacionado con el estado del sistema total.

- **Eliminación de la ancilla**. La ancilla puede ser eliminada por el correspondiente observador, esta operación corresponde a

$$\rho_{ABC} \to \rho'_{AB} = Tr_C[\rho_{ABC}]. \tag{3.67}$$

Las comunicaciones clásicas permiten que algunas de las operaciones cuánticas locales dependan del resultado de otras operaciones cuánticas locales. Esto origina la existencia de transformaciones locales que no corresponden a operaciones cuánticas locales. Sin embargo, estas transformaciones pueden ser escritas en términos de los cuatro procesos básicos vistos anteriormente junto con un nuevo proceso. Supongamos que los observadores A y B comparten un sistema compuesto caracterizado por el espacio de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$. Estos espacios de Hilbert pueden estar asociados, por ejemplo, a dos partículas de idénticas características, una en poder de A y otra en poder de B. El estado de ambos sistemas está descrito por el operador densidad $\rho^{(1)}_{AB}$. Los observadores comparten un segundo par de partículas en el estado $\rho^{(2)}_{AB}$. Supongamos que el observador A, con probabilidad q_1 elimina una de las partículas en su poder de modo que termina con el estado $\rho^{(1)}_{AB}$, si comunica su intención al observador B, de modo que éste elimine la partícula correspondiente. Después de éste proceso, los observadores finalizan el proceso con uno de los dos posibles estados, es decir

$$\rho = \rho^{(1)}_{AB} \otimes \rho^{(2)}_{AB} \to \{q_1, \rho^{(1)}_{AB} \otimes \mathbf{1}^{(2)}; 1 - q_1, \mathbf{1}^{(1)} \otimes \rho^{(2)}_{AB}\}. \tag{3.68}$$

Ahora, si el observador A no comunica su elección de partícula para eliminar y borra el registro de las elecciones anteriores, el estado final será

$$\rho = \rho^{(1)}_{AB} \otimes \rho^{(2)}_{AB} \to \rho' = q_1 \rho^{(1)}_{AB} \otimes \mathbf{1}^{(2)} + (1 - q_1)\mathbf{1}^{(1)} \otimes \rho^{(2)}_{AB}. \tag{3.69}$$

El obtener alguno de los estados (3.68) ó (3.69) depende únicamente de la información disponible a los observadores, lo cual puede ser realizado localmente por medio del control del flujo de información clásica entre ellos. Luego, tenemos un quinto proceso fundamental,

- **Reducción en la información disponible sobre el sistema total:**

$$\{q_k, \rho_k\} \to \rho' = \sum_k q_k \rho_k, \tag{3.70}$$

donde $\sum_k q_k \rho_k$ es cualquier ensamble que realiza ρ'.

3.5.2. Condiciones que Satisfacen las Operaciones Cuánticas

Las operaciones cuánticas son las transformaciones de estados cuánticos más generales permitidas por los axiomas de la mecánica cuántica. Lo cual implica que deben satisfacer las siguientes condiciones [4]:

- Dado que $Tr[\mathcal{E}(\rho)]$ representa la probabilidad que el proceso $\mathcal{E}$ ocurra, cuando el estado inicial es ρ. Entonces, para todo estado ρ, se tiene

$$0 \leq Tr[\mathcal{E}(\rho)] \leq 1. \tag{3.71}$$

Esto implica que $\mathcal{E}$ no necesariamente preserva la propiedad de traza de las operadores densidad, $Tr(\rho) = 1$. En el caso que el proceso es determinista, esto se reduce a la condición $Tr[\mathcal{E}(\rho)] = 1 = Tr(\rho)$, para todo ρ. Por otro lado, una medida no preserva la traza con lo cual $Tr[\mathcal{E}(\rho)] \leq 1$, dado que los propios $\mathcal{E}$ no proveen una completa descripción del proceso. Es decir, pueden ocurrir otros resultados en la medida, con alguna probabilidad. Una operación cuántica para que sea físicamente realizable debe satisfacer la condición que la probabilidad nunca sea mayor de uno, es decir $Tr[\mathcal{E}(\rho)] \leq 1$.

- La operación cuántica $\mathcal{E}$ es un mapeo lineal convexo sobre un conjunto de operadores densidad, es decir

$$\mathcal{E}(\sum_i p_i \rho_i) = \sum_i p_i \mathcal{E}(\rho_i), \tag{3.72}$$

donde p_i es la probabilidad de encontrar al sistema en el estado ρ_i. Consistente con la interpretación de ensamble de un operador densidad; si el sistema se encuentra en el estado ρ_0 con probabilidad p, o en el estado ρ_1 con probabilidad $1-p$, entonces el estado final del sistema debería estar en $\mathcal{E}(\rho_0)$ o en $\mathcal{E}(\rho_1)$ con las probabilidades p ó $1-p$, respectivamente.

- El mapeo $\mathcal{E}$ es completamente positivo. Esto implica que no sólamente $\mathcal{E}(\rho)$, debe ser válido como operador densidad (hasta una constante de normalización). Además, si $\rho = \rho_{AB}$ es el operador densidad de un sistema compuesto AB y, si $\mathcal{E}$ actúa sólo en el sistema B, entonces

$$\forall \ \rho_{AB} \geq 0 \ \ \Rightarrow \ \ (1_A \otimes \mathcal{E})\rho_{AB} \geq 0, \tag{3.73}$$

donde $\mathbf{1}_A$ denota el mapeo idéntidad sobre el sistema A. El operador $\mathbf{1}_A \otimes \mathcal{E}$ debe mapear operadores positivos a operadores positivos.

La operación cuántica $\mathcal{E}$ satisface las tres condiciones anteriores, si y sólo si, puede ser escrito de la forma

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger, \tag{3.74}$$

para un conjunto de operadores $\{E_i\}$ que mapea el espacio de Hilbert de entrada al espacio de Hilbert de salida, y

$$\sum_i E_i^\dagger E_i \leq \mathbf{1}. \tag{3.75}$$

La operación cuántica $\mathcal{E}$ de la ecuación (3.74), es un mapeo completamente positivo que se descompone en una representación de suma de operadores, conocida como representación de Kraus. La igualdad en la expresión (3.75) se tiene sólo para operaciones deterministas y, los operadores E_i son llamados operadores de Kraus [55].

3.6. Imposibilidad de Copiar Estados

Una de las propiedades de los sistemas cuánticos, es la imposibilidad de copiar o duplicar un estado arbitrario desconocido $|\psi\rangle$. Esto constrasta fuertemente con el caso clásico, donde es posible copiar de manera perfecta la información. Este resultado, conocido como "no-cloning theorem", fue publicado el año 1982 por Wootters y Zurek [44].

En forma más precisa, este teorema enuncia que no existe una operación cuántica $\mathcal{E}$ tal que $|\psi\rangle|\phi\rangle \xrightarrow{\mathcal{E}} |\psi\rangle|\psi\rangle$, para un estado inicial $|\phi\rangle$ cualquiera. Esta es una propiedad de la linealidad de la Mecánica Cuántica y, por lo tanto, de las operaciones cuánticas. Consideremos un sistema cuántico bidimensional y una transformación sobre la base $\{|0\rangle, |1\rangle\}$ tal que se tiene

$$|0\rangle|\phi\rangle \rightarrow |0\rangle|0\rangle, \tag{3.76}$$
$$|1\rangle|\phi\rangle \rightarrow |1\rangle|1\rangle, \tag{3.77}$$

es decir, podemos copiar en forma perfecta estos estados. Sin embargo, si deseamos copiar un estado cuántico más general, por ejemplo, una superposición como $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, aplicando la transformación definida por las ecuaciones (3.76) y (3.77) tenemos,

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\phi\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \tag{3.78}$$

pero el estado final es distinto al estado que se deseaba copiar, ya que

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \neq \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle). \tag{3.79}$$

Por lo tanto, es imposible copiar en forma perfecta un estado cuántico arbitrario desconocido. Este resultado es conocido como "no-cloning theorem".

Sin embargo, es posible copiar estados arbitrarios de manera imperfecta [56], es decir, con una fidelidad menor que la unidad. Para ello se utiliza una máquina universal de clonado cuántico, y se considera un estado de la forma $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ donde α y β son números complejos que satisfacen $|\alpha|^2 + |\beta|^2 = 1$. La máquina de clonado con un estado inicial $|C\rangle$ y con un estado inicial en blanco $|0\rangle_B$ del sistema B donde se copiará la información, opera de la siguiente manera,

$$|0\rangle|0\rangle|C\rangle \rightarrow |\Sigma_0\rangle, \tag{3.80}$$
$$|1\rangle|0\rangle|C\rangle \rightarrow |\Sigma_1\rangle, \tag{3.81}$$

donde los estados finales $|\Sigma_0\rangle$ y $|\Sigma_1\rangle$ pertenecen al espacio de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, donde A y B denotan los estados de las dos copias y C denota el estado de la máquina de clonado. Por la linealidad de la Mecánica Cuántica, un estado arbitrario $|\psi\rangle$ es clonado como

$$|\psi\rangle|0\rangle|C\rangle \rightarrow \alpha|\Sigma_0\rangle + \beta|\Sigma_1\rangle \equiv |\Sigma\rangle. \tag{3.82}$$

Los estados finales para cada copia son,

$$\rho_A = Tr_{BC}(|\Sigma\rangle\langle\Sigma|), \tag{3.83}$$
$$\rho_B = Tr_{AC}(|\Sigma\rangle\langle\Sigma|), \tag{3.84}$$

y la fidelidad de cada copia con respecto al estado original es,

$$F_A(\psi) = \langle\psi|\rho_A|\psi\rangle, \tag{3.85}$$
$$F_B(\psi) = \langle\psi|\rho_B|\psi\rangle, \tag{3.86}$$

que cuantifica la semejanza entre el estado que deseamos copiar $|\psi\rangle$ y el estado de salida de cada copia, ρ_A ó ρ_B. Si imponemos la condición que las fidelidades de salida sean iguales $F_A(\psi) = F_B(\psi)$, la máquina de clonado cuántico es independiente de los estados $|\psi\rangle$ a copiar. Además, los estados de salida son dados por

$$\rho_A = \rho_B = \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{6}\mathbf{1}, \tag{3.87}$$

y se obtiene la fidelidad más alta que permite la Mecánica Cuántica para la transformación de clonado de un estado arbitrario $|\psi\rangle$, la cual es igual a $F^{univ} = 5/6$.

Es posible generalizar el clonado de estados de sistemas bidimensionales [56], al caso de estados en un espacio de Hilbert de dimensión d [57]. La transformación unitaria, que define la máquina de clonado universal desde una copia inicial hasta dos copias finales, actuando sobre sus vectores base es

$$|i\rangle|R\rangle|\mathcal{M}\rangle \to \sqrt{\frac{2}{d+1}}|i\rangle|i\rangle|i\rangle + \frac{1}{\sqrt{2(d+1)}}\sum_{j\neq i}^{d}[|i\rangle|j\rangle + |j\rangle|i\rangle]|j\rangle\,, \tag{3.88}$$

donde $|R\rangle$ es el estado de la ancilla, en el cual se realizará el proceso de copiado del estado $|i\rangle$ y $|\mathcal{M}\rangle$ denota el estado de la máquina de copiado.

Para un estado arbitrario en un espacio d dimensional, $|\psi\rangle = \sum_{i=1}^{d}\alpha_i|i\rangle$, los estados de salida son

$$\rho_A = \rho_B = \frac{\mathbf{1}}{2(d+1)} + \frac{d+2}{2(d+1)}|\psi\rangle\langle\psi|\,, \tag{3.89}$$

y la fidelidad para el clonado $1 \to 2$ copias de estados d dimensionales es

$$F_A = F_B = \frac{d+3}{2(d+1)}. \tag{3.90}$$

En general, es posible generar M estados clonados a partir de un estado desconocido que posee N copias, es decir $|\psi\rangle^{\otimes N}$ con $M > N$. Se define un proceso de clonado de estados puros, para el caso de $N \to M$ copias como,

$$(|\psi\rangle^{\otimes N}) \otimes (|R\rangle^{\otimes M-N}) \otimes |\mathcal{M}\rangle \to |\Psi\rangle\,, \tag{3.91}$$

donde $|\psi\rangle$ es el estado a ser copiado en un espacio de Hilbert $\mathcal{H}$, $|R\rangle$ es el estado de referencia elegido arbitrariamente en el mismo espacio de Hilbert $\mathcal{H}$ y $|\mathcal{M}\rangle$ es el estado de la máquina.

El proceso de clonado, ecuación (3.91), es definido por la máquina de clonado cuántico (MCC), la cual es un mapeo completamente positivo y que preserva la traza [58]. La eficiencia de una MCC se mide a través de la fidelidad de los estados clonados. La fidelidad se define para cada estado de salida ρ_j, $j = 1, ..., M$, de la máquina de clonado como

$$F_j = \langle\psi|\rho_j|\psi\rangle\,, \tag{3.92}$$

donde $|\psi\rangle$ es el estado inicial a ser copiado y ρ_j es el estado parcial del estado clonado j en el estado $|\Psi\rangle$ definido en la ecuación (3.91). En el caso, de un sistema de dimensión d, la menor

fidelidad para el proceso de clonado es $F_j = 1/d$, y es obtenida cuando ρ_j es un estado completamente mixto $\mathbf{1}/d$.

Es posible realizar una clasificación de las máquinas de clonado cuántico, en términos de la fidelidad de salida de las copias [58]. Una MCC es llamada universal cuando los estados son clonados con la misma fidelidad, independiente del estado a clonar $|\psi\rangle$. Cuando la fidelidad depende de los estados a copiar, la MCC es llamada estado dependiente. Una MCC es simétrica si los estados de salida clonados tienen la misma fidelidad, esto es, si $F_j = F_{j'}$ para todo $j, j' = 1, ..., M$. Finalmente, una MCC es llamada óptima si las fidelidades de los estados clonados son las máximas permitidas por la Mecánica Cuántica. De acuerdo a esta clasificación, la MCC de Bužek y Hillery [57] es universal, simétrica y óptima para qubits en el proceso de $1 \to 2$ estados clonados. La fidelidad óptima, para el caso de una máquina de clonado universal de estados de sistemas de dimensión d, en el proceso de clonado de $N \to M$ [59, 60], es igual a

$$F^{univ}_{N\to M}(d) = \frac{M(N+1) + (d-1)N}{M(N+d)}. \tag{3.93}$$

3.7. Criptografía Cuántica

El principal problema de los esquemas de criptografía clásica, como discutimos en la sección (2.3), está en la distribución en forma segura de la clave de encriptación y desencriptación del mensaje. En criptografía clásica, la seguridad en la distribución de la clave se basa en la dificultad para resolver ciertos algoritmos matemáticos. Los cuales no son insolubles y por lo tanto, la criptografía clásica no provee de seguridad incondicional en la transmisión de un mensaje secreto. Este problema es resuelto al utilizar la criptografía cuántica, que permite la distribución de la clave en forma segura. El principio de la criptografía cuántica consiste en la utilización de estados cuánticos no ortogonales. En este caso, la información (clave) es codificada en estados no ortogonales, los cuales no pueden ser identificados, copiados o divididos sin introducidir perturbaciones detectables en el estado [5].

El primer protocolo de distribución cuántica de claves fue propuesto por C. Bennett y G. Brassard en el año 1984, el cual es conocido como BB84 [61]. En el protocolo BB84 se utilizan estados bidimensionales y dos bases conjugadas para codificar el mensaje. Por ejemplo, si se utiliza la polarización del fotón como sistema cuántico, una de las bases estará compuesta por los estados $\{|H\rangle, |V\rangle\}$, es decir polarización horizontal y vertical del fotón, respectivamente. La otra base, consiste de los estados $\{|A\rangle, |D\rangle\}$ con polarización lineal a 45° y 135°, respectivamente, donde se tiene que

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \tag{3.94}$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle). \tag{3.95}$$

En este caso, se logra identificar completamente el estado si la medida se realiza en la base en que fueron preparados los estados. Sin embargo, si la medida se realiza en la base equivocada se obtienen resultados aleatorios con igual probabilidad. Tanto el emisor (Alice) y el receptor (Bob) del mensaje están de acuerdo en la siguiente asignación; los estados $|H\rangle$ y $|A\rangle$ codifican

el bit de valor "0" y los estados $|V\rangle$ y $|D\rangle$ codifican el bit de valor "1". Alice genera una secuencia aleatoria de bits que serán transmitidos a Bob, y aleatoriamente e independientemente para cada bit elige la base de medición. Esto implica que los fotones transmitidos tendrán uno de los estados $|H\rangle, |V\rangle, |A\rangle, |D\rangle$, con igual probabilidad de generación. Bob aleatóriamente e independientemente de Alice elige la base de medida para identificar el estado. En el 50 % de los casos las bases de Alice y Bob coinciden y los resultados de Bob están completamente de acuerdo con los bits de Alice. De manera de saber cuales de los resultados han sido correctos, Alice y Bob necesitan un canal clásico auxiliar para que se comuniquen sólo las bases utilizadas y no los resultados de las mediciones. Si las bases coinciden, Alice y Bob mantienen el bit. En otro caso, el bit es descartado. En este punto, Alice y Bob comparten una cadena de bits correspondientes a los resultados de la medidas realizadas en la misma base. Sin embargo, dado que: el canal cuántico posee ruido, la eficiencia de los detectores no es perfecta y debido a la posible presencia de un intruso en el canal de comunicación, la correlación de los datos de Alice y Bob es menor a la esperada.

De manera de establecer la clave criptográfica en forma segura, Alice y Bob monitorean el canal cuántico mediante la determinación de la tasa de error cuántico (QBER). Para ello Alice selecciona un subconjunto de n bits que comparte con Bob y comparan sus valores. Si en los bit seleccionados los errores son mayores que un cierto valor, ellos detienen el protocolo. Si la tasa de error cuántica está dentro de un valor esperado, Alice y Bob realizan reconciliación de la información y amplificación de la información. Finalmente, Alice y Bob comparten una clave criptográfica de m bits.

El principal problema de los protocolos de criptografía cuántica es determinar el máximo QBER que permite generar una clave de encriptación en forma segura.

- **Estrategias del espía**

Las pruebas de seguridad de los protocolos de criptografía cuántica consideran la existencia de un intruso (Eva) en el canal de comunicación de Alice y Bob. Se asume que Eva tiene la capacidad de controlar el entorno, y por lo tanto, todos los errores que registran Alice y Bob son debido a la interacción de Eva con el canal cuántico. La seguridad de los protocolos de criptografía cuántica se basan en que Eva en su intento por obtener información, está sometida a las leyes de la Mecánica Cuántica. Las posibles estrategias que Eva puede aplicar se clasifican en [62]: a) Ataques individuales, b) Ataques colectivos y c) Ataques generales.

- **Ataques individuales**

Aquí, se asume que Eva aplica la misma interacción a cada estado en forma individual, y mide su estado inmediatamente después de la interacción. Este tipo de ataque también es conocido como ataque incoherente. En este caso, Alice, Bob y Eva tienen información clásica en términos de variables aleatorias α, β, γ, respectivamente. Las leyes de la Mecánica Cuántica imponen restricciones sobre la distribución de probabilidad conjunta $\mathrm{P}(\alpha, \beta, \gamma)$, la cual permite determinar la información mutua entre Alice y Bob $I(A:B)$, y la información mutua entre Alice y Eva $I(A:E)$. Para este tipo de ataque usando comunicación en una dirección[3] $K_{\rightarrow}$, la tasa de

[3] La información siempre es transferida en una dirección predeterminada .

error cuántico está acotada por el límite de Csiszár-Körner [63],

$$K_{\rightarrow} \geq I(A:B) - I(A:E). \tag{3.96}$$

Este resultado indica que el protocolo es seguro si Bob posee más información que Eva. Para este tipo de ataque, el máximo QBER permitido para que Alice y Bob intercambien información en forma segura es de $QBER \cong 14{,}6\,\%$ [64]. Se ha demostrado [65] que en un ataque individual óptimo, Eva utiliza una máquina de copiado de estados llamada fase-covariante. La máquina de copiado fase-covariante permite copiar con igual fidelidad $F = 1 - QBER = 0{,}854$ todos los estados que pertenecen a un plano de la esfera de Bloch.

- **Ataques colectivos**

En este caso, Eva puede aplicar la misma interacción a cada estado cuántico y además, posee memoria cuántica. Esto implica que después de la interacción que le permite obtener información, puede esperar hasta que el proceso de reconciliación de la clave entre Alice y Bob haya finalizado. Esto le permite adaptar su estrategia en función de la información pública intercambiada entre Alice y Bob. Nuevamente la tasa de error cuántico, usando comunicación en una dirección, se determina de la relación

$$K_{\rightarrow} \geq I(A:B) - I(A:E), \tag{3.97}$$

donde las correlaciones clásicas entre Alice y Bob son cuantificadas por medio de la información mutua $I(A:B)$. Por otro lado, Eva posee variables cuánticas y la información mutua entre Alice y Eva se determina por medio del límite de Holevo[4] [66],

$$I(A:E) = S(\rho_E) - \sum_x p_x S(\rho_x), \tag{3.98}$$

donde $S(\rho)$ denota la entropía de Shannon del estado ρ, y $\rho_E = \sum_x p_x \rho_x$ es el estado cuántico que posee Eva. Bajo estas condiciones Shor y Preskill [67] determinarón que el protocolo criptográfico BB84 es seguro para una tasa de error cuántico máximo de un $QBER \simeq 11\,\%$.

- **Ataques generales**

En este tipo de ataque Eva puede realizar cualquier tipo de interacción. En comparación con los ataques anteriores no se conocen límites sobre la máxima tasa de error cuántico permitido para los ataques generales. Sin embargo, se ha demostrado [68] que si el protocolo criptográfico es simétrico en el uso del canal cuántico, entonces un ataque general no puede ser más eficiente que un ataque colectivo. Este resultado es conocido como teorema de Finetti.

El protocolo criptográfico BB84 como se ha indicado utiliza cuatro estados cuánticos y dos bases de medida. Un esquema similar al BB84 que utiliza seis estados y tres bases de medida es conocido como "six protocol" y se ha demostrado [69] que entrega mejores resultados que el protocolo BB84. En el año 1991 Ekert [70] publicó un esquema criptográfico que se basa en el teorema de Bell y que utiliza estados entrelazados como portadores de la información. En el año

[4] El límite de Holevo, entrega una cota superior para la capacidad de un canal cuántico con ruido para la transmisión de información clásica.

1992 Bennett [71] construyó un esquema criptográfico conocido como protocolo B92 que utiliza sólo dos estados no ortogonales. En el mismo año 1992 [72] se demostró que los protocolos BB84 y el protocolo de Ekert basado en el teorema de Bell son equivalentes. Este último resultado, ha motivado el estudio de esquemas criptográficos que utilizan el entrelazamiento de estados cuánticos para determinar los límites bajo los cuales los protocolos son seguros [62, 69]. Esto se justifica dado que un esquema criptográfico que utiliza entrelazamiento tiene su contraparte en un esquema criptográfico que no utiliza entrelazamiento pero los límites de seguridad son equivalente en los dos esquemas de criptografía.

3.8. Computación Cuántica

En el año 1982 R. Feymann [73] sugirió que el poder computacional de un computador cuántico podría ser mayor que el de los actuales equipos computacionales. Posteriomente, en el año 1985 D. Deutsch propuso una máquina cuántica de Turing [74] que permite resolver eficientemente problemas computacionales que no tienen una solución eficiente en un computador clásico o en una máquina probabilista de Turing. La máquina cuántica de Turing de Deutsch se compone de un conjunto de sistemas cuánticos bidimensionales (qubits) cuya evolución es dada por un conjunto de operaciones lógicas las cuales pueden ser implementadas mediante transformaciones unitarias.

Uno de los resultados más destacados al utilizar algoritmos cuánticos fue obtenido por Shor [75] en el año 1994, para encontrar la descomposición de un número de n dígitos en sus factores primos. El algoritmo cuántico de Shor requiere del orden de $O(n^2 log^d(n/e))$ operaciones básicas, en comparación con el mejor algoritmo clásico requiere de $O(2^{d\sqrt{nlogn}})$ operaciones básicas. Este resultado indica que los algoritmos cuánticos podrían ser exponencialmente más rapidos que los algoritmos clásicos. Otro resultado importante es el algoritmo cuántico de busqueda de Grover [76]. Por ejemplo, si se tiene un directorio telefónico que contiene N nombres ordenados en forma aleatoria y se requiere encontrar un número telefónico con una probabilidad de un 50 %, cualquier algoritmo clásico necesitará acceder a la base de datos como mínimo $N/2$ veces. Los sistemas cuánticos pueden estar en una superposición de estados y simultáneamente examinar múltiples nombres. Según el algoritmo de busqueda de Grover, ajustando adecuadamente las fases de varias operaciones, algunas operaciones se refuerzan mientras que otras interfieren aleatoriamente. Como resultado el número telefónico deseado puede ser obtenido en sólo $O(\sqrt{N})$ accesos a la base de datos.

Sin embargo, en la máquina cuántica de Turing se asume que: las operaciones unitarias pueden ser implementadas en forma perfecta, el conjunto de qubits está complemente aislado de influencias del medio ambiente y que en todo instante los estados del conjunto de qubits se encuentran en un estado puro. Por lo tanto, una implementación física de un computador cuántico requiere del perfecto control de la evolución coherente de un sistema de muchas partículas. Además, los estados cuánticos no pueden ser completamente aislados del medio ambiente, de manera que el requerimiento de una evolución controlada no puede ser satisfecha. Afortunadamente, las técnicas de corrección cuántica de errores puede ser desarrollada para estabilizar un computador cuántico contra imperfecciones en la implementación de las transformaciones unitarias y contra las influencias del medio ambiente [11].

Capítulo 4

Discriminación de Estados Cuánticos

En Teoría Cuántica de la Información se utiliza el estado de un sistema cuántico para codificar la información [4]. Sin embargo, el estado no es un observable en Mecánica Cuántica y por lo tanto, no podemos acceder directamente a la información codificada en el estado. Para lograr obtener la información es preciso determinar el estado cuántico. En el lenguaje de la Mecánica Cuántica, decimos que debemos determinar (cuando el estado es desconocido) o discriminar (cuando pertenece a un conjunto conocido de estados) el estado en el cual se encuentra el sistema.

Usualmente, la discriminación de estados cuánticos es introducida en el contexto de las comunicaciones cuánticas. Un usuario dispone de un conjunto de estados cuánticos para transmitir información. De manera de acceder a esta información, el receptor procede a identificar los estados. Sin embargo, esto puede ser realizado deterministicamente sólo si el conjunto de estados está compuesto por estados mutuamente ortogonales. En otro caso, la discriminación puede ser realizada con una cierta probabilidad de éxito. La optimización de esta probabilidad de éxito se puede realizar por medio de dos estrategias distintas de discriminación, conocidas como discriminación con mínimo error y discriminación sin ambigüedad, esto es, sin error.

De esta forma para discriminar o distinguir estados cuánticos no ortogonales debemos realizar una medida proyectiva o una medida generalizada. La aplicación de una medida proyectiva o generalizada dependerá del tipo de estados que deseamos discriminar. A continuación se analizan las características de las medidas proyectivas y posteriormente, las medidas generalizadas.

4.1. Medida Proyectiva

De los postulados de medición en Mecánica Cuántica sabemos que: una medición es descrita por un conjunto de operadores de medida $\{M_m\}$ que actúan en el espacio Hilbert del sistema. Además, de la condición de completitud, estos operadores de medida deben sumar el operador identidad. Esto se debe, a que cada operador tiene asociado un resultado de la medida con cierta probabilidad de ocurrir y las probabilidades de los posibles resultados deben sumar la unidad.

Un caso partícular de medida son las medidas proyectivas, también conocidas como medida de von Neumann. En una medida cuántica siempre se miden observables O, que son operadores

hermíticos y tienen una descomposición espectral de la forma

$$O = \sum_k \lambda_k |k\rangle \langle k| , \tag{4.1}$$

donde $\{|k\rangle\}$ es una base del espacio de Hilbert del sistema. Los proyectores $P_k = |k\rangle \langle k|$, expanden el espacio de Hilbert del sistema dado que

$$\sum_k P_k = \sum_k |k\rangle \langle k| = \mathbf{1}. \tag{4.2}$$

Los proyectores cumplen con las siguientes propiedades

$$P_k P_j = P_k \delta_{kj}, \tag{4.3}$$
$$P_k^2 = P_k. \tag{4.4}$$

Si el estado del sistema es $|\psi\rangle = \sum_k c_k |k\rangle$ y se realiza la medida de un observable O, se obtiene uno de los autovalores λ_k. Luego, el estado inmediatamente después de la medida es

$$\frac{P_k |\psi\rangle}{\sqrt{\langle\psi| P_k |\psi\rangle}}, \tag{4.5}$$

y la probabilidad p_k de este resultado es

$$p_k = |c_k|^2 = \| P_k |\psi\rangle \|^2 = \langle\psi| P_k P_k |\psi\rangle = \langle\psi| P_k |\psi\rangle . \tag{4.6}$$

En este caso, el número de resultados posibles es exactamente igual a la dimensión del espacio de Hilbert. Esto se debe, a que el operador identidad se descompone en términos de proyectores.

4.2. Medida Generalizada

En las medidas cuánticas generalizadas, se reeemplaza los operadores de proyección ortogonales P_k por los operadores de detección cuántica Π_k que no son necesariamente ortogonales. Por lo tanto, el número de resultados posibles puede ser mayor a la dimensión del espacio de Hilbert original, pero deben sumar el operador identidad

$$\sum_k \Pi_k = \mathbf{1}. \tag{4.7}$$

Si el estado inicial del sistema es descrito por un operador densidad ρ, la probabilidad de obtener el resultado k es

$$P(k|\rho) = Tr(\rho \Pi_k). \tag{4.8}$$

Cuando el estado ρ es un estado puro $|\psi\rangle$, la probabilidad de obtener k es

$$P(k|\psi) = \langle\psi| \Pi_k |\psi\rangle . \tag{4.9}$$

Como las probabilidades son números reales, los operadores de detección deben ser hermíticos. Además, las probabilidades son números positivos entre cero y uno. Esto implica que los valores de esperados de Π_k deben ser siempre valores no negativos [77]. Por esta razón, los operadores

de detección Π_k deben ser operadores de medida definidos positivos (POVM). Esta condición, se denota como $\Pi_k \geq 0$ y asegura la existencia del operador $\Pi_k^{1/2}$. Los operadores de detección, se pueden descomponer de la siguiente manera

$$A_k = U_k \Pi_k^{1/2}, \tag{4.10}$$

donde U_k es cualquier operador unitario. Por lo tanto, el operador de detección Π_k tiene la siguiente forma

$$\Pi_k = A_k^\dagger A_k. \tag{4.11}$$

De esta manera, si el estado inicial es ρ la probabilidad de obtener el resultado k puede ser expresada como

$$P(k|\rho) = Tr(A_k^\dagger A_k \rho), \tag{4.12}$$

y el estado inmediatamente después de la medida es

$$\rho'_k = \frac{A_k \rho A_k^\dagger}{P(k|\rho)}. \tag{4.13}$$

La presencia de la probabilidad en el denominador permite que el estado final este bien normalizado. Si no se registra la medida, entonces el operador densidad es una distribución de operadores densidad ρ_k correspondientes a los posibles resultados de la medida. Los cuales promediados por sus respectivas probabilidades $P(k|\rho)$, permiten expresar el estado final como

$$\rho' = \sum_k P(k|\rho)\rho'_k = \sum_k A_k \rho A_k^\dagger. \tag{4.14}$$

Por lo tanto, una medida generalizada es un caso particular de una operación cuántica (3.5). Bajo ciertas condiciones, la discriminación de estados se debe realizar en un espacio de Hilbert extendido a una mayor dimensión. En este caso el proceso se realiza mediante el teorema de Neumark [78]. Para ello, se debe insertar el espacio de Hilbert del sistema original, en un espacio de Hilbert con grados de libertad extra. Los grados de libertad adicionales pueden ser aportados por un sistema llamado ancilla. Luego, una transformación unitaria entrelaza los grados de libertad del sistema con los de la ancilla. Finalmente, después de la interacción, se puede realizar mediciones de von Neumann sobre el espacio de Hilbert extendido. Es posible seleccionar la transformación unitaria y la posterior medida de von Neumann, de manera de obtener un resultado k en el espacio de Hilbert extendido. La transformación resultante sobre el estado inicial es $A_k |\psi\rangle$, y corresponde a un elemento de los POVM en el espacio de Hilbert del sistema cuántico original. La posible extensión del espacio de Hilbert del sistema original $\mathcal{H}$, se puede realizar mediante el método de la suma directa de espacios de Hilbert $\mathcal{K} = \mathcal{H} \oplus \mathcal{A}$, o por medio del producto tensorial $\mathcal{K} = \mathcal{H} \otimes \mathcal{A}$ de los espacios de Hilbert. En el caso de la suma directa, un estado en $\mathcal{K}$ es una superposición de dos términos $|\Psi\rangle = |\psi\rangle + |\phi\rangle$, donde el primero de ellos pertenece al espacio de Hilbert original $\mathcal{H}$ y el segundo término corresponde al espacio de la ancilla $\mathcal{A}$. Por otro lado, en el producto tensorial de espacios, un estado en $\mathcal{K}$ es una superposición de productos de estados $|\psi\rangle |\phi\rangle$, donde cada producto, el primer miembro corresponde al espacio de Hilbert original $\mathcal{H}$ y el segundo miembro corresponde al espacio de Hilbert de la ancilla $\mathcal{A}$.

Las medidas generalizadas son utilizadas para la discriminación de estados cuánticos no ortogonales. A continuación se analizan la discriminación de estados con mínimo error y la discriminación de estados sin ambigüedad.

4.3. Discriminación con Mínimo Error

El caso más simple para el análisis de la discriminación de estados, es considerar sólo dos estados no ortogonales. En este caso, la estrategia óptima de discriminación con mínimo error conduce al límite de Helstrom [79]. Los estados no ortogonales son discriminados con la mínima probabilidad de error eligiendo apropiadamente los operadores de detección. Por ejemplo, si los estados son puros, denotados por $\{|\psi_+\rangle, |\psi_-\rangle\}$, y con probabilidad de preparación, η_+, η_-, respectivamente, la mínima probabilidad de error es

$$P_e(opt) = \frac{1}{2}\left(1 - \sqrt{1 - 4\eta_+\eta_-|\langle\psi_+|\psi_-\rangle|^2}\right). \tag{4.15}$$

Sin pérdida de generalidad, los estados pueden ser escritos como

$$|\psi_+\rangle = \cos\frac{\theta}{2}|-\rangle + \sin\frac{\theta}{2}|+\rangle, \tag{4.16}$$

$$|\psi_-\rangle = \cos\frac{\theta}{2}|-\rangle - \sin\frac{\theta}{2}|+\rangle. \tag{4.17}$$

En el caso, que las probabilidades de preparación sean iguales $\eta_+ = \eta_- = \frac{1}{2}$, la medida óptima es una medida de von Neumann y la mínima probabilidad de error es dada por

$$P_e(opt) = \frac{1}{2}(1 - \sin\theta), \tag{4.18}$$

la cual es obtenida rotando la base de medida de manera que los detectores midan en la base $\{|\omega_+\rangle, |\omega_-\rangle\}$ como en la figura (4.1).

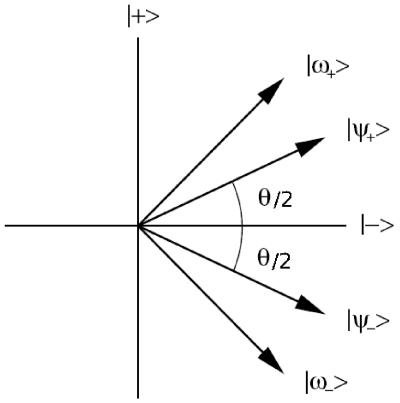

Figura 4.1: Discriminación con mínimo error de dos estados cuánticos no ortogonales.

En principio, podemos utilizar la base de medida denotada por $\{|+\rangle, |-\rangle\}$ para discriminar los dos estados. Sin embargo, al utilizar esta base la probabilidad de error es igual a 1/2 para cualquier par de estados $\{|\psi_+\rangle, |\psi_-\rangle\}$. Esta elección de la base representa el caso más desfavorable, esto se debe a que los dos estados tienen la misma amplitud de probabilidad en cada

uno de los estados de la base $\{|+\rangle, |-\rangle\}$. La óptima elección para la discriminación es considerar la base

$$|\omega_+\rangle = \frac{1}{\sqrt{2}}(|-\rangle + |+\rangle), \tag{4.19}$$

$$|\omega_-\rangle = \frac{1}{\sqrt{2}}(|-\rangle - |+\rangle). \tag{4.20}$$

Con la base $\{|\omega_+\rangle, |\omega_-\rangle\}$ se obtiene la mínima probabilidad de error (4.18) en la discriminación de los dos estados no ortogonales $\{|\psi_+\rangle, |\psi_-\rangle\}$. En esta base, por ejemplo, si los estados son ortogonales la probabilidad de mínimo error es igual a cero y por lo tanto, discriminamos con certeza los dos estados ortogonales.

En el caso que los estados sean no ortogonales, por ejemplo, si el estado fue preparado en $|\psi_+\rangle$ y medimos un observable con vectores propios $\{|\omega_+\rangle, |\omega_-\rangle\}$ podemos obtener $|\omega_+\rangle$ ó $|\omega_-\rangle$. Si obtenemos $|\omega_+\rangle$ en el proceso de medida, hay una probabilidad de éxito igual a $P_s = 1 - P_e(opt)$ que el estado haya sido preparado en el estado $|\psi_+\rangle$. Sin embargo, también tenemos una probabilidad de error igual a $P_e(opt)$, dado que la detección del estado $|\omega_+\rangle$ pudo ser originada por la componente del estado $|\psi_-\rangle$ sobre $|\omega_+\rangle$. De esta manera, no tenemos certeza en el proceso de medida, sólo sabemos que nuestra estrategia de discriminación tiene la mínima probabilidad de error. Discriminación con mínimo error en el límite de Helstrom fue demostrada experimentalmente por medio de pulsos laser, donde los dos estados a ser discriminados corresponden estados de polarización no ortogonales de los fotones generados [80].

En general, deseamos discriminar con el mínimo error posible N estados no ortogonales, con $N \geq 2$, siendo caracterizados por operadores densidad ρ_j, donde $j = 1, 2, ..., N$, con probabilidades de preparación η_j, respectivamente. En este caso, la estrategia de mínimo error es descrita en términos de un conjunto de operadores de detección hermíticos $\{\Pi_k\}$ llamados POVM (operadores de medida definidos positivos). El resultado de la medida denotada por k está asociada con el operador de detección Π_k. Los elementos de un POVM deben sumar el operador identidad, es decir,

$$\sum_k \Pi_k = \mathbf{1}. \tag{4.21}$$

Los operadores de detección $\{\Pi_k\}$ deben ser hermíticos y definidos positivos dado que las probabilidades de detección son números reales no negativos. Además, la suma de los operadores de detección debe ser igual al operador unidad, ya que la suma de todas las probabilidades de los posibles resultados de las medidas debe ser igual a la unidad.

La probabilidad que el receptor del estado encuentre el resultado k dado que fue enviado el estado ρ_j, es $P(k|j) = Tr(\Pi_k \rho_j)$. Luego, la probabilidad de discriminar el estado ρ_j correctamente es $P(j|j) = Tr(\Pi_j \rho_j)$. Por lo tanto, la probabilidad total de discriminación, es un promedio sobre todos los posibles resultados, la cual es igual a

$$P_s = \sum_{j=0}^{N-1} \eta_j Tr(\Pi_j \rho_j). \tag{4.22}$$

Por lo tanto, la probabilidad de error $P_e = 1 - P_s$, es igual a

$$P_e = 1 - \sum_{j=0}^{N-1} \eta_j Tr(\Pi_j \rho_j). \tag{4.23}$$

Las condiciones necesarias y suficientes para la estrategia de medida con mínimo error que deben satisfacer el conjunto de operadores de detección $\{\Pi_k\}$, fueron encontradas por Holevo [81] y Yuen [82], y son dadas por

$$\Pi_k(\eta_k\rho_k - \eta_j\rho_j)\Pi_j = 0 \qquad \forall j,k, \tag{4.24}$$

$$\sum_k \eta_k \Pi_k \rho_k - \eta_j\rho_j \geq 0 \qquad \forall j. \tag{4.25}$$

De manera de minimizar el error, Barnett y Croke demostraron [83] que se requiere que el operador

$$\Gamma = \sum_k \eta_k \Pi_k \rho_k, \tag{4.26}$$

sea hermítico y que se cumpla la condición (4.25). Para ello se considera otro conjunto de operadores de detección Π'_k. Luego, se restan las respectivas probabilidades de discriminación de los dos conjuntos de operadores, obteniendo

$$P_s - P'_s = \sum_j \eta_j Tr(\rho_j \Pi_j) - \sum_k \eta_k Tr(\rho'_k \Pi'_k), \tag{4.27}$$

$$= \sum_k Tr[(\Gamma - \eta_k\rho_k)\Pi'_k] \geq 0, \tag{4.28}$$

donde se ha utilizado la relación de completitud (4.21) para los operadores de detección del sistema primado. Los operadores de detección Π'_k deben ser positivos, dado que representan un conjunto de operadores de detección. Luego, si los operadores $\Gamma - \eta_k\rho_k$ son también positivos se tiene que $\sum_k Tr[(\Gamma - \eta_k\rho_k)\Pi'_k] \geq 0$. Por lo tanto, si se encuentra un POVM que satisface la relación (4.25) entonces los operadores de detección minimizan el error.

En el caso particular de la discriminación de dos operadores densidad, denotados por ρ_1 and ρ_2, la mínima probabilidad de error es

$$P_e(opt) = \frac{1}{2}(1 - Tr|\eta_2\rho_2 - \eta_1\rho_1|), \tag{4.29}$$

donde $|\Lambda| = \sqrt{\Lambda^\dagger \Lambda}$. Si los estados son puros, la expresión (4.29) se reduce al límite de Helstrom [79] dado por la expresión (4.15).

La estrategia óptima de medida puede ser derivada para un conjunto de N estados mixtos simétricos ρ_j, con probabilidad de preparación η_j [84]. El conjunto de estados simétricos satisface las siguientes condiciones

$$\rho_k = R^k \rho_0 R^{\dagger k}, \qquad k = 0, 1, ..., N-1, \tag{4.30}$$

$$R^N = \pm \mathbf{1}. \tag{4.31}$$

Es decir, a partir del estado ρ_0 y por medio de rotaciones de un operador unitario R podemos generar el resto de estados simétricos. Los operadores de medida $\{\Pi_k\}$ para la estrategia óptima de discriminación del conjunto de estados simétricos son

$$\Pi_k = \Phi^{-1/2}(\eta_k\rho_k)\Phi^{-1/2}, \tag{4.32}$$

$$\Phi = \sum_k \eta_k\rho_k, \tag{4.33}$$

donde ρ_k denota el k-ésimo estado a discriminar y el operador Φ es invariante ante la transformación R.

En particular, si un conjunto de N estados simétricos son puros, existe un operador unitario V tal que

$$|\psi_k\rangle = V|\psi_{k-1}\rangle = V^k|\psi_0\rangle, \tag{4.34}$$

$$|\psi_1\rangle = V|\psi_0\rangle, \tag{4.35}$$

donde $V^N = I$, con lo cual, aplicar N veces el operador unitario V es equivalente a aplicar el operador identidad sobre los estados. Si los estados simétricos tienen la misma probabilidad de preparación $\eta_k = 1/N$, los operadores óptimos para la discriminación con mínimo error son dados por [85]

$$\Pi_k = A_k^\dagger A_k = B^{-1/2}|\psi_k\rangle\langle\psi_k|B^{-1/2} \equiv |u_k\rangle\langle u_k|, \tag{4.36}$$

donde

$$B = \sum_{k=0}^{N-1} |\psi_k\rangle\langle\psi_k|. \tag{4.37}$$

Los estados $|u_k\rangle = B^{-1/2}|\psi_k\rangle$ en general, no están normalizados y son llamados estados de detección. Para este conjunto de estados la mínima probabilidad de error es

$$P_e = 1 - \frac{1}{N}\sum_{k=1}^{N} |\langle u_k|\psi_k\rangle|^2. \tag{4.38}$$

Cuando los estados de detección $|u_k\rangle$ son ortogonales, los operadores de detección son proyectores y la medida con mínimo error es una medición de von Neumann, en otro caso es una medida generalizada [86].

La estrategia para discriminar con mínimo error estados puros que son multiplemente simétricos, fue encontrada por Barnett [87]. En este caso, los estados son simétricos con respecto a más de una transformación unitaria. La discriminación con mínimo error de estados simétricos linealmente dependientes, ha sido realizada experimentalmente [88, 89, 90], utilizando óptica lineal para el proceso de discriminación.

Cuando tenemos un conjunto de N estados mixtos linealmente independientes, Eldar [91] demostró que la estrategia para discriminar con mínimo error es siempre una medida de von Neumann. Esto implica que los operadores de detección son mutuamente ortogonales $\Pi_j\Pi_k = \delta_{jk}\Pi_j$, donde $1 \leq j,k \leq N$, en el espacio de Hilbert del sistema cuántico. Por otro lado, para un conjunto de N estados mixtos, Qiu [92] obtuvo un límite inferior para la probabilidad de discriminación con mínimo error.

4.4. Discriminación de Estados sin Ambigüedad

En la discriminación de estados sin ambigüedad, se impone la condición que los estados deben ser identificados con certeza, es decir, sin error. Esto es posible, a expensas de introducir un resultado inconclusivo, es decir que no permite discriminar sin error los estados. Al obtener un resultado inconclusivo, el proceso de discriminación falla y no obtenemos información del estado que está siendo discriminado.

La discriminación sin ambigüedad óptima para dos estados puros, denotados por $\{|\psi_+\rangle, |\psi_-\rangle\}$, con igual probabilidad de preparación, fue obtenida por Ivanovic-Dieks-Peres (IDP) [93]. En este caso, detectamos los estados sin error pero tenemos un resultado inconclusivo. La probabilidad de la correcta detección de los estados es

$$P_{IDP} = 1 - |\langle\psi_+|\psi_-\rangle|. \tag{4.39}$$

El límite IDP (4.39) nos indica que cuando los estados son ortogonales, $\langle\psi_+|\psi_-\rangle = 0$, la probabilidad de discriminación sin ambigüedad es igual a la unidad y por lo tanto, siempre discriminamos correctamente los estados. Por otro lado, si los dos estados son iguales, $\langle\psi_+|\psi_-\rangle = 1$, entonces la probabilidad de discriminación sin ambigüedad es cero y por lo tanto, no es posible discriminar los estados sin error. En el caso que el producto interior asuma otro valor, por ejemplo $\langle\psi_+|\psi_-\rangle = 1/2$, la probabilidad de discriminación sin ambigüedad es igual a $P_{IDP} = 1/2$. Esto implica que en la mitad de los casos discriminamos sin error los estados y tenemos certeza del resultado de la medición. Sin embargo, se tiene una probabilidad de $1/2$ que la medida genere un resultado inconclusivo y el proceso de discriminación falla.

Para realizar la discriminación sin ambigüedad el sistema cuántico original $\mathcal{H}$, que es expandido por los estados $\{|\psi_+\rangle, |\psi_-\rangle\}$, se inserta en un espacio de Hilbert de mayor dimensión $\mathcal{K}$. Para ello, se agrega grados de libertad extra con un sistema auxiliar llamado ancilla, que inicialmente está en el estado $|0\rangle_a$. Ahora, el estado inicial del sistema compuesto está en uno de los estados $\{|\psi_+\rangle|0\rangle_a, |\psi_-\rangle|0\rangle_a\}$ y, aplicando una evolución unitaria condicional $\mathcal{U}$ sobre el espacio compuesto $\mathcal{K}$, tenemos

$$\mathcal{U}|\psi_+\rangle|0\rangle_a = \sin\frac{\theta}{2}[|0\rangle + |1\rangle]|0\rangle_a + \cos\frac{\theta}{2}\sqrt{1-\tan^2\frac{\theta}{2}}|1\rangle|1\rangle_a, \tag{4.40}$$

$$\mathcal{U}|\psi_-\rangle|0\rangle_a = \sin\frac{\theta}{2}[|0\rangle - |1\rangle]|0\rangle_a + \cos\frac{\theta}{2}\sqrt{1-\tan^2\frac{\theta}{2}}|1\rangle|1\rangle_a. \tag{4.41}$$

Es decir, el sistema compuesto evoluciona de manera diferente si el estado inicial es $|\psi_+\rangle|0\rangle_a$, ó $|\psi_-\rangle|0\rangle_a$, y este hecho, nos permite discriminar sin ambigüedad los estados. Para tal propósito, primero se realiza una medida proyectiva sobre el espacio de la ancilla. Si obtenemos $|0\rangle_a$ el proceso es conclusivo y los estados no ortogonales $\{|\psi_+\rangle, |\psi_-\rangle\}$ son proyectados a los estados ortogonales $\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$, respectivamente, con una probabilidad igual a $P_{IDP} = 1 - \cos\theta$. En este caso, los estados en el espacio de Hilbert original son ortogonales y por lo tanto, se pueden discriminar sin ambigüedad. Sin embargo, si en la medida en la ancilla obtenemos $|1\rangle_a$ el proceso es inconclusivo y este evento tiene una probabilidad igual a $P_I = \cos\theta$. En la figura (4.2) se representa este proceso.
Mediante la transformación unitaria $\mathcal{U}$ los estados que están originalmente en un plano son llevados a un espacio tridimensional. Esto se realiza sin modificar el producto interior de los estados

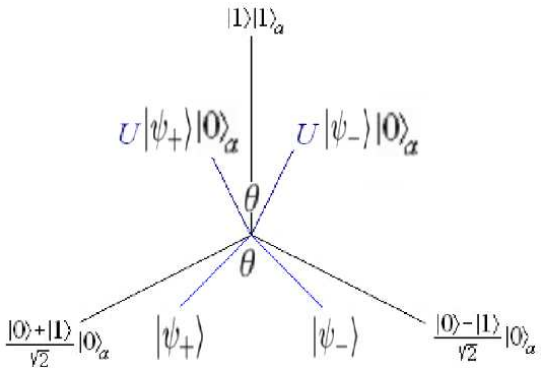

Figura 4.2: Discriminación sin ambigüedad de dos estados no ortogonales.

$\{|\psi_+\rangle, |\psi_-\rangle\}$. Finalizado el proceso, tenemos tres posibles resultados: un resultado inconclusivo, y los resultados asociados a la correcta discriminacion de $\{|\psi_+\rangle, |\psi_-\rangle\}$.

La discriminación sin ambigüedad de dos estados no ortogonales ha sido experimentalmente implementada cerca del límite de IDP [94]. Para ello se utilizó estados de polarización de pulsos atenuados de laser que se propagarón a través de fibra óptica. La discriminación sin ambigüedad en el límite de IDP, fue experimentalmente realizada a través de un interferómetro lo cual permitió registrar los eventos conclusivos e inconclusivos [95]. El resultado IDP fue generalizado por Jaeger y Shimony [96], la probabilidad óptima de discriminación sin ambigüedad de dos estados puros $\{|\psi_+\rangle, |\psi_-\rangle\}$ con probabilidades de preparación η_+, η_-, respectivamente, es dada por

$$P_s = 1 - 2\sqrt{\eta_+\eta_-}|\langle\psi_+|\psi_-\rangle|. \tag{4.42}$$

A continuación, se considera el caso de la discriminación sin ambigüedad de un conjunto de N estados puros y posteriormente, se analiza el caso de la discriminación de estados mixtos.

4.4.1. Discriminación de Estados Puros

En general, la discriminación sin ambigüedad de estados puros no ortogonales se describe por medio de los operadores de medida definidos positivos (POVM). Para ello, consideramos un conjunto de estados cuánticos no ortogonales $\{|\Psi_k\rangle\}$, con $k = 0, ..., N-1$, generados con probabilidades de preparación igual a η_k, respectivamente. Chefles [97] demostró que la discriminación sin ambigüedad se puede realizar si y sólo si, el conjunto de estados $\{|\Psi_k\rangle\}$ es linealmente independiente. La estrategia de discriminación se basa en la existencia de operadores A_k con $k = 0, \ldots, N-1$, asociados univocamente con los estados $\{|\Psi_k\rangle\}$ y del operador A_I, que representa al resultado inconclusivo, que satisfacen las siguientes relaciones

$$A_I^\dagger A_I + \sum_{k=0}^{N-1} A_k^\dagger A_k = \mathbf{1}, \tag{4.43}$$

esto implica, que la suma de las probabilidades de todos los posibles resultados debe ser igual a uno, y

$$\langle\psi_j| A_k^\dagger A_k |\psi_j\rangle = p_j\delta_{j,k}, \qquad \forall k, j = 0, \ldots, N-1, \tag{4.44}$$

lo que implica que cada operador de detección A_k tiene asociado el estado $|\Psi_k\rangle$, con una probabilidad de discriminación sin ambigüedad igual a p_k. Es posible establecer la forma del operador A_k dado que

$$A_k |\psi_k\rangle = p_k^{1/2} |\phi_k\rangle , \tag{4.45}$$

donde los estados $|\phi_k\rangle$ forman una base ortonormal para el espacio de Hilbert $\mathcal{H}$ del sistema. Además, desde la relación (4.44) vemos que el operador A_k aniquila el subespacio expandido por todos los estados $|\psi_j\rangle$ para $j \neq k$. Se denota este subespacio como $\mathcal{H}_k$, que tiene como complemento ortogonal un espacio expandido por sólo el estado $|\psi_k^{\perp}\rangle$. Por lo tanto, la forma del operador A_k es

$$A_k = \frac{p_k^{1/2}}{\langle \psi_k^{\perp} | \psi_k \rangle} |\phi_k\rangle \langle \psi_k^{\perp}|. \tag{4.46}$$

Cabe destacar que los estados $|\psi_k^{\perp}\rangle$ también son linealmente independientes. Ahora, el problema se reduce a determinar los valores de las probabilidades p_k, de manera que la probabilidad de éxito en la discriminación sea la máxima posible. La función que debemos maximizar es la probabilidad promedio de discriminación P_D, la cual es

$$P_D = \sum_{k=0}^{N-1} \eta_k p_k, \tag{4.47}$$

que debe satisfacer la condición que el operador

$$A_I^{\dagger} A_I \;=\; I - \sum_{k=0}^{N-1} A_k^{\dagger} A_k = I - \sum_{k=0}^{N-1} \frac{p_k |\psi_k^{\perp}\rangle\langle\psi_k^{\perp}|}{|\langle \psi_k | \psi_k^{\perp} \rangle|^2}, \tag{4.48}$$

sea un operador positivo.

La discriminación sin ambigüedad de tres estados no ortogonales fue analizada por Sun *et al.* [98]. Los tres estados linealmente independientes considerados tienen coeficientes reales. La extensión del espacio de Hilbert fue realizada por el método de la suma directa de espacios. La ancilla puede agregar una o dos dimensiones adicionales a las tres que poseen inicialmente los estados. Utilizando óptica lineal, Mohseni *et al.* [99] realizó la discriminación experimental de los tres estados no ortogonales. Donde se obtiene una probabilidad de éxito en la discriminación de un 55 %, que mejora sustancialmente el obtenido con una medida proyectiva de un 25 %.

La discriminación sin ambigüedad de un conjunto de N estados simétricos, con la misma probabilidad de preparación, fue analizada por Chefles y Barnett [100]. Un conjunto de N estados son simétricos si existe un operador unitario V tal que

$$|\psi_k\rangle \;=\; V |\psi_{k-1}\rangle = V^k |\psi_0\rangle , \tag{4.49}$$

$$|\psi_1\rangle \;=\; V |\psi_0\rangle , \tag{4.50}$$

donde $V^N = I$. Los estados puros $|\psi_k\rangle$, $k = 0, ..., N-1$, se asumen como linealmente independientes y por lo tanto, expanden todo el espacio de Hilbert del sistema. Dado que los estados

forman una base, esto implica que $V^N = I$ y, el operador unitario V puede ser expresado de la forma

$$V = \sum_{k=0}^{N-1} e^{2\pi ik/N} \left|\gamma_k\right\rangle \left\langle\gamma_k\right|, \tag{4.51}$$

donde $|\gamma_k\rangle$ es un vector propio del operador V con valor propio $e^{2\pi ik/N}$. Los estados a ser discriminados pueden ser expresados de la forma

$$|\psi_j\rangle = \sum_{k=0}^{N-1} e^{2\pi ijk/N} c_k \left|\gamma_k\right\rangle. \tag{4.52}$$

Los estados del complemento ortogonal $|\psi_j^{\perp}\rangle$ son también simétricos con respecto a la transformación V y tienen la siguiente forma

$$|\psi_j^{\perp}\rangle = \frac{1}{\sqrt{z}} \sum_{k=0}^{N-1} \frac{1}{c_k^*} e^{2\pi ijk/N} \left|\gamma_k\right\rangle, \tag{4.53}$$

donde z es un factor de normalización de los estados, igual a $z = \sum_k |c_k|^{-2}$. La probabilidad de discriminación óptima para un conjunto de estados simétricos es

$$P = N \times min|c_k|^2, \tag{4.54}$$

donde $min|c_k|^2$ corresponde al mínimo sobre todos los coeficientes c_k y se ha considerado que las probabilidades de preparación son iguales.

En general, la probabilidad de discriminar sin ambigüedad un conjunto de N estados puros $|\psi_k\rangle$, con probabilidades de preparación η_k, tiene un límite superior [101] dado por

$$P \leq 1 - \frac{1}{N-1} \sum_{j=0}^{N-1} \sum_{k=0, k\neq j}^{N-1} \sqrt{\eta_j \eta_k} \left|\left\langle\psi_j|\psi_k\right\rangle\right|. \tag{4.55}$$

4.4.2. Discriminación de Estados Mixtos

La discriminación sin ambigüedad de estados mixtos resulta ser más complicada de tratar que el caso de los estados puros. Dos estados mixtos ρ_0 y ρ_1, con probabilidades de preparación igual a η_0 y η_1 respectivamente, pueden ser discriminados sin ambigüedad si la intersección de sus respectivos soportes $\mathcal{K}_0$ y $\mathcal{K}_1$ es el conjunto vacío [102]. El soporte $\mathcal{K}$ de un operador es definido como el subespacio expandido por los autovectores con autovalores distintos de cero [103, 104].

La discriminación sin ambigüedad de los estados mixtos ρ_0 y ρ_1 se puede representar por medio de tres POVM, los cuales son denotados por $\{\Pi_0, \Pi_1, \Pi_I\}$. Dado que en la identificación de los estados no debemos tener errores asociados a la detección, se requiere que

$$Tr(\rho_0 \Pi_1) = Tr(\rho_1 \Pi_0) = 0, \tag{4.56}$$

y la probabilidad de éxito en la discriminación es

$$P = \eta_0 Tr(\rho_0 \Pi_0) + \eta_1 Tr(\rho_1 \Pi_1). \tag{4.57}$$

Una condición necesaria y suficiente para satisfacer la relación (4.56) es que el operador de detección Π_0 (Π_1) tenga soporte sólo en el subespacio $\mathcal{K}_0$ ($\mathcal{K}_1$). Esto ocurre si y sólo si el soporte de ρ_0 no es igual al soporte de ρ_1. Para maximizar la relación (4.57) debemos tener en cuenta la condición (4.56) y el vínculo que los operadores de detección Π_0, Π_1, y Π_I sean positivos y sumen el operador identidad. Por lo tanto, debemos variar los operadores positivos Π_0, Π_1, de manera de satisfacer la siguiente condición

$$I - \Pi_0 - \Pi_1 \geq 0. \tag{4.58}$$

Cuando las probabilidades de preparación de los estados mixtos ρ_0 y ρ_1 son iguales, y la intersección de los soportes es vacía, la óptima probabilidad de discriminación sin ambigüedad [104, 105] es

$$P = 1 - F(\rho_0, \rho_1), \tag{4.59}$$

donde F es la fidelidad definida por

$$F(\rho_0, \rho_1) = Tr\left(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}\right). \tag{4.60}$$

En general, Raynal y Lütkenhaus [104] determinarón la probabilidad de discriminación sin ambigüedad óptima para dos estados mixtos ρ_0 y ρ_1 con probabilidades de preparación η_0 y η_1, tal que sus soportes cumplan con la condición $\mathcal{K}_{\rho_0} \cap \mathcal{K}_{\rho_1} = \{0\}$. Para ello definen dos operadores $F_0 = \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ y $F_1 = \sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. Donde, la fidelidad F de los dos estados ρ_0 y ρ_1, se obtiene de $F = Tr(F_0) = Tr(F_1)$. En este caso, la probabilidad de discriminación sin ambigüedad óptima es

$$P^{opt} = 1 - \eta_0 - \eta_1 F^2 \quad \text{para} \quad \sqrt{\frac{\eta_1}{\eta_0}} \leq F, \tag{4.61}$$

$$P^{opt} = 1 - 2\sqrt{\eta_0\eta_1}F \quad \text{para} \quad F \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{1}{F}, \tag{4.62}$$

$$P^{opt} = 1 - \eta_1 - \eta_0 F^2 \quad \text{para} \quad \frac{1}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}}. \tag{4.63}$$

Cuando la intersección de los soportes de los estados ρ_0 y ρ_1 es el conjunto vacío, el espacio de Hilbert del sistema es expandido por los subespacios de soporte de ρ_0 y ρ_1. En general, la dimensión del espacio de Hilbert satisface la siguiente condición

$$dim(\mathcal{H}) = dim(\mathcal{K}_{\rho_0}) + dim(\mathcal{K}_{\rho_1}) - dim(\mathcal{K}_{\rho_0} \cap \mathcal{K}_{\rho_1}). \tag{4.64}$$

En el caso, que $\mathcal{K}_{\rho_0} \cap \mathcal{K}_{\rho_1} \neq 0$ se debe utilizar el procedimiento de reducción del subespacio en común [103]. El procedimiento de reducción del subespacio en común, puede ser generalizado al caso de la discriminación sin ambigüedad de N estados mixtos con probabilidades de preparación denotadas por η_k.

Un límite superior fue obtenido por Zhang [106] para la probabilidad de discriminación sin ambigüedad de un conjunto de N estados mixtos ρ_k con sus respectivas probabilidades de preparación η_k. Para ello, se define el subsespacio $Mix(\rho_k)$ como

$$Mix(\rho_k) = \mathcal{K}_{\rho_k} \cap \sum_{j \neq k} \mathcal{K}_{\rho_j}. \tag{4.65}$$

Luego, se divide ρ_k en dos partes, $\widetilde{\rho}_i$ y $\hat{\rho}_i$ de manera que $\mathcal{K}_{\hat{\rho}_i} = Mix(\rho_k)$ y

$$\mathcal{K}_{\widetilde{\rho}_i} \cap \mathcal{K}_{\hat{\rho}_i} = 0. \tag{4.66}$$

Finalmente, se considera la fidelidad de dos estados mixtos ρ_k y ρ_j como aparece en la ecuación (4.60) $F(\rho_k, \rho_j) = Tr\left(\sqrt{\sqrt{\rho_k}\rho_j\sqrt{\rho_k}}\right)$. Entonces, la probabilidad de éxito en la discriminación sin ambigüedad tiene un límite superior dado por

$$P \leq \sum_{k=0}^{N-1} \eta_k Tr(\widetilde{\rho}_k) - \sqrt{\frac{N}{N-1} \sum_{k \neq j}^{N-1} \eta_k \eta_j F^2(\widetilde{\rho}_k, \widetilde{\rho}_j)}. \tag{4.67}$$

La igualdad en la expresión (4.67) se tiene cuando los estados mixtos ρ_k no tienen soportes en común. En general, no es posible obtener un resultado analítico y el problema debe ser resuelto por métodos numéricos. Por ejemplo, Eldar *et al.* deducen las condiciones para maximizar la probabilidad de discriminación sin ambigüedad de un conjunto de N estados mixtos, llamados geométricamente uniformes [107].

Capítulo 5

Discriminación de Estados Simétricos

Una etapa fundamental en los protocolos de comunicaciones cuánticas es la discriminación de estados. Por ejemplo, la discriminación sin ambigüedad ha sido aplicada en: la concentración del entrelazamiento [97], teleportación cuántica de qudits [108], intercambio de entrelazamiento de qudits [109] y codificación densa [110]. Bajo ciertas condiciones los estados no ortogonales a ser discriminados forman un conjunto de estados simétricos linealmente independientes. La discriminación conclusiva de esta clase de estados permite la teleportación de estados cuánticos desconocidos con fidelidad unitaria y con cierta probabilidad de éxito. Un resultado similar se obtiene en los casos del intercambio del entrelazamiento y de la codificación densa. Es por este motivo que es importante la implementación experimental de estos esquemas, dado que permiten mejorar la capacidad de los protocolos de comunicación cuántica.

En este capítulo, proponemos un esquema experimental para discriminar estados simétricos no ortogonales linealmente independientes [111]. El esquema experimental utiliza óptica lineal y considera los procesos requeridos para generar, propagar y discriminar los estados. El esquema se puede configurar para implementar la discriminación sin ambigüedad y la discriminación con mínimo error, de estados simétricos y de dos estados mixtos.

Un conjunto de estados cuánticos es simétrico si los estados satisfacen las siguientes condiciones:

$$|\Psi_k\rangle = V|\Psi_{k-1}\rangle = V^k|\Psi_0\rangle, \tag{5.1}$$

$$|\Psi_1\rangle = V|\Psi_0\rangle, \tag{5.2}$$

para algún operador unitario V y para $k = 0, 1, ..., N-1$, donde los índices obedecen a la aritmética modular[1].

En general, para discriminar sin ambigüedad un conjunto de N estados no ortogonales, los estados deben ser linealmente independientes [97]. Por lo tanto, se considera estados simétricos

[1] En la aritmética modular, dado cualquier entero positivo x y n, x puede ser escrito en la forma $x = kn + r$, donde k es un entero no negativo que es el resultado de dividir x por n. El resto r está en el rango de valores $0, ..., n-1$, incluido sus extremos y es el valor que asume x en la suma modulo n [4].

no ortogonales linealmente independientes $\{|\Psi_k\rangle\}$, los cuales están definidos por:

$$|\Psi_k\rangle = Z^k|\Psi_0\rangle, \tag{5.3}$$

donde, $|\Psi_0\rangle$ es una superposición arbitraria pero conocida de estados en un espacio de Hilbert N-dimensional,

$$|\Psi_0\rangle = \sum_{n=0}^{N-1} c_n|n\rangle, \tag{5.4}$$

cuyos coeficientes obedecen la condición de normalización, es decir,

$$\sum_{n=0}^{N-1} |c_n|^2 = 1. \tag{5.5}$$

La acción del operador Z sobre un estado de la base $\{|n\rangle\}$ del espacio de Hilbert N-dimensional, es

$$Z|n\rangle = exp(\frac{2\pi in}{N})|n\rangle, \tag{5.6}$$

donde $Z^N = I$, es el operador identidad. Si las probabilidades de preparación η_k de los estados simétricos son iguales, es decir $\eta_k = 1/N$, la probabilidad óptima de discriminación sin ambigüedad de los estados simétricos [100], es dada por

$$P_{opt} = N \times |c_{min}|^2, \tag{5.7}$$

donde, $|c_{min}|$ es el menor coeficiente del estado $|\Psi_0\rangle$ en la base $\{|n\rangle\}$, es decir, $|c_{min}| \leq |c_n|$ para $n = 0, 1, ..., N-1$.

5.1. Discriminación de cuatro Estados Simétricos

Aquí, proponemos un esquema experimental para discriminar cuatro estados simétricos no ortogonales linealmente independientes, los cuales son denotados por $\{|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$. El esquema experimental utiliza óptica lineal y considera los procesos requeridos para generar, propagar y discriminar los estados. El esquema se puede configurar para implementar la discriminación sin ambigüedad y la discriminación con mínimo error. Mostramos que en los dos casos el esquema entrega la óptima probabilidad de éxito en el proceso de discriminación. Además, el esquema puede ser directamente generalizado para discriminar N estados simétricos no ortogonales linealmente independientes.

5.1.1. Discriminación sin Ambigüedad

Para realizar las operaciones necesarias en el proceso de discriminación sin ambigüedad de N estados simétricos no ortogonales se requiere utilizar a lo menos un espacio de Hilbert $(N+1)$-dimensional. Para suministrar la o las dimensiones adicionales al espacio de Hilbert N-dimensional expandido por los N estados simétricos, se puede considerar: un subespacio no utilizado por las partículas, un grado de libertad interno del sistema que no ha sido utilizado o agregar partículas extras. Las dimensiones extra que se utilizarán constituyen la "ancilla" del

sistema, la cual es necesaria para el proceso de discriminación sin ambigüedad. En este caso, se considera utilizar la polarización del fotón como ancilla en el proceso de discriminación, por lo que utilizaremos un grado de libertad interno del sistema cuántico. De esta manera, a los N estados simétricos $|\Psi_k\rangle$, donde $k = 0, ..., N-1$, se le agrega la ancilla que se encuentra en el estado inicial conocido denotado por $|0\rangle_a$. Por lo tanto, el estado inicial conjunto del sistema-ancilla es $|\Psi_k\rangle \otimes |0\rangle_a$. Luego, debemos aplicar una evolución unitaria condicional U sobre el espacio conjunto sistema-ancilla. La acción de la evolución unitaria condicional, sobre un espacio bidimensional de la ancilla y el sistema original, se puede expresar como:

$$U|\Psi_k\rangle \otimes |0\rangle_a = \sqrt{p_k}|u_k\rangle|0\rangle_a + \sqrt{1-p_k}|\phi_k\rangle|1\rangle_a. \tag{5.8}$$

La utilización de una ancilla que posee un espacio de Hilbert bidimensional es suficiente para nuestro proceso de discriminación sin ambigüedad. Esto se debe a que después de la evolución unitaria condicional U debemos realizar una medida proyectiva en el espacio de la ancilla. Los dos posibles resultados en el espacio de la ancilla, $\{|0\rangle_a, |1\rangle_a\}$, representan los eventos de éxito y falla, respectivamente, en el proceso de discriminación sin ambigüedad. De esta manera, si en la medida en la ancilla obtenemos $|0\rangle_a$ el proceso de discriminación es conclusivo y los estados $|\Psi_k\rangle$ son proyectados a los estados ortogonales $|u_k\rangle$ con una probabilidad igual a p_k. Por otro lado, si en la medida en la ancilla obtenemos $|1\rangle_a$ el proceso de discriminación falla y los estados $|\Psi_k\rangle$ son proyectados a los estados linealmente dependientes $|\phi_k\rangle$ con una probabilidad igual a $1-p_k$. Los estados ortogonales $|u_k\rangle$ se pueden discriminar con certeza y además, están univocamente asociados a los estados simétricos $|\Psi_k\rangle$, y por lo tanto, nos permite determinar en que estado simétrico fue preparado inicialmente el sistema cuántico. Los estados linealmente dependientes $|\phi_k\rangle$ representan el resultado inconclusivo dado que estados linealmente dependientes no pueden ser discriminados sin ambigüedad. Si elegimos adecuadamente la transformación unitaria U, es posible alcanzar la óptima probabilidad de discriminar conclusivamente los estados simétricos, con lo cual se tiene $p_k = N \times |c_{min}|^2$.

Para simplificar el análisis consideramos el caso de cuatro estados simétricos no ortogonales linealmente independientes, los cuales son denotados por $\{|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$. Estos estados son generados aplicando la transformación unitaria Z^k sobre el estado $|\Psi_0\rangle$, de manera que

$$|\Psi_k\rangle = Z^k|\Psi_0\rangle, \tag{5.9}$$

con $k = 0, 1, 2, 3$. El estado $|\Psi_0\rangle$ es conocido y esta definido por:

$$|\Psi_0\rangle = \sum_{n=0}^{3} c_n|n\rangle, \tag{5.10}$$

donde los coeficientes c_n obedecen la condición de normalización y son considerados como números reales. En general, estos coeficientes se pueden parametrizar en función de los ángulos θ_1, θ_2 y θ_3, de la siguiente forma,

$$c_0 = cos\theta_1, \tag{5.11}$$
$$c_1 = cos\theta_2 sin\theta_1, \tag{5.12}$$
$$c_2 = cos\theta_3 sin\theta_2 sin\theta_1, \tag{5.13}$$
$$c_3 = sin\theta_3 sin\theta_2 sin\theta_1, \tag{5.14}$$

donde hemos utilizado las coordenadas hiperesféricas. Esta parametrización de los coeficientes c_k permite generalizar fácilmente el esquema de discriminación a más de cuatro estados simétricos y además, como se verá más adelante facilita la implementación física del protocolo de discriminación.

La estrategia de discriminación se basa en la existencia de operadores de detección definidos positivos (POVM) que satisfacen la siguiente relación,

$$A_I^\dagger A_I + \sum_{k=0}^{N-1} A_k^\dagger A_k = \mathbf{1}, \tag{5.15}$$

donde $\mathbf{1}$ denota el operador identidad del espacio de Hilbert del sistema cuántico original, y

$$p_{k,j} = Tr(|\Psi_k\rangle \langle\Psi_k| A_j^\dagger A_j) = p_k \delta_{k,j}, \quad \forall \quad k,j = 0,...,N-1, \tag{5.16}$$

donde p_k es la probabilidad de discriminar sin ambigüedad el estado $|\Psi_k\rangle$.

Para construir la evolución unitaria condicional U recurrimos a las técnicas desarrolladas por He y Bergou [112]. Primero, se obtiene la forma diagonal de los operadores de detección inconclusiva $A_I^\dagger A_I$; esto se puede realizar cuando existe un operador unitario U_o actuando sobre el espacio de Hilbert inicial que nos entrega

$$U_o A_I^\dagger A_I U_o^\dagger = \sum_{i=0}^{N-1} \lambda_i |\alpha_i\rangle\langle\alpha_i|, \tag{5.17}$$

donde $|\alpha_i\rangle$ es un vector propio del operador $A_I^\dagger A_I$ con valor propio λ_i. Dado que el operador $A_I^\dagger A_I$ es positivo y sus valores propios están entre cero y uno. Por lo tanto, podemos definir los operadores hermíticos

$$A_I^\dagger = A_I = U_o^\dagger \sum_{i=0}^{N-1} \sqrt{\lambda_i} |\alpha_i\rangle\langle\alpha_i| U_o, \tag{5.18}$$

$$A_s^\dagger = A_s = U_o^\dagger \sum_{i=0}^{N-1} \sqrt{1-\lambda_i} |\alpha_i\rangle\langle\alpha_i| U_o. \tag{5.19}$$

Luego, la transformación unitaria en el espacio ampliado sistema-ancilla, toma la siguiente forma:

$$U = \begin{pmatrix} A_s & -A_I \\ A_I & A_s \end{pmatrix}, \tag{5.20}$$

donde

$$A_s^\dagger A_s = \sum_{k=0}^{N-1} A_k^\dagger A_k, \tag{5.21}$$

es el operador correspondiente al resultado conclusivo. El operador U no es único, puede tener tres formas similares [112]. Hemos asumido que el sistema de la ancilla es un sistema cuántico bidimensional, es decir un qubit, con base $\{|0\rangle_a, |1\rangle_a\}$ e inicialmente preparado en el estado $|0\rangle_a$.

Después de la evolución condicional del sistema compuesto sistema-ancilla, se debe medir en el espacio de la ancilla. Si el resultado de la medida sobre la ancilla es el estado $|0\rangle_a$, entonces determina la acción del operador $A_k^\dagger A_k$ sobre el sistema cuántico original y, el proceso de discriminación es conclusivo. En el otro caso, si la medida sobre la ancilla es $|1\rangle_a$, el elemento $A_I^\dagger A_I$ de los POVM ha actuado sobre el sistema cuántico y por lo tanto, el proceso de discriminación falla. La forma explícita de los operadores A_k fue encontrada por Chefles [97],

$$A_k = \frac{\sqrt{p_k}}{\langle \Psi_k^\perp | \Psi_k \rangle} |u_k\rangle\langle \Psi_k^\perp|, \tag{5.22}$$

donde los estados $|u_k\rangle$ forman una base ortogonal para el espacio de Hilbert en el espacio del sistema original $\mathcal{H}$. Los estados $|\Psi_k^\perp\rangle$ son llamados estados recíprocos; y p_k es la probabilidad de obtener el resultado k-ésimo, es decir $|\Psi_k\rangle$. Este operador es consistente con

$$A_k|\psi_k\rangle = \sqrt{p_k}|u_k\rangle. \tag{5.23}$$

Los estados recíprocos $|\Psi_k^\perp\rangle$ cumplen con la siguiente propiedad

$$\langle \Psi_k^\perp | \Psi_j \rangle = 0 \quad \forall \quad k \neq j, \tag{5.24}$$

y son definidos por

$$|\Psi_k^\perp\rangle = \frac{1}{\sqrt{q}} \sum_{r=0}^{N-1} \frac{1}{c_r^*} e^{\frac{2\pi i}{N} kr} |r\rangle, \tag{5.25}$$

donde $q = \sum_j |c_j|^{-2}$ [100]. Los estados recíprocos son también linealmente independientes y simétricos con respecto a la transformación Z. Luego, dado que el operador de detección conclusiva es

$$A_s^\dagger A_s = p_D \sum_k \frac{|\Psi_k^\perp\rangle\langle \Psi_k^\perp|}{|\langle \Psi_k^\perp | \Psi_k \rangle|^2}, \tag{5.26}$$

los operadores A_s y A_I en el caso de la discriminación sin ambigüedad de los estados simétricos $\{|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ son:

$$A_s = tan\theta_1 sin\theta_2 sin\theta_3 |0\rangle\langle 0| + tan\theta_2 sin\theta_3 |1\rangle\langle 1| + tan\theta_3 |2\rangle\langle 2| + |3\rangle\langle 3|, \tag{5.27}$$

$$A_I = \sqrt{1 - tan^2\theta_1 sin^2\theta_2 sin^2\theta_3}|0\rangle\langle 0| + \sqrt{1 - tan^2\theta_2 sin^2\theta_3}|1\rangle\langle 1| + \sqrt{1 - tan^2\theta_3}|2\rangle\langle 2|. \tag{5.28}$$

Aquí, hemos asumido que todas las probabilidades de preparación η_k son iguales, con valor $1/N$ y las probabilidades de discriminación son todas iguales a $p_k = p_D$ [100].

Después de aplicar la evolución condicional sobre el sistema compuesto sistema-ancilla, tenemos:

$$U|\Psi_k\rangle \otimes |0\rangle_a = \sqrt{p_D}|u_k\rangle|0\rangle_a + \sqrt{1 - p_D}|\phi_k\rangle|1\rangle_a. \tag{5.29}$$

De manera que cuando el resultado de la medida proyectiva sobre el espacio de la ancilla ha sido el estado $|0\rangle_a$, los estados simétricos no ortogonales $\{|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ son proyectados a los estados ortogonales $\{|u_0\rangle, |u_1\rangle, |u_2\rangle, |u_3\rangle\}$, respectivamente. En este caso, el proceso es conclusivo y este evento tiene una probabilidad igual a $p_D = 4 \times |c_{\min}|^2$ de ocurrir. Donde, el mínimo coeficiente es uno del conjunto $|c_{\min}| = \text{mín}\{|c_0|, |c_1|, |c_2|, |c_3|\}$. Si los ángulos θ_1, θ_2 y

θ_3, pertenecen a los siguientes intervalos $0 \leq \theta_1 \leq \pi/3$, $0 \leq \theta_2 \leq 0{,}3\pi$ y $0 \leq \theta_3 \leq \pi/4$ entonces, el mínimo coeficiente del estado $|\Psi_0\rangle$ es dado por $c_3 = \sin\theta_3 \sin\theta_2 \sin\theta_1$.

En el caso de una medida conclusiva, los estados ortogonales $|u_k\rangle$, se pueden obtener aplicando la transformada cuántica de Fourier tetra-dimensional actuando sobre los estados lógicos $|k\rangle$. Es decir, estos estados son dados por:

$$|u_k\rangle = \mathcal{F} \mid k\rangle = \frac{1}{2}\sum_{j=0}^{3} e^{i\pi jk/2}|j\rangle. \tag{5.30}$$

Dado que los estados ortogonales $|u_k\rangle$ son superposiciones de estados en la base lógica. Debemos aplicar la transformada de fourier inversa $\mathcal{F}^{-1}$ de manera de discriminar los estados $|\Psi_k\rangle$ en la base lógica, la cual en su representación matricial esta dada por:

$$\mathcal{F}^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}. \tag{5.31}$$

En términos de óptica lineal, la transformación (5.31) puede ser considerada como un divisor de haces simétrico de ocho puertos [113].

5.1.2. Esquema Experimental para la Discriminación sin Ambigüedad

En esta sección describimos un esquema experimental que permite una implementación óptima[2] de la discriminación sin ambigüedad de estados simétricos linealmente independientes, por medio de la utilización de sistemas ópticos. Para el protocolo de discriminación se requiere la generación de fotones individuales. En nuestro caso, se considera la generación de fotones gemelos en el proceso de conversión paramétrica espontánea descendente [114]. Uno de los fotones se denomina "signal" y el otro fotón gemelo se llama "idler", el fotón signal es utilizado para el protocolo de discriminación y el fotón "idler" es usado como testigo de la presencia del fotón "signal" [114, 115]. La presencia del fotón signal, permite generar uno de los estados no ortogonales $|\Psi_k\rangle$, mientras que el fotón "idler" al ser medido en coincidencia con el fotón "signal" permite asegurar la presencia de un único fotón en el esquema de discriminación.

El protocolo de discriminación está dividido en cuatro etapas: preparación de los estados simétricos $|\Psi_k\rangle$ definidos en la ecuación (5.3), evolución condicional conjunta U del sistema y la ancilla, medida proyectiva sobre la ancilla, y finalmente, en el caso de medida conclusiva, identificación del estado que pertenece a un conjunto de estados mutuamente ortogonales $|u_k\rangle$.

El esquema experimental para la discriminación de los estados simétricos utiliza óptica lineal. A continuación se describen los elementos ópticos necesarios para generar, propagar y discriminar los estados simétricos:

[2] Es óptimo en el sentido que el protocolo maximiza la probabilidad de éxito en el proceso de discriminación de los estados.

- **Placa de** $\lambda/2$ (HWP): Las placas de $\lambda/2$ o placas de media onda permiten rotar el vector de campo eléctrico alrededor de la dirección de propagación del haz [116]. Si inicialmente el vector de campo electrico es $\mathcal{E}$ y χ es el ángulo de rotación del vector campo eléctrico alrededor de la dirección de propagación, el vector de campo eléctrico final $\mathcal{E}'$ será

$$\mathcal{E}' = \mathcal{E} \begin{pmatrix} cos\chi & sin\chi \\ -sin\chi & cos\chi \end{pmatrix}. \tag{5.32}$$

  Por lo tanto, la matriz de transmisión T_R de la placa de $\lambda/2$ es

$$T_R = \begin{pmatrix} cos\chi & sin\chi \\ -sin\chi & cos\chi \end{pmatrix}. \tag{5.33}$$

- **Divisor de haz en polarización** (PBS): El campo electromagnético correspondiente a un vector de onda $\mathbf{k}$, que se propaga a lo largo del eje z, puede ser representado por un vector de amplitud de campo $\hat{\mathcal{A}}(\mathbf{k})$ tal que

$$\hat{\mathcal{A}}(\mathbf{k}) = \hat{a}_x \varepsilon_x + \hat{a}_y \varepsilon_y, \tag{5.34}$$

  donde $\hat{a}_x$, $\hat{a}_y$ son los operadores de aniquilación del fotón correspondientes a las componentes ortogonales de la polarización en las direcciones x e y, y ε_x, ε_y son los vectores unitarios de polarización.
  Suponemos que el haz de luz pasa a través del divisor de haz en polarización, la matriz de transmisión es representada por

$$T(\theta) = \begin{pmatrix} cos^2\theta & cos\theta sin\theta \\ cos\theta sin\theta & sin^2\theta \end{pmatrix}. \tag{5.35}$$

  La transformación $T(\theta)$ representa un polarizador lineal cuya dirección de polarización está inclinada en un ángulo θ con respecto al eje x.

- **Divisor de haz** (BS): Un divisor de haz o "beamsplitter" se puede describir mediante una transformación de dos operadores de entrada $\widehat{A}_{in}$ y $\widehat{A}_u$ en dos operadores de salida $\widehat{A}_r$ y $\widehat{A}_t$ [117]. La transformación toma la forma

$$\begin{pmatrix} \widehat{A}_r \\ \widehat{A}_t \end{pmatrix} = \begin{pmatrix} \sqrt{\epsilon} & \sqrt{1-\epsilon} \\ \sqrt{1-\epsilon} & \sqrt{\epsilon} \end{pmatrix} \begin{pmatrix} \widehat{A}_{in} \\ \widehat{A}_u \end{pmatrix}. \tag{5.36}$$

  En nuestro caso utilizaremos un divisor de haz 50/50 balanceado, esto implica que tanto el coeficiente de reflección $r = \sqrt{\epsilon}$ como el coeficiente de transmisión $t = \sqrt{1-\epsilon}$ son iguales dado que $\epsilon = 1/2$. De esta manera, la transformación del divisor de haz es

$$T_{BS} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{5.37}$$

- **Desfasador** (PS): Si denotamos por α_1 y α_2 los cambios de fase producidos en las componentes del campo eléctrico E_x y E_y respectivamente, que se produce en un haz de luz que se propaga en la dirección z a través de un desfasador, la diferencia de fase será

$$\delta = \alpha_2 - \alpha_1, \tag{5.38}$$

la cual es función de la frecuencia λ del haz. El campo eléctrico final $\mathcal{E}'$ es de la forma

$$\mathcal{E}' = [E_x e^{i\alpha_1} \;\; E_y e^{i\alpha_2}] = \mathcal{E} \begin{pmatrix} e^{i\alpha_1} & 0 \\ 0 & e^{i\alpha_2} \end{pmatrix}. \tag{5.39}$$

Dado que sólo la diferencia de fase de las componentes cartesianas del campo eléctrico son importantes, es posible expresar la relación entre $\mathcal{E}$ y $\mathcal{E}'$ de la forma

$$\mathcal{E}' = \mathcal{E} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}. \tag{5.40}$$

Luego, la matriz de transmisión del desfasador, la cual es denotada por T_c, es

$$T_c = \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}. \tag{5.41}$$

- **Espejo** (M): Los espejos introducen un cambio de fase de $\pi/2$ entre el haz reflejado y el haz incidente en el espejo, por lo que se debe incluir un factor i en cada reflección producida en los espejos.

Con los elementos ópticos descritos anteriormente es posible construir las diferentes etapas en el protocolo de discriminación de los estados simétricos.

La primera etapa del esquema de discriminación es la generación de los estados simétricos. Los cuatro estados simétricos considerados $|\Psi_k\rangle$ donde $k = 0, 1, 2, 3$, se codifican en los caminos de propagación de uno de los fotones gemelos. Así, los estados lógicos $|j\rangle$, con $j = 0, 1, 2, 3$, corresponden al $j-$ésimo camino de propagación del fotón, como se representa en la figura 5.1. Usando placas de retardación de media onda (HWP), divisor de haces en polarización (PBS) y desfasadores (PS) se pueden generar los cuatro estados simétricos. Las HWP_i rotan la polarización del fotón en un ángulo $\pi/2-\theta_i$. Luego, la polarización vertical de los fotones es reflejada en los PBS_i y esta componente es usada para definir el estado lógico $|i-1\rangle$. La polarización horizontal es transmitida y pasa a través de HWP_{i+1}. Aquí, nuevamente se repite este proceso, hasta obtener una superposición de los cuatro estados lógicos. Considerando que hemos elegido los valores de rotación de los ángulos de las HWP de tal manera que el mínimo coeficiente es $c_3 = \sin\theta_3 \sin\theta_2 \sin\theta_1$, finalmente hemos generado el estado $|\Psi_0\rangle$.

Se debe destacar que HWP_4 rota la polarización del camino de propagación cuatro desde polarización horizontal hasta polarización vertical. Por lo tanto, al final de la etapa de preparación de los estados simétricos, la polarización del fotón está factorizada de los estados de caminos (5.42), es decir, en todos los caminos de propagación la polarización permanece vertical, y tenemos el siguiente estado

$$|\Psi_0\rangle\,|0\rangle_a = i(c_0\,|0\rangle + c_1\,|1\rangle + c_2\,|2\rangle + c_3\,|3\rangle) \otimes |0\rangle_a\,, \tag{5.42}$$

donde los coeficientes c_n obedecen la condición de normalización y tienen la siguiente forma,

$$c_0 = cos\theta_1, \tag{5.43}$$
$$c_1 = cos\theta_2 sin\theta_1, \tag{5.44}$$
$$c_2 = cos\theta_3 sin\theta_2 sin\theta_1, \tag{5.45}$$
$$c_3 = sin\theta_3 sin\theta_2 sin\theta_1. \tag{5.46}$$

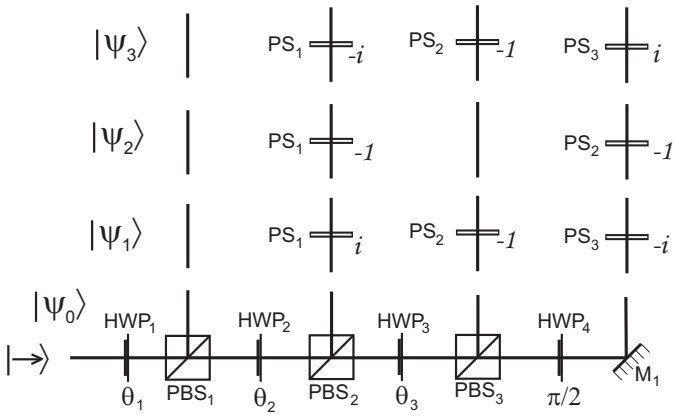

Figura 5.1: Esquema experimental para la generación de los estados simétricos de la ecuación (5.9). En todas las figuras PBS, HWP y PS, denotan divisor de haz en polarización, placas de media onda, y desfasador, respectivamente.

El siguiente estado simétrico $|\Psi_1\rangle$ se puede generar insertando las fases i, -1 y $-i$, en los caminos de propagación correspondientes a los estados lógicos $|1\rangle$, $|2\rangle$ y $|3\rangle$, respectivamente. De esta manera, el estado simétrico $|\Psi_1\rangle$ es

$$|\Psi_1\rangle |0\rangle_a = i(c_0 |0\rangle + ic_1 |1\rangle - c_2 |2\rangle - ic_3 |3\rangle) \otimes |0\rangle_a . \tag{5.47}$$

Los restantes estados simétricos $|\Psi_2\rangle$ y $|\Psi_3\rangle$, son generados insertando las correspondientes fases en cada camino de propagación del fotón, Fig. 5.1. Como se requiere una ancilla de dimensión dos para el proceso de discriminación, se utilizará la polarización del fotón como ancilla. Desde las ecuaciones (5.42) y (5.47) vemos que la polarización se encuentra inicialmente en el estado $|0\rangle_a$ y además, está factorizada de los estados simétricos.

El segundo paso en el protocolo de discriminación, es aplicar la evolución condicional (5.20) sobre el espacio ampliado sistema-ancilla. La transformación unitaria condicional U, es dada por

$$U = \begin{pmatrix} A_s & -A_I \\ A_I & A_s \end{pmatrix}. \tag{5.48}$$

La transformación unitaria U se puede expresar de la siguiente forma

$$U = A_s \otimes (|0\rangle_a \langle 0| + |1\rangle_a \langle 1|) + A_I \otimes (|1\rangle_a \langle 0| - |0\rangle_a \langle 1|), \tag{5.49}$$

donde los operadores A_s y A_I en el caso de la discriminación sin ambigüedad de los estados $\{|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ son:

$$\begin{aligned} A_s &= tan\theta_1 sin\theta_2 sin\theta_3 |0\rangle\langle 0| + tan\theta_2 sin\theta_3 |1\rangle\langle 1| + tan\theta_3 |2\rangle\langle 2| + |3\rangle\langle 3|, \\ A_I &= \sqrt{1 - tan^2\theta_1 sin^2\theta_2 sin^2\theta_3}\,|0\rangle\langle 0| + \sqrt{1 - tan^2\theta_2 sin^2\theta_3}\,|1\rangle\langle 1| + \sqrt{1 - tan^2\theta_3}\,|2\rangle\langle 2|. \end{aligned} \tag{5.50}$$

Por lo tanto, la transformación unitaria U definida por su acción sobre los estados lógicos y

sobre la ancilla en el estado inicial $|0\rangle_a$, tiene la siguiente forma:

$$\begin{aligned} U|0\rangle|0\rangle_a &= tan\theta_1 sin\theta_2 sin\theta_3|0\rangle|0\rangle_a + \sqrt{1-(tan\theta_1 sin\theta_2 sin\theta_3)^2}|0\rangle|1\rangle_a\,, \\ U|1\rangle|0\rangle_a &= tan\theta_2 sin\theta_3|1\rangle|0\rangle_a + \sqrt{1-tan^2\theta_2 sin^2\theta_3}|1\rangle|1\rangle_a\,, \\ U|2\rangle|0\rangle_a &= tan\theta_3|2\rangle|0\rangle_a + \sqrt{1-tan^2\theta_3}|2\rangle|1\rangle_a\,, \\ U|3\rangle|0\rangle_a &= |3\rangle|0\rangle_a\,. \end{aligned} \tag{5.51}$$

En este caso, la transformación unitaria U aplicada sobre los estados $|j\rangle|0\rangle_a$ con $j = 0, 1, 2, 3$, sólo cambia el estado de la polarización y mantiene el estado lógico inicial $|j\rangle$. Por lo tanto, la evolución unitaria condicional U corresponde a una rotación de la polarización (ancilla) dependiendo del camino de propagación del fotón (estados lógicos). La transformación unitaria U puede ser implementada con las placas de retardación de media onda HWP_5, HWP_6 y HWP_7 como aparece en la figura (5.2), dado que una HWP permite rotar la polarización en un ángulo dado. Por ejemplo, para el estado $|3\rangle|0\rangle_a$ no es necesario modificar la polarización y por lo tanto, no debemos introducir una HWP en el camino $|3\rangle$ del fotón. Por otro lado, para el estado $|2\rangle|0\rangle_a$, el ángulo de rotación de la polarización debe generar la siguiente transformación

$$U|2\rangle|0\rangle_a = |2\rangle \otimes (tan\theta_3|0\rangle_a + \sqrt{1-tan^2\theta_3}|1\rangle_a), \tag{5.52}$$

esto se puede obtener si el ángulo de rotación de la polarización que designamos por θ_7 es tal que $cos\theta_7 = \tan\theta_3$. Luego, el ángulo de rotación θ_7, para generar la transformación requerida en el proceso de discriminación sin ambigüedad, debe ser igual a $\theta_7 = \cos^{-1}(\tan\theta_3)$. De manera similar se deben elegir los ángulos de rotación de la polarización para los estados $|0\rangle|0\rangle_a$ y $|1\rangle|0\rangle_a$. Por lo tanto, el proceso de discriminación óptimo es obtenido cuando elegimos los ángulos de rotación de estas HWP como

$$\theta_5 = \cos^{-1}(\tan\theta_1 \sin\theta_2 \sin\theta_3), \tag{5.53}$$

$$\theta_6 = \cos^{-1}(\tan\theta_2 \sin\theta_3), \tag{5.54}$$

$$\theta_7 = \cos^{-1}(\tan\theta_3). \tag{5.55}$$

La tercera etapa del proceso de discriminación es la medida proyectiva sobre el espacio de la ancilla, la cual es implementada después de la aplicación de la evolución condicional U. En este caso, la medida proyectiva sobre la ancilla es la medida de la polarización del fotón en cada uno de los caminos de propagación del fotón $|j\rangle$ con $j = 0, 1, 2, 3$. Los posibles resultados en la medida proyectiva en la ancilla son $|0\rangle_a$ y $|1\rangle_a$, que corresponden a los estados de polarización vertical y polarización horizontal del fotón, respectivamente. Dado que un divisor de haz en polarización (PBS) permite separar las componentes vertical y horizontal de la polarización del fotón. Para realizar la medida proyectiva en la ancilla, se debe insertar divisores de haces en polarización PBS_4, PBS_5 y PBS_6 en los caminos de propagación 0, 1 y 2, respectivamente, como aparece en la figura (5.2). En el camino de propagación 4 no es necesario realizar una medida en la ancilla, ya que no fue modificada la polarización de este camino en la etapa de la aplicación de la transformación unitaria U. Se tiene una medida inconclusiva cuando el fotón con polarización horizontal es transmitido a través de alguno de los PBS. Por otro lado, en el proceso de discriminación se tiene éxito, si en la medida proyectiva se transmite la polarización

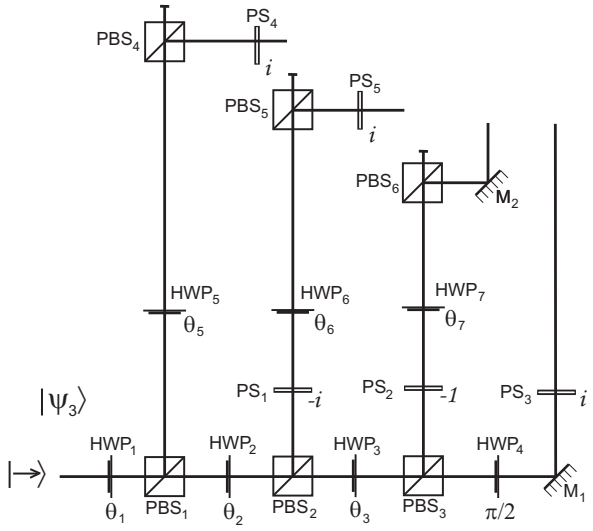

Figura 5.2: Evolución condicional de la ancilla (polarización) dependiendo del estado lógico (camino de propagación) es obtenida insertando una HWP en los caminos de propagación del fotón que corresponden a los estados lógicos $|0\rangle$, $|1\rangle$ y $|2\rangle$. La medida proyectiva sobre la ancilla se realiza insertando PBS en los mismos caminos de propagación, de manera que una medida no conclusiva se obtiene cuando el fotón es transmitido por uno de estos PBS.

vertical en los PBS y en este caso, los estados ortogonales del sistema original son

$$|u_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle), \tag{5.56}$$

$$|u_1\rangle = \frac{1}{2}(|0\rangle + i\,|1\rangle - |2\rangle - i\,|3\rangle), \tag{5.57}$$

$$|u_2\rangle = \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle), \tag{5.58}$$

$$|u_3\rangle = \frac{1}{2}(|0\rangle - i\,|1\rangle - |2\rangle + i\,|3\rangle). \tag{5.59}$$

Los estados ortogonales $|u_k\rangle$ con $k = 0, 1, 2, 3$, son superposiciones de los caminos de propagación, y están univocamente asociados con uno de los estados no ortogonales $|\Psi_k\rangle$. Por ejemplo, el estado simétrico $|\Psi_0\rangle$ tiene asociado el estado ortogonal $|u_0\rangle$ y la misma asignación se debe realizar con los restantes estados simétricos.

El último paso del protocolo de discriminación sin ambigüedad es determinar en cual de los estados ortogonales se ha proyectado el sistema. Para este propósito, es conveniente implementar la transformada inversa de Fourier tetra-dimensional que satisface $|k\rangle = \mathcal{F}^{-1}|u_k\rangle$ con $k = 0, 1, 2, 3$. Esto nos permite realizar la discriminación al detectar el fotón en el camino de propagación k. La transformada inversa de Fourier se puede implementar utilizando divisores de haz (BS), desfasadores (PS) y espejos (M), como aparece en la Fig. (5.3).
Para generar la transformada inversa de Fourier, primero mezclamos los caminos de propagación

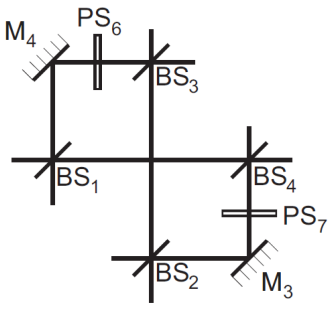

Figura 5.3: Implementación de la transformada inversa de Fourier en dimensión $N = 4$, utilizando óptica lineal.

0 y 2 en el divisor de haz BS1. Esto se describe por la siguiente matriz de transformación

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{5.60}$$

Si incluimos en una única transformación la acción de los BS1 y BS2, donde el BS1 mezcla los caminos 0 y 2, y el BS2 mezcla los caminos 1 y 3, se tiene

$$T_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}. \tag{5.61}$$

Luego, podemos ajustar las fases en los desfasadores PS_6 y PS_7 de manera de generar la transformación

$$T_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}. \tag{5.62}$$

Finalmente, si ahora incluimos en una única transformación la acción de los BS3 y BS4, donde el BS3 mezcla los caminos 0 y 1, y el BS4 mezcla los caminos 2 y 3, se tiene

$$T_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \tag{5.63}$$

Por lo tanto, la acción conjunta de las tres transformaciones T_1, T_2 y T_3, genera la transformada inversa de Fourier en una dimensión $N = 4$

$$\mathcal{F}^{-1} = T_3 T_2 T_1 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}. \tag{5.64}$$

De esta manera, la transformada de Fourier es implementada usando un interferómetro de ocho puertos [113]. La figura (5.4) presenta el esquema general para la discriminación sin ambigüedad de los cuatro estados estados simétricos no ortogonales. La figura (5.4) muestra las cuatro etapas para la discriminación: (I) Preparación de los estados $|\Psi_l\rangle$; (II) Evolución condicional del sistema compuesto; (III) Medida proyectiva; y (IV) detección.

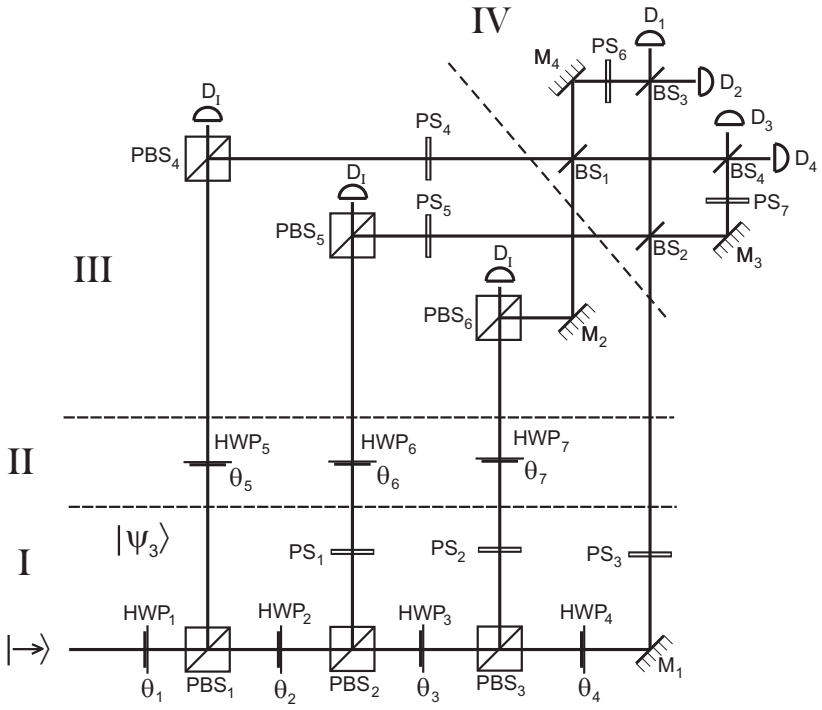

Figura 5.4: Esquema general para la discriminación de los cuatro estados simétricos: (I) Preparación de los estados $|\Psi_l\rangle$; (II) Evolución condicional del sistema compuesto; (III) Medida proyectiva; y (IV) detección.

En la figura (5.4), la detección del fotón en uno de los detectores D_1, D_2, D_3 y D_4 está en correspondiencia uno a uno con los estados $|\Psi_0\rangle$, $|\Psi_2\rangle$, $|\Psi_1\rangle$ y $|\Psi_3\rangle$ respectivamente. Por ejemplo, si el fotón es detectado en D_1 el estado en que fue preparado el sistema fue $|\Psi_0\rangle$. En este caso, la detección del estado $|\Psi_0\rangle$ es conclusiva, es decir, no hay error asociado en la detección. Sin embargo, el proceso tiene una probabilidad igual a $P_D = 4 \times |c_{min}|^2$ de ocurrir, la cual es la máxima posible para el conjunto de estados simétricos.

Dado que en este proceso se tiene tres posibles puntos donde se detecta el resultado inconclusivo, la discriminación sin ambigüedad se realiza en un espacio de Hilbert de dimensión siete. El protocolo descrito es fácilmente generalizado al caso de la discriminación de $N = 2^M$ estados simétricos. La tabla (5.1) detalla el número de elementos ópticos que se requieren en función del número de estados no ortogonales a discriminar. En el caso de otras dimensiones el protocolo también puede ser implementado. Para ello, se requiere la descomposición de la transformada inversa de Fourier en una dimensión N en términos de divisores de haces y placas de retardación. Por ejemplo, para el caso de $N = 3$ la transformada de fourier se puede descomponer [118], lo

Número de estados (2^M)	HWP	PBS	BS
4	7	6	4
8	15	14	12
16	31	30	32

Cuadro 5.1: Cantidad de componentes ópticos para el protocolo de discriminación para distintos números de estados no ortogonales a ser discriminados. La cantidad total de estos componentes es aproximadamente igual a $2^M(M+2)$. El número de otros componentes ópticos, tales como espejos y desfasadores, son del mismo orden.

cual puede ser mapeado en componentes ópticos lineales. En particular, la transformada cuántica de Fourier para $N = 8$ ha sido implementada usando óptica lineal [119] y fibras ópticas [120].

5.1.3. Discriminación con Mínimo Error

La estrategia de discriminación con mínimo error en la detección de los estados simétricos $|\Psi_k\rangle$, consiste en determinar el conjunto de operadores de detección [121] definidos por:

$$\Pi_k = \Phi^{-1/2}(\eta_k |\Psi_k\rangle \langle\Psi_k|)\Phi^{-1/2}, \tag{5.65}$$

$$\Phi = \sum_{k=0}^{3} \eta_k |\Psi_k\rangle \langle\Psi_k|, \tag{5.66}$$

donde Φ es el operador densidad formado por la superposición incoherente de los estados simétricos no ortogonales $|\Psi_k\rangle$, con probabilidades de preparación de los estados η_k, respectivamente. Como en el caso de la discriminación sin ambigüedad, se considera que la probabilidad de generación de los estados son iguales, es decir, $\eta_k = 1/4$. Al reemplazar los estados simétricos en la ecuación (5.66) obtenemos

$$\Phi = \sum_{n=0}^{3} c_n^2 |n\rangle \langle n|, \tag{5.67}$$

y por lo tanto,

$$\Phi^{-1/2} = \sum_{n=0}^{3} \frac{1}{c_n} |n\rangle \langle n|. \tag{5.68}$$

Luego, los operadores de detección en la expresión (5.65) son dados por:

$$\Pi_k = |u_k\rangle \langle u_k|, \tag{5.69}$$

donde los estados ortogonales $|u_k\rangle$ son los mismos que en el caso de la discriminación sin ambigüedad (5.59). Los cuales se pueden obtener aplicando la transformada cuántica de Fourier tetra-dimensional actuando sobre los estados lógicos $|k\rangle$. Es decir, estos estados son dados por:

$$|u_k\rangle = \mathcal{F} \mid k\rangle = \frac{1}{2} \sum_{j=0}^{3} e^{i\pi jk/2} |j\rangle. \tag{5.70}$$

Dado que los estados ortogonales $|u_k\rangle$ son superposiciones de estados en la base lógica. Debemos aplicar la transformada de fourier inversa $\mathcal{F}^{-1}$ de manera de discriminar los estados $|\Psi_k\rangle$ en la base lógica.

Finalmente, la probabilidad de discriminación con mínimo error el conjunto de estados simétricos es (4.38)

$$P^{\mathrm{ME}} = 1 - \sum_{k=0}^{3} \eta_k \left|\langle u_k|\Psi_k\rangle\right|^2 = 1 - \frac{1}{4}\left(c_0 + c_1 + c_2 + c_3\right)^2 . \tag{5.71}$$

El esquema general para la discriminación de los cuatro estados simétricos con mínimo error aparece en la figura (5.5). En este caso, a diferencia del protocolo de discriminación sin ambigüedad, sólo se requiere dos etapas: la generación de los estados simétricos $|\Psi_k\rangle$ y la detección de los estados. Por lo que, la II etapa no está incluida y los PBS en la III etapa deben ser reemplazados por espejos.

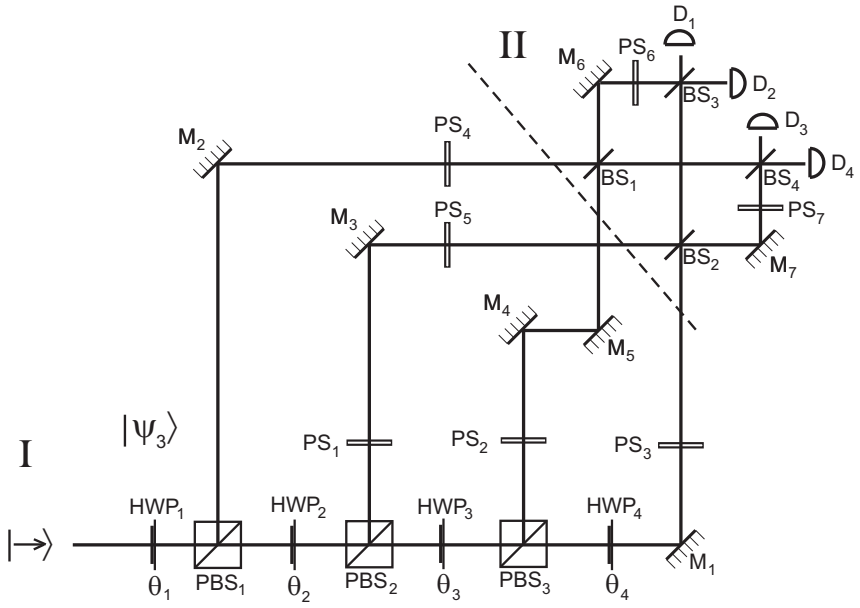

Figura 5.5: Esquema general para la discriminación de cuatro estados simétricos con mínimo error: (I) Etapa de preparación del estado $|\Psi_k\rangle$; y (II) detección.

En este caso, el proceso de discriminación se realiza sobre un espacio tetra-dimensional y la medida óptima corresponde a una medida proyectiva. Es decir, la discriminación con mínimo error se obtiene ajustado la base de medida, de manera que las detecciones de los estados se realice en la base que minimiza el error. El esquema general de discriminación con mínimo error aparece en la figura (5.5), donde la detección del fotón en los detectores D_1, D_2, D_3 y D_4 está en correspondencia uno a uno con los estados $|\Psi_0\rangle$, $|\Psi_3\rangle$, $|\Psi_2\rangle$ y $|\Psi_1\rangle$, respectivamente. Por ejemplo, si el fotón es detectado en D_1 el sistema fue preparado en el estado $|\Psi_0\rangle$. Sin embargo, la medida no es conclusiva ya que existe una probabilidad de error en la detección del estado $|\Psi_0\rangle$, la cual es la mínima posible P^{ME} en la discriminación de los estados simétricos.

La probabilidad de error (P^{ME}) en la discriminación con mínimo error y la probabilidad de obtener un resultado inconclusivo en la discriminación sin ambigüedad ($1 - P_D$) satisfacen la siguiente relación:

$$P^{\mathrm{ME}} \leq 1 - P_D, \tag{5.72}$$

$$1 - \frac{1}{4}\left(c_0 + c_1 + c_2 + c_3\right)^2 \leq 1 - 4c_3^2, \tag{5.73}$$

cuando c_3 es el menor de los coeficientes. Por lo tanto, la probabilidad de error en el esquema de discriminación con mínimo error es siempre menor o igual a la probabilidad de obtener un resultado inconclusivo en el esquema de discriminación sin ambigüedad.

5.2. Discriminación de dos Estados Mixtos

En esta sección se muestra como una modificación del esquema experimental puede ser utilizado para la discriminación de dos estados mixtos. Como en la sección anterior, se consideran esquemas para la discriminación sin ambigüedad y para la discriminación con mínimo error. Los estados mixtos considerados son superposiciones incoherentes de dos estados simétricos, los cuales están definidos por:

$$\rho_+ = \frac{1}{2}(|\Psi_0\rangle\langle\Psi_0| + |\Psi_2\rangle\langle\Psi_2|), \tag{5.74}$$

$$\rho_- = \frac{1}{2}(|\Psi_1\rangle\langle\Psi_1| + |\Psi_3\rangle\langle\Psi_3|). \tag{5.75}$$

En este caso, la intersección entre los soportes de los estados mixtos ρ_+ y ρ_- es vacía, lo que permite discriminar sin ambigüedad los estados mixtos. El soporte de los estados es definido como el subespacio expandido por los autovectores de un operador con autovalores distintos de cero [103, 104]. Los estados mixtos ρ_+ y ρ_- son llamados estados geometricamente uniformes [91, 105] dado al hecho que están conectados por la transformación unitaria Z , esto es

$$\rho_- = Z\rho_+ Z^\dagger, \tag{5.76}$$

donde la acción del operador unitario Z sobre un estado de la base $\{|n\rangle\}$, es

$$Z|n\rangle = exp(\frac{2\pi in}{N})|n\rangle, \tag{5.77}$$

en este caso, la dimensión del espacio de Hilbert del sistema es $N = 4$. Estos estados mixtos tienen la siguiente descomposición en la base lógica:

$$\rho_\pm = \sum_{n=0}^{3} c_n^2 \left|n\right\rangle \left\langle n\right| \pm c_0 c_2 \left(\left|0\right\rangle \left\langle 2\right| + \left|2\right\rangle \left\langle 0\right|\right) \pm c_1 c_3 \left(\left|1\right\rangle \left\langle 3\right| + \left|3\right\rangle \left\langle 1\right|\right). \tag{5.78}$$

Hemos asumido que los estados mixtos $\rho_\pm$ son generados con la misma probabilidad, es decir, $\eta_\pm = \frac{1}{2}$.

5.2.1. Discriminación sin Ambigüedad

En el caso de que probabilidades de preparación sean iguales, la óptima probabilidad de discriminación sin ambigüedad de los estados mixtos es dada por [104, 105]:

$$P^{\text{opt}} = 1 - F(\rho_+, \rho_-), \tag{5.79}$$

donde F es la fidelidad, definida por $F(\rho_+, \rho_-) = Tr[(\sqrt{\rho_-}\rho_+\sqrt{\rho_-})^{1/2}]$. En este caso, la óptima probabilidad de falla Q^{opt} es igual a la fidelidad. En la representación matricial los estados ρ_+ y ρ_- son:

$$\rho_\pm = \begin{pmatrix} c_0^2 & 0 & \pm c_0c_2 & 0 \\ 0 & c_1^2 & 0 & \pm c_1c_3 \\ \pm c_0c_2 & 0 & c_2^2 & 0 \\ 0 & \pm c_1c_3 & 0 & c_3^2 \end{pmatrix}, \tag{5.80}$$

y el operador $\sqrt{\rho_-}$ está definido de manera que $\rho_- = \sqrt{\rho_-}\sqrt{\rho_-}$, luego se tiene

$$\sqrt{\rho_-} = \begin{pmatrix} \frac{c_0^2}{\sqrt{c_0^2+c_2^2}} & 0 & -\frac{c_0c_2}{\sqrt{c_0^2+c_2^2}} & 0 \\ 0 & \frac{c_1^2}{\sqrt{c_1^2+c_3^2}} & 0 & -\frac{c_1c_3}{\sqrt{c_1^2+c_3^2}} \\ -\frac{c_0c_2}{\sqrt{c_0^2+c_2^2}} & 0 & \frac{c_2^2}{\sqrt{c_0^2+c_2^2}} & 0 \\ 0 & -\frac{c_1c_3}{\sqrt{c_1^2+c_3^2}} & 0 & \frac{c_3^2}{\sqrt{c_1^2+c_3^2}} \end{pmatrix}, \tag{5.81}$$

con lo cual, el operador $(\sqrt{\rho_-}\rho_+\sqrt{\rho_-})^{1/2}$ toma la forma,

$$(\sqrt{\rho_-}\rho_+\sqrt{\rho_-})^{1/2} = \begin{pmatrix} \frac{c_0^2(c_0^2-c_2^2)}{c_0^2+c_2^2} & 0 & \frac{c_0c_2(c_0^2-c_2^2)}{c_0^2+c_2^2} & 0 \\ 0 & \frac{c_1^2(c_1^2-c_3^2)}{c_1^2+c_3^2} & 0 & \frac{c_1c_3(c_1^2-c_3^2)}{c_1^2+c_3^2} \\ \frac{c_0c_2(c_0^2-c_2^2)}{c_0^2+c_2^2} & 0 & \frac{c_2^2(c_0^2-c_2^2)}{c_0^2+c_2^2} & 0 \\ 0 & \frac{c_1c_3(c_1^2-c_3^2)}{c_1^2+c_3^2} & 0 & \frac{c_3^2(c_1^2-c_3^2)}{c_1^2+c_3^2} \end{pmatrix}. \tag{5.82}$$

Por lo tanto, para los estados ρ_+ y ρ_- definidos por (5.78) la óptima probabilidad de discriminación sin ambigüedad es igual a

$$P^{\text{opt}} = 1 - Tr[(\sqrt{\rho_-}\rho_+\sqrt{\rho_-})^{1/2}] = 2(c_2^2 + c_3^2). \tag{5.83}$$

De manera que, la probabilidad de discriminación sin ambigüedad de los estados mixtos $\rho_\pm$, la cual es igual a $P^{\text{opt}} = 2(c_2^2+c_3^2)$, es mayor que la probabilidad de discriminación sin ambigüedad de los estados simétricos, igual a $P_D = 4 \times c_3^2$, dado que hemos asumido que los coeficientes c_k están ordenados en forma decreciente.

Para generar experimentalmente los estados mixtos ρ_+ y ρ_- considerados el esquema de la figura (5.6). En esta figura, hemos insertado en cada uno de los caminos de propagación un interferómetro desbalanceado en la configuración de Mach-Zehnder.

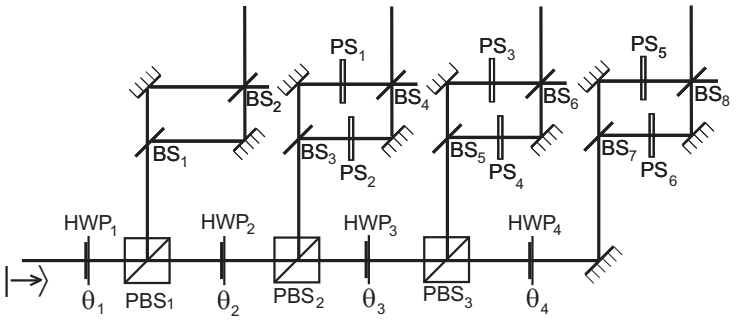

Figura 5.6: Esquema experimental para la generación de estados mixtos.

De la figura (5.6) si consideramos el camino 1 de propagación del fotón, el divisor de haz BS_3 genera una transformación T_1, luego el espejo y el desfasador PS_1 y PS_2 generan fases denotadas por f_1 y $f_{1'}$ en el camino superior e inferior del fotón, respectivamente. La transformación de los espejos junto con las fases PS_1 y PS_2 generan la transformación denotada por T_2, finalmente el divisor de haz BS_4 produce la transformación T_3. La transformación efectiva sobre el camino 1 del fotón es

$$\begin{aligned} T_3T_2T_1 &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} f_1 & 0 \\ 0 & f_{1'} \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \\ &= \frac{1}{2}\begin{pmatrix} f_1+f_{1'} & f_1-f_{1'} \\ f_1-f_{1'} & f_1+f_{1'} \end{pmatrix}. \end{aligned} \tag{5.84}$$

Si consideramos la transformación conjunta T_t de los 4 caminos de propagación del fotón, se tiene

$$T_t = \frac{1}{2}\begin{pmatrix} f_0+f_{0'} & f_0-f_{0'} & 0 & 0 & 0 & 0 & 0 & 0 \\ f_0-f_{0'} & f_0+f_{0'} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & f_1+f_{1'} & f_1-f_{1'} & 0 & 0 & 0 & 0 \\ 0 & 0 & f_1-f_{1'} & f_1+f_{1'} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & f_2+f_{2'} & f_2-f_{2'} & 0 & 0 \\ 0 & 0 & 0 & 0 & f_2-f_{2'} & f_2+f_{2'} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & f_3+f_{3'} & f_3-f_{3'} \\ 0 & 0 & 0 & 0 & 0 & 0 & f_3-f_{3'} & f_3+f_{3'} \end{pmatrix}. \tag{5.85}$$

Ahora, como el estado que ingresa el interferómetro desbalanceado es de la siguiente forma $|\Psi_i\rangle = \begin{pmatrix} 0 & c_0 & 0 & c_1 & 0 & c_2 & 0 & c_3 \end{pmatrix}^T$, entonces el estado a la salida del interferómetro desbalanceado, al considerar sólo el estado que ingresa a la segunda etapa de discriminación de los estados mixtos es

$$|\Psi_s\rangle = \begin{pmatrix} c_0(f_0-f_{0'}) & 0 & c_1(f_1-f_{1'}) & 0 & c_2(f_2-f_{2'}) & 0 & c_3(f_3-f_{3'}) & 0 \end{pmatrix}^T.$$

Al escribir el estado final en el espacio de Hilbert original, tenemos que

$$|\Psi_s\rangle = |\Psi_a\rangle + |\Psi_b\rangle, \tag{5.86}$$

donde el estado (5.86) no está normalizado y

$$|\Psi_a\rangle = c_0f_0|0\rangle + c_1f_1|1\rangle + c_2f_2|2\rangle + c_3f_3|3\rangle, \tag{5.87}$$

$$|\Psi_b\rangle = -(c_0f_{0'}|0\rangle + c_1f_{1'}|1\rangle + c_2f_{2'}|2\rangle + c_3f_{3'}|3\rangle). \tag{5.88}$$

Luego, si elegimos apropiadamente las fases f_i y $f_{i'}$ con $i = 0, 1, 2, 3$, podemos generar cualquiera de los cuatro estados simétricos. Además, como hemos considerado que la superposición de los estados $|\Psi_a\rangle$ y $|\Psi_b\rangle$ es incoherente, tenemos que

$$|i\rangle \left\langle j'\right| = 0, \forall i, j. \tag{5.89}$$

Por lo tanto, el estado final a la salida del interferometro desbalanceado es el siguiente estado mixto

$$\rho = \frac{1}{2}(|\Psi\rangle_a \langle\Psi| + |\Psi\rangle_b \langle\Psi|). \tag{5.90}$$

En el caso de la generación ρ_+ (ρ_-) se debe agregar las correspondientes fases de manera de generar los estados $|\Psi_0\rangle$ ($|\Psi_1\rangle$) y $|\Psi_2\rangle$ ($|\Psi_3\rangle$), en las ramas superiores e inferiores de los interferómetros. Por lo tanto, después de los interferómetros el estado generado es $\rho_+ \otimes |0\rangle_a\langle 0|$ o el estado $\rho_- \otimes |0\rangle_a\langle 0|$, donde $|0\rangle_a\langle 0|$ es el estado inicial de la ancilla, en este caso la polarización vertical del fotón.

Si utilizamos el esquema de la figura (5.4) para discriminar los estados mixtos ρ_+ y ρ_-, la probabilidad de la discriminación sin ambigüedad es igual a $P_D = 4 \times c_3^2$. Sin embargo, esta probabilidad es menor que la óptima $P^{\text{opt}} = 2(c_2^2 + c_3^2)$, dado que hemos asumido que los coeficientes c_k están ordenados en forma decreciente. La óptima probabilidad puede ser obtenida por medio de una operación de intercambio entre los caminos de propagación 1 y 2. Esta operación mapea el estado inicial de los estados mixtos $\rho_\pm$ en los estados mixtos $\tilde{\rho}_\pm$, dados por

$$\tilde{\rho}_\pm = U_{12}\rho_\pm U_{12}^\dagger = p_1 \left|\phi_{1_\pm}\right\rangle \left\langle\phi_{1_\pm}\right| + p_2 \left|\phi_{2_\pm}\right\rangle \left\langle\phi_{2_\pm}\right|. \tag{5.91}$$

La operación de intercambio efectúa un cambio de índices entre el camino 1 y el camino 2 no alterando los estados mixtos iniciales $\rho_\pm$. La transformación U_{12} entre los caminos de propagación 1 y 2 es

$$U_{12} = |0\rangle \langle 0| + |1\rangle \langle 2| + |2\rangle \langle 1| + |3\rangle \langle 3|, \tag{5.92}$$

La operación de intercambio U_{12} permite dejar los estados mixtos iniciales $\rho_\pm$ en una forma diagonal por bloques $\tilde{\rho}_\pm$, los cuales se expanden por los siguientes estados puros

$$\left|\phi_{1_\pm}\right\rangle = c_0'|0\rangle \pm c_2'|1\rangle, \tag{5.93}$$
$$\left|\phi_{2_\pm}\right\rangle = c_1'|2\rangle \pm c_3'|3\rangle, \tag{5.94}$$

donde

$$c_0' = \frac{c_0}{\sqrt{p_1}}, \qquad c_2' = \frac{c_2}{\sqrt{p_1}}, \qquad \text{con} \qquad p_1 = c_0^2 + c_2^2,$$
$$c_1' = \frac{c_1}{\sqrt{p_2}}, \qquad c_3' = \frac{c_3}{\sqrt{p_2}}, \qquad \text{con} \qquad p_2 = c_1^2 + c_3^2.$$

Luego, de manera de discriminar los estados mixtos $\tilde{\rho}_\pm$ se requiere discriminar sin ambigüedad los estados puros $\left|\phi_{1_\pm}\right\rangle$ y $\left|\phi_{2_\pm}\right\rangle$. Por ejemplo, para discriminar sin ambigüedad los estados $\left|\phi_{1_\pm}\right\rangle$ en el primer subespacio, primero se requiere aplicar la siguiente transformación unitaria sobre el sistema-ancilla

$$U = \begin{pmatrix} A_s & -A_I \\ A_I & A_s \end{pmatrix}, \tag{5.95}$$

de manera de generar la siguiente transformación

$$U\left|\phi_{1_\pm}\right\rangle|0\rangle_a = \sqrt{p_1}\,|u_\pm\rangle\,|0\rangle_a + \sqrt{1-p_1}\,|\gamma_\pm\rangle\,|1\rangle_a\,. \tag{5.96}$$

El proceso de discriminación al interior del primer subespacio tiene éxito, si después de una medida en la ancilla obtenemos $|0\rangle_a$. Esto se produce con una probabilidad igual a p_1 y los estados no ortogonales $|\phi_\pm\rangle$ son proyectados a los estados ortogonales $|u_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Por otro lado, si la medida en la ancilla se obtiene el estado $|1\rangle_a$ el proceso falla, ya que en este caso los estados $|\phi_\pm\rangle$ son proyectados a los estados linealmente dependientes $|\gamma_\pm\rangle$, con una probabilidad igual a $1-p_1$. En este caso, los operadores de detección conclusiva y detección inconclusiva son respectivamente dados por

$$A_s = \frac{c_2}{c_0}\,|0\rangle\langle 0| + |1\rangle\langle 1|\,, \tag{5.97}$$

$$A_I = \sqrt{1-\left(\frac{c_2}{c_0}\right)^2}\,|0\rangle\langle 0|\,, \tag{5.98}$$

y la transformación unitaria condicional es

$$U = A_s \otimes |0\rangle_a\langle 0| - A_I \otimes |0\rangle_a\langle 1| + A_I \otimes |1\rangle_a\langle 0| + A_s \otimes |1\rangle_a\langle 1|\,. \tag{5.99}$$

Ahora, el efecto que produce la transformación unitaria sobre los estados de entrada $|0\rangle|0\rangle_a$ y $|1\rangle|0\rangle_a$ es

$$U|0\rangle|0\rangle_a = \frac{c_2}{c_0}\,|0\rangle|0\rangle_a + \sqrt{1-\left(\frac{c_2}{c_0}\right)^2}\,|0\rangle|1\rangle_a\,, \tag{5.100}$$

$$U|1\rangle|0\rangle_a = |1\rangle|0\rangle_a\,. \tag{5.101}$$

Por lo tanto, sólo se genera una rotación en la polarización del camino 0. Como ya hemos visto en el caso de la discriminación de estados simétricos, la polarización se puede modificar introduciendo una placa de media onda en el respectivo camino de propagación del fotón. Luego, esta tranformación unitaria se implementa con la rotación de la polarización en un ángulo θ_5 en la HWP_5 de la figura (5.7). El ángulo de rotación θ_5 que se requiere debe satisfacer

$$cos\theta_5 = \frac{c_2}{c_0} = tan\theta_1 sin\theta_2 cos\theta_3, \tag{5.102}$$

luego, el ángulo de rotación de la polarización $\theta_5 = cos^{-1}(tan\theta_1 sin\theta_2 cos\theta_3)$.

La siguiente etapa en el proceso de discriminación es realizar una medida proyectiva en la ancilla. Los posibles resultados en la medida en la ancilla son $|0\rangle_a$ y $|1\rangle_a$, que corresponden a la polarización vertical y horizontal del fotón, respectivamente. Para realizar este proceso de medida insertamos el divisor de haz en polarización PBS_4 tal como aparece en la figura (5.7). La componente horizontal de la polarización es transmitida en el PBS_4, y posteriormente el fotón es detectado en D_I con lo cual obtenemos un resultado inconclusivo. En cambio, si el fotón tiene polarización vertical es transmitido generando uno de los siguientes estados ortogonales

$$|u_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{5.103}$$

La última etapa del proceso de discriminación es distinguir en el cual de los estados ortogonales $|u_{\pm}\rangle$ se ha proyectado el sistema. Para ello se inserta el divisor de haz BS_9 como aparece en la figura (5.7), que genera la transformación

$$T_{BS} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5.104}$$

esto nos permite detectar el fotón en la base lógica, ya que

$$|0\rangle = T_{BS}\,|u_{+}\rangle\,, \tag{5.105}$$
$$|1\rangle = T_{BS}\,|u_{-}\rangle\,. \tag{5.106}$$

Por lo tanto, si el fotón es detectado en D_1 (D_2), como aparece en la figura (5.7), el estado sin ambigüedad corresponde a $\left|\phi_{1_+}\right\rangle$ ($\left|\phi_{1_-}\right\rangle$). De manera similar se discrimina entre los estados $\left|\phi_{2_\pm}\right\rangle$ del segundo subespacio, pero en este caso el ángulo de rotación de la polarización es $\theta_6 = cos^{-1}(tan\theta_2 sin\theta_3)$.

La discriminación conjunta de los dos subespacios permite la discriminación de los estados mixtos $\rho_{\pm}$. El esquema general para la discriminación sin ambigüedad de los estados mixtos $\rho_{\pm}$ se representa en la figura (5.7). En la figura se presentan las etapas de: (I) Preparación de los estados $\rho_{\pm}$; (II) Evolución condicional del sistema compuesto; (III) Medida proyectiva; y (IV) detección de los estados.

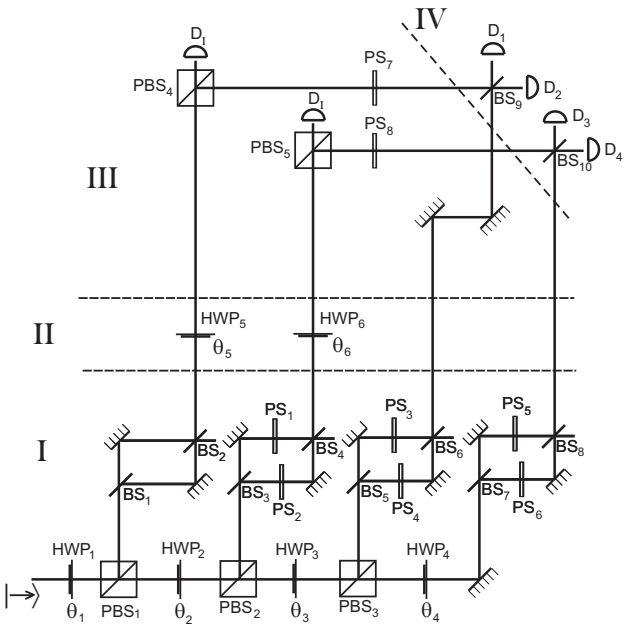

Figura 5.7: Esquema general para la discriminación sin ambigüedad de estados simétricos mixtos (5.75): (I) Preparación de los estados $\rho_{\pm}$; (II) Evolución condicional del sistema compuesto; (III) Medida proyectiva; y (IV) detección de los estados.

Este esquema permite la discriminación de dos pares independientes de estados puros; para cada par de estados tenemos que la probabilidad de discriminación sin ambigüedad es dada por $P_j^{\mathrm{UD}} = 2c_{\mathrm{mín}_j}'^2$, donde c_2' y c_3' corresponden a los mínimos coeficientes para los estados $\left|\phi_{1_\pm}\right\rangle$ y $\left|\phi_{2_\pm}\right\rangle$, respectivamente. Si el fotón es detectado en D_1 o D_3 (D_2 o D_4) el sistema fue preparado en ρ_+ (ρ_-). Por lo tanto, la probabilidad total de discriminación sin ambigüedad es dada por:

$$P^{\mathrm{UD}} = p_1 P_1^{\mathrm{UD}} + p_2 P_2^{\mathrm{UD}} = 2(c_2^2 + c_3^2) = P^{\mathrm{opt}}. \tag{5.107}$$

Si detectamos el fotón en los detectores D_I, obtenemos un resultado inconclusivo y la probabilidad para este evento es igual a $Q_F = 1 - P^{\mathrm{opt}}$. Aquí, el proceso de discriminación sin ambigüedad fue realizado en un espacio de Hilbert seis dimensional.

5.2.2. Discriminación con Mínimo Error

Ahora, consideramos la discriminación con mínimo error de los estados mixtos $\rho_\pm$, los cuales son superposiciones incoherentes de dos estados simétricos (5.75). Esto es equivalente a discriminar con mínimo error los estados mixtos $\tilde{\rho}_\pm$, esto es después de la operación de intercambio U_{12} de la ecuación (5.92). En este caso, el problema se reduce a la discriminación con mínimo error al interior de los subespacios generados por los estados $|\phi_{1\pm}\rangle$ y $|\phi_{2\pm}\rangle$. La probabilidad de detectar el fotón en el primer (segundo) subespacio $|\phi_{1\pm}\rangle$ ($|\phi_{2\pm}\rangle$) es igual a $p_1(p_2)$. Aquí, describimos el esquema para los estados $|\phi_{1\pm}\rangle$; lo mismo se aplica para los estados $|\phi_{2\pm}\rangle$, de manera que la probabilidad total para la discriminación con mínimo error es dada por:

$$P^{\mathrm{ME}} = p_1 P_1^{\mathrm{ME}} + p_2 P_2^{\mathrm{ME}}, \tag{5.108}$$

donde P_j^{ME} es la probabilidad de mínimo error para la discriminación de los estados $\left|\phi_{j_\pm}\right\rangle$, con $j = 1, 2$. Si consideramos el caso en el cual ρ_+ y ρ_- tienen igual probabilidad de preparación, entonces los estados $|\phi_{1+}\rangle$ y $|\phi_{1-}\rangle$ también tienen igual probabilidad de preparación. En este caso, los operadores de medida definidos positivos $\Pi_{1\pm}$, son dados por [121]:

$$\Pi_{1\pm} = \frac{1}{2}\Phi^{-1/2} \left|\phi_{1\pm}\right\rangle \left\langle\phi_{1\pm}\right| \Phi^{-1/2}, \tag{5.109}$$

donde

$$\begin{aligned} \Phi &= \frac{1}{2}\left|\phi_{1+}\right\rangle \left\langle\phi_{1+}\right| + \frac{1}{2}\left|\phi_{1-}\right\rangle \left\langle\phi_{1-}\right|, \\ &= c_0'^2 \left|0\right\rangle \left\langle 0\right| + c_2'^2 \left|1\right\rangle \left\langle 1\right|. \end{aligned} \tag{5.110}$$

Desde estas expresiones obtenemos que los operadores de proyección son

$$\Pi_{1\pm} = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, \tag{5.111}$$

con lo cual, estos operadores de detección son ortogonales y se pueden implementar mediante un divisor de haces. La probabilidad de discriminación con mínimo error para los estados $|\phi_{1\pm}\rangle$ se obtiene de

$$P_1^{\mathrm{ME}} = 1 - \frac{1}{2}[Tr(\Pi_{1+}\rho_{1+}) + Tr(\Pi_{1-}\rho_{1-})] = \frac{1}{2} - c_0' c_2'. \tag{5.112}$$

En forma similar, se obtiene que $P_2^{\mathrm{ME}} = \frac{1}{2} - c_1' c_3'$. Entonces, la probabilidad de error total es dada por la expresión

$$P^{\mathrm{ME}} = \frac{1}{2} - c_0 c_2 - c_1 c_3. \tag{5.113}$$

El esquema general para la discriminación de los estados mixtos simétricos con mínimo error aparece en la figura (5.8). El esquema experimental es similar al que aparece en la figura (5.7), pero la etapa II no esta incluida y los PBS en la etapa III deben ser reemplazados por espejos. Esto se debe a que no se requiere utilizar una ancilla para el proceso de discriminación. En este caso, el proceso de discriminación se realiza en un espacio de Hilbert tetra-dimensional.

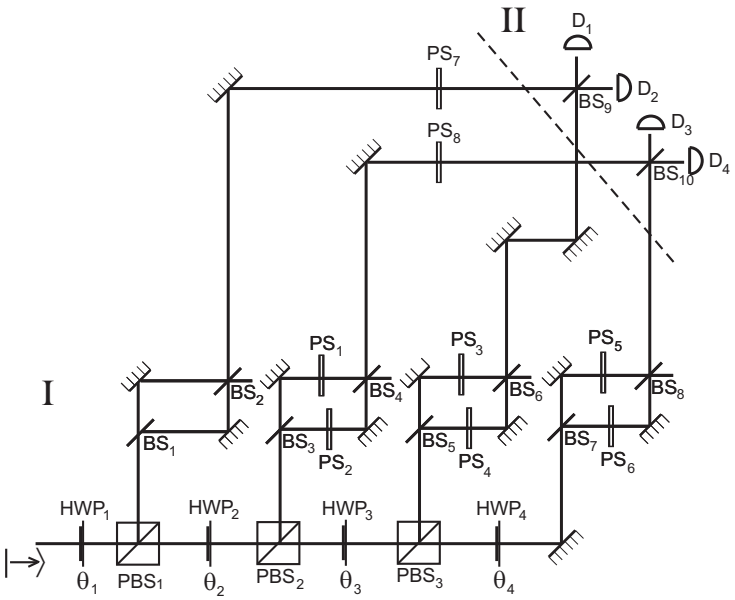

Figura 5.8: Esquema general para la discriminación de dos estados mixtos simétricos con mínimo error, ecuación (5.75): (I) Preparación del estado $\rho_{\pm}$; (II) detección de los estados.

Si detectamos el fotón en los detectores D_1 o D_3 (D_2 o D_4) el estado es identificado como ρ_+ (ρ_-). Sin embargo, estos resultados son ambiguos y la probabilidad de obtener un resultado incorrecto es dado por P^{ME}, lo cual coincide con la probabilidad de mínimo error. Esto también puede ser calculado con el límite de Helstrom [79], lo cual es determinado por medio de la siguiente expresión:

$$P_e^{\mathrm{opt}} = \frac{1}{2}(1 - Tr|\eta_+\rho_+ - \eta_-\rho_-|), \tag{5.114}$$

donde $|\Lambda| = \sqrt{\Lambda^\dagger \Lambda}$. En nuestro caso P_e^{opt} resulta ser igual a P^{ME} dado por la ecuación (5.113). Por lo tanto, la discriminación con mínimo error de los estados mixtos $\rho_{\pm}$ se realiza con la probabilidad de discriminación óptima dada por el límite de Helstrom (5.114).

5.3. Conclusiones

Hemos propuesto un esquema experimental para discriminar cuatro estados simétricos. El protocolo ha sido diseñado para obtener el valor optimo de medida conclusiva, el cual es dado por el límite de Chefles. El esquema considera un número reducido de elementos ópticos y puede ser generalizado facilmente al caso de 2^N estados simétricos. En el caso de otras dimensiones, el protocolo también funciona con la implementación óptica de la transformada inversa de Fourier. El esquema experimental se basa en la generación de estados de dos fotones en el proceso de conversión paramétrica espontánea descendente, lo cual nos permite alcanzar el valor óptimo en la discriminación conclusiva. El principal requerimiento experimental es la estabilización de los interferómetros en la configuración de Mach-Zehnder. También hemos considerado una versión modificada del esquema anterior para realizar la discriminación con mínimo error de los cuatro estados simétricos, en este caso nuestra propuesta también alcanza el valor óptimo. Con los cuatro estados simétricos considerados es posible construir dos estados mixtos, los cuales son superposiciones incoherentes de los estados simétricos. Modificando el esquema experimental para la discriminación de los estados simétricos es posible realizar la discriminación sin ambigüedad y con mínimo error de los estados mixtos. Los esquemas de discriminación propuestos para los estados simétricos y los estados mixtos en los procesos de discriminación sin ambigüedad y con mínimo error permiten alcanzar las máximas probabilidades de detección de los estados permitidas por la Mecánica Cuántica.

Capítulo 6

Distribución de Estados Cuánticos

La criptografía cuántica provee una forma segura para transmitir información entre dos o más usuarios. Los protocolos de criptografía cuántica son diseñados de manera que cualquier intruso en el canal de comunicación deje una marca en la llave usada para codificar la información. Por medio de esto, es posible decidir si una llave puede ser usada en forma segura o se debe generar una nueva.

En este capítulo se estudia la distribución de estados cuánticos de dimensión d entre tres usuarios. El protocolo funciona de manera similar al proceso de teleportación cuántica descrito en la sección (3.4.2). Sin embargo, en este caso se utilizan cuatro partículas en el protocolo. Además, se caracteriza el conjunto de estados maximalmente entrelazados que pueden ser usados como canal cuántico en el protocolo. También se analiza la seguridad del protocolo al considerar que se tiene un usuario deshonesto al interior del esquema de distribución de estados cuánticos. Como extensión del esquema anterior se considera el uso de un canal cuántico no ideal, es decir, estados que están parcialmente entrelazados. En este caso, relacionamos los protocolos para distribuir un qudit con el problema de la discriminación de estados. Esto se debe a que para finalizar el proceso de distribución de estados se debe discriminar estados no ortogonales, los cuales son estados simétricos linealmente independientes. Esto permite la formulación de un protocolo, donde la recuperación del estado se logra con una cierta probabilidad de éxito.

6.1. Introducción

La distribución clásica de secretos tiene su origen en los trabajos de Shamir y Blakley, que independientemente el 1979 propusieron un esquema para codificar un secreto entre n usuarios [122, 123]. La propuesta de Shamir [122] consiste en dividir la información "D", que constituye los datos secretos, entre n partes de manera que la información "D" es facilmente reconstruida por k usuarios. Sin embargo, el conocimiento completo de $k-1$ de las partes no revela absolutamente nada acerca de la información secreta "D". Este procedimiento permite la construcción de esquemas robustos para el manejo de "claves" en sistemas criptográficos. Este esquema de distribución clásica de secretos, puede funcionar con seguridad y confiabilidad aún cuando se destruye parte de la información y la violación de seguridad expone sólo una de las partes de la información en el esquema. Esto permite que un usuario deshonesto en el esquema de distribución de secretos, no pueda reconstruir por si sólo la información de la clave "D" y debe

someterse al acuerdo de k usuarios para obtener la información.

Recientemente, la criptografía cuántica ha sido extendida al caso de distribución de secretos cuánticos. Esta generalización se origina cuando examinamos la versión clásica del problema de distribución de secretos, esto es, la distribución de información sensible entre muchas partes de manera que una parte deshonesta no puede tener acceso a la información completa. En el caso cuántico el secreto a ser distribuido puede ser una clave clásica [124] o un estado cuántico. En este contexto, Hillery et al. [125] propusieron un protocolo para la distribución de estados cuánticos utilizando un estado GHZ[1]. Este protocolo nos permite distribuir un estado cuántico de dimensión dos entre tres usuarios. El estado distribuido puede ser recuperado por una de las partes si las restantes cooperan, al entregarle la información de sus respectivas medidas. La utilización de estados entrelazados de mayor dimensión también ha sido analizada [126, 127].

6.2. Protocolo de Distribución de Estados Cuánticos

Nuestro principal objetivo en esta sección es la distribución de un estado cuántico desconocido entre tres usuarios. Uno de los usuarios puede recuperar el estado cuando los dos restantes usuarios están de acuerdo en cooperar. Esta cooperación entre los usuarios, consiste en compartir la información clásica que cada uno de ellos obtiene, mediante mediciones cuánticas locales de sus correspondientes partículas.

Para implementar este protocolo se considera tres usuarios en puntos distantes y cuatro qudits. El espacio de Hilbert de cada qudit es expandido por la base de estados $\{|i\rangle_k\}$, donde el subíndice $k = 1, 2, 3, 4$, denota un qudit particular y el índice $i = 0, ..., d-1$ corresponde a d estados ortogonales. Se considera que la dimensión d es un número primo o una potencia de un número primo. En este caso, los valores de los índices i están en Z_d, los enteros modulo d, y forman un campo algebraico finito[2].

La información que se desea proteger y distribuir entre los usuarios autorizados está codificada en los coeficientes c_k del estado de la partícula 1, el cual corresponde a una superposición de d estados de la siguiente forma,

$$|\psi\rangle_1 = \sum_{k=0}^{d-1} c_k |k\rangle_1. \tag{6.1}$$

Esta información será distribuida en tres partes, para ello se utiliza como canal cuántico el estado dado por:

$$|A\rangle_{234} = \sum_{p,q,r=0}^{d-1} A_{pqr} |p\rangle_2 \otimes |q\rangle_3 \otimes |r\rangle_4. \tag{6.2}$$

Donde el qudit uno y dos pertenecen al primer usuario y los qudit tres y cuatro pertenecen a la segundo y tercer usuario, respectivamente. Al distribuir el estado en varias partes, la seguridad del protocolo aumenta. En este esquema, es posible detectar a un posible intruso externo al canal

[1] Un estado GHZ (Greenberger-Horne-Zeilinger) es un estado de tres partículas maximalmente entrelazado de la forma $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

[2] Forman un grupo Abeliano con respecto a las operaciones de suma y multiplicación.

de comunicación y también a un posible deshonesto al interior del protocolo. Además, el canal $|A\rangle_{234}$ es simétrico ante el intercambio de las partículas tres y cuatro, por cuanto el protocolo no cambia si reconstruye el estado el segundo o el tercer usuario.

El estado inicial del sistema compuesto es de la siguiente forma,

$$|\psi\rangle_1 \otimes |A\rangle_{234} = \sum_{p,q,r,k=0}^{d-1} A_{pqr} c_k |k\rangle_1 \otimes |p\rangle_2 \otimes |q\rangle_3 \otimes |r\rangle_4, \tag{6.3}$$

el cual se puede expresar, utilizando la base generalizada de Bell $|\Psi_{m,k}\rangle_{12}$ en las partículas uno y dos, como

$$|\psi\rangle_1 |A\rangle_{234} = \sum_{m,k=0}^{d-1} \frac{\omega(-mk)}{\sqrt{d}} |\Psi_{m,k}\rangle_{12} \sum_{p,q,r=0}^{d-1} \omega(-mp) A_{pqr} c_{k+p} |q\rangle_3 |r\rangle_4, \tag{6.4}$$

donde $\omega(k) = \exp\left(\frac{2\pi i}{d} k\right)$ son las raíces de la unidad y los estados $|\Psi_{a,b}\rangle_{12}$ son definidos por:

$$|\Psi_{a,b}\rangle_{12} = \frac{1}{\sqrt{d}} \sum_k \omega(ka) |k\rangle_1 |k-b\rangle_2. \tag{6.5}$$

Estos estados forman una base maximalmente entrelazada para el espacio de Hilbert de los qudit uno y dos, los cuales son una generalización de la base de Bell en el caso de dos qubits.

El protocolo de distribución de estados funciona de manera similar al proceso de teleportación cuántica. Al medir en la base de Bell en los qudits uno y dos del estado compuesto (6.4), se determinan los valores de m y k. Luego, asociamos los coeficientes c_k del estado original $|\psi\rangle_1$ al estado compuesto de los qudits tres y cuatro, esto es:

$$\frac{1}{\sqrt{d}} \sum_{p,q,r=0}^{d-1} \omega(-mp) A_{pqr} c_{k+p} |q\rangle_3 \otimes |r\rangle_4. \tag{6.6}$$

En una medida en el qudits tres se obtiene el valor de q y se proyecta el qudit cuatro al siguiente estado

$$\frac{1}{N_{m,k,q}\sqrt{d}} \sum_{r=0}^{d-1} X^{r-k} Z^{-m} P(r,k,q) |\psi\rangle_4, \tag{6.7}$$

donde $N_{m,k,q}$ es una constante de normalización que depende de los resultados de las medidas, y los operadores X, Z y $P(r,k,q)$ son definidos por

$$X = \sum_{n=0}^{d-1} |n+1\rangle\langle n|, \qquad Z = \sum_{n=0}^{d-1} \omega(n) |n\rangle\langle n|, \tag{6.8}$$

y

$$P(r,k,q) = \sum_{t=0}^{d-1} A_{t-k,q,r+t-k} |t\rangle\langle t|. \tag{6.9}$$

Para recuperar el estado inicial del qudit uno, las tres partes deben permitir aplicar al qudit cuatro el operador inverso de Φ, el cual es definido por

$$\Phi = \frac{1}{N_{m,k,q}\sqrt{d}} \sum_{r=0}^{d-1} X^{r-k} Z^{-m} P\left(r,k,q\right), \tag{6.10}$$

que depende del resultado de las medidas m, k, q y de los coeficientes $A_{p,q,r}$ del canal cuántico. Por lo tanto, este operador es en principio desconocido para el tercer usuario. Sólo si el primer y el segundo usuario están de acuerdo en cooperar con el tercer usuario, entonces el tercer usuario puede reconstruir el estado $|\psi\rangle$ aplicando el operador inverso de Φ sobre la partícula cuatro.

6.2.1. Condiciones sobre el Canal Cuántico

El operador Φ debe ser unitario, es decir $\Phi\Phi^\dagger = I$ y $\Phi^\dagger\Phi = I$, donde I es el operador idéntidad. Dado que el operador Φ depende de los coeficientes del canal, entonces se tienen dos condiciones que deben satisfacer los posibles estados que serán utilizados como canal cuántico.

La condición de unitariedad del operador Φ se satisface si se cumplen las siguientes restricciones sobre los coeficientes A_{pqr} del canal cuántico

$$\frac{1}{dN_{m,k,q}^2} \sum_{t=0}^{d-1} A_{t-k,q,r} A^*_{t-k,q,r'} = \delta_{r,r'} \quad \forall \quad k,q = 0,\ldots,d-1, \tag{6.11}$$

y

$$\frac{1}{dN_{m,k,q}^2} \sum_{r=0}^{d-1} A^*_{t-k,q,r} A_{t'-k,q,r} = \delta_{t,t'} \quad \forall \quad k,q = 0,\ldots,d-1. \tag{6.12}$$

De la condición de normalización $1/N_{m,k,q}^2 = d^3$ válido para todo valor de (m,k,q), se tiene que las relaciones (6.11) y (6.12) quedan de la siguiente forma,

$$\sum_{a=0}^{d-1} A_{a,b,c} A^*_{a,b,c'} = \frac{\delta_{c,c'}}{d^2} \quad \forall \quad b = 0,\ldots,d-1, \tag{6.13}$$

y

$$\sum_{c=0}^{d-1} A_{a,b,c} A^*_{a',b,c} = \frac{\delta_{a,a'}}{d^2}, \quad \forall \quad b = 0,\ldots,d-1. \tag{6.14}$$

Ahora, se considera que el protocolo es simétrico, es decir, la clave puede ser recuperada tanto por el segundo o tercer usuario del protocolo. Esta nueva condición se logra cuando el canal cuántico es simétrico ante el intercambio de los qudits tres y cuatro. Por lo tanto, los coeficientes del canal satisfacen la siguiente propiedad $A_{a,b,c} = A_{a,c,b}$ y las relaciones (6.13) y (6.14) toman finalmente la siguiente forma

$$\sum_{a=0}^{d-1} A_{a,b,c} A^*_{a,b',c} = \frac{\delta_{b,b'}}{d^2} \quad \forall\ c = 0,\ldots,d-1, \tag{6.15}$$

y

$$\sum_{b=0}^{d-1} A_{a,b,c} A^*_{a',b,c} = \frac{\delta_{a,a'}}{d^2}, \quad \forall\ c = 0,\ldots,d-1. \tag{6.16}$$

Estas condiciones sobre el canal cuántico permiten probar que

$$Tr_{k_1k_2}\left(|A\rangle_{234}\langle A|\right) = \frac{\mathbf{1}}{d} \;\forall\; k_1, k_2 = 2, 3, 4,\;\; k_1 \neq k_2. \tag{6.17}$$

Por lo tanto, cualquier qudit del canal cuántico está maximalmente entrelazado con los restantes qudits del canal cuántico.

El protocolo funciona de la siguiente manera: Un estado cuántico conjunto de los qudits dos, tres y cuatro, es seleccionado como canal cuántico. Este estado debe satisfacer las condiciones (6.15) y (6.16). Luego, el primer usuario (Alice) realiza una medida de Bell sobre las partículas uno y dos. A continuación, la segunda parte (Bob) mide el qudit tres. En el momento que las tres partes (Alice, Bob y Charlie) están de acuerdo en recuperar el estado, los resultados de las medidas son enviados al tercer usuario (Charlie). Esto permite al tercer usuario aplicar el operador inverso de Φ para lograr recuperar el estado $|\psi\rangle$. En el caso de un canal simétrico, el segundo o tercer usuario pueden recuperar el estado $|\psi\rangle$ dependiendo de que usuario mide su qudit.

6.2.2. Ejemplos de Canal Cuántico

Una familia de estados que satisfacen las condiciones (6.15) y (6.16) es

$$|A(\eta)\rangle_{234} = \frac{1}{\sqrt{d^3}} \sum_{p,q,r=0}^{d-1} \omega\left(\eta pqr\right) |p\rangle_2 |q\rangle_3 |r\rangle_4 . \tag{6.18}$$

El operador Φ asociado a este conjunto de canales cuánticos está dado por

$$\Phi = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \omega\left(\eta qk^2 - \eta qkr\right) X^{r-k} Z^{\eta qr - 2\eta qk - m} U_{\eta q}, \tag{6.19}$$

donde $$U_{\eta q} = \sum_{t=0}^{d-1} \omega\left(\eta qt^2\right) |t\rangle \langle t| .$$

Una segunda familia de estados que satisfacen las condiciones (6.15) y (6.16) está formada por los estados

$$|A(\gamma, \varepsilon)\rangle_{234} = \frac{1}{d} \sum_{p,q=0}^{d-1} \omega\left(\gamma p + \gamma q\right) |p + q - \varepsilon\rangle_2 |p\rangle_3 |q\rangle_4 . \tag{6.20}$$

Dos estados dentro de esta familia son ortogonales, esto es

$$\langle A(\gamma', \varepsilon') | A(\gamma, \varepsilon)\rangle = \delta_{\gamma\gamma'}\delta_{\varepsilon\varepsilon'}, \tag{6.21}$$

El operador Φ asociado a esta familia de canales cuánticos es

$$\Phi = \omega\left(\gamma\epsilon - \gamma k\right) Z^{\gamma - m} X^{\epsilon - p - k}. \tag{6.22}$$

Los valores de m y k son obtenidos después de la medida de Bell sobre las partículas uno y dos, y el valor de q es obtenido después de la medida sobre la partícula tres.

6.2.3. Seguridad del Protocolo

Ahora, se analiza la seguridad del protocolo de distribución de claves. Suponemos que Charlie trata de obtener el estado cuántico $|\psi\rangle$ sin la colaboración de Bob. Una posible estrategia que podría emplear Charlie consiste en obtener el qudit de Bob, medirlo y reenviar un qudit a Bob en el mismo estado. Esto permite a Charlie obtener el valor de la medida de Bob sin ser detectado. En el momento que Charlie recibe los valores de las medidas realizadas por Alice, el podría realizar la operación unitaria para recuperar el estado $|\psi\rangle$ sin la colaboración de Bob. Esta estrategia del deshonesto en el canal, se puede evitar alternando el receptor del estado cuántico codificado. Esto es posible, dado que estamos considerando canales cuánticos que son simétricos ante el intercambio de los qudit tres y cuatro, es decir, con respecto a los qudits que pertenecen a Bob y Charlie respectivamente. Por cuanto, Alice puede decidir, después de distribuir los qudits tres y cuatro, que usuario recibirá el estado al seleccionar que usuario medirá su qudit. Asumimos que Alice seleciona a Bob para obtener el estado cuántico. Antes que Alice declare por un canal clásico el receptor del estado, Charlie debe enviar un qudit a Bob de otro manera sería detectado. Sin embargo, dado que Charlie no conoce el estado que comparte con Alice y Bob, y además, no conoce los resultados de las medidas de Alice, el no puede preparar adecuadamente el qudit que debe enviar a Bob. Esta estrategia de un posible deshonesto en el canal debería ser detectada, si Alice compara el estado que envía con los estados recibidos por Bob.

Un segundo esquema para prevenir la acción de un deshonesto en el canal es que Alice pueda aplicar una transformación unitaria sobre el qudit tres. Por ejemplo, Alice puede elegir aleatoriamente entre dos transformaciones unitarias U_a y U_b. Estas transformaciones cambian el estado seleccionado como canal cuántico. De manera de completar el protocolo, Bob debe revertir la transformación aplicada por Alice. Sin embargo, como Alice mantiene en secreto su elección, Bob también debe elegir aleatoriamente entre aplicar la inversa de U_a y U_b. En el caso que Charlie intercepte el qudit de Bob, el también necesita revertir el cambio sobre el canal cuántico antes de la medida en el qudit de Bob. Por cuanto, Charlie debe aplicar la operación inversa de U_a ó U_b aleatoriamente. Por lo tanto, él aplica U_a ó U_b sobre un qudit y lo envía a Bob, quien elige una transformación, aplica su inversa sobre su qudit y realiza la medida. Finalmente, Bob comunica su elección sobre la transformación a Alice, quien declara si el intento de compartir el estado cuántico es válido o no lo es. De acuerdo a este esquema es posible que la transformación elegida por Alice y Bob sean iguales, aunque la elegida por Charlie sea diferente. En este caso, las correlaciones entre los resultados de las medidas de Alice y Bob cambian permitiendo la posibilidad de detectar el intento de Charlie de obtener la clave.

Los esquemas anteriores pueden ser reinterpretados al notar que la acción de una transformación unitaria sobre el qudit tres de un canal cuántico genera un nuevo canal cuántico. Esto implica que Bob puede controlar localmente el canal cuántico que será utilizado durante la implementación del protocolo. Esto agrega un mayor grado de seguridad al protocolo, dado que el operador a ser aplicado sobre el qudit cuatro depende del canal cuántico utilizado. Por lo tanto, Charlie requiere del resultado de la medida de Bob y del conocimiento de la transformación unitaria usada por Bob. Esta transformación puede mantenerse en secreto hasta que Alice decida completar el protocolo.

6.3. Protocolo usando un Canal Parcialmente Entrelazado

La perfecta implementación de los protocolos de comunicación cuántica requiere del uso de estados maximalmente entrelazados utilizados como canal cuántico. Sin embargo, si el estado no está maximalmente entrelazado aún es posible utilizar este grado de entrelazamiento para llevar a cabo algunos protocolos de comunicación cuántica. En el contexto de distribución de estados bidimensionales, esto ha sido estudiado por Gordon y Rigolin [128], y por Bandyopadhyay [129]. En esta sección se muestra que el protocolo para la distribución de qudits introducida en la sección anterior puede ser modificada de manera que sea posible utilizar un estado cuántico que no satisface las relaciones (6.13) y (6.14). En este caso, al utilizar un estado parcialmente entrelazado el protocolo para distribución de la clave se realiza en forma probabilista. Se considera el siguiente estado conjunto formado por los qudits dos, tres y cuatro, parcialmente entrelazado como posible canal cuántico

$$|B\rangle_{234} = \sum_{p,q,r=0}^{d-1} A_{p,q,r} f_p \, |p\rangle_2 \otimes |q\rangle_3 \otimes |r\rangle_4 \,, \tag{6.23}$$

con la condición de normalización

$$\sum_{p,q,r=0}^{d-1} |A_{p,q,r} f_p|^2 = 1. \tag{6.24}$$

El estado inicial del sistema compuesto obedece a la siguiente identidad

$$XOR_{21}|\psi\rangle_1 \, |B\rangle_{234} = \frac{\sqrt{Q}}{d^2} \sum_{q,k,\alpha=0}^{d-1} Z_1^{-\alpha} \, |k\rangle_1 \otimes |\nu_\alpha\rangle_2 \otimes |q\rangle_3 \otimes \Phi\,(k,\alpha,q)\,|\psi\rangle_4 \,, \tag{6.25}$$

donde el operador $\Phi\,(k,\alpha,q)$ es dado por

$$\Phi\,(k,\alpha,q) = d \sum_{r=0}^{d-1} X^r Z^{-\alpha} \sum_{p=0}^{d-1} A_{p+k,q,p+r} \, |p\rangle \, \langle p| \,, \tag{6.26}$$

y la acción de la transformación XOR [130] es dada por $XOR|i\rangle_c|j\rangle_t = |i\rangle_c|i \ominus j\rangle_t$, donde c y t indican el sistema de control y el sistema "blanco" respectivamente. Los estados $|\nu_\alpha\rangle_2$ son definidos por

$$|\nu_\alpha\rangle = Z^\alpha \sum_{n=0}^{d-1} \tilde{f}_n |n\rangle, \tag{6.27}$$

donde

$$\tilde{f}_p = \frac{f_p}{\sqrt{Q}}, \qquad Q = \sum_{p=0}^{d-1} |f_p|^2. \tag{6.28}$$

Al igual que en el caso del estado maximalmente entrelazado, la recuperación del estado $|\psi\rangle$ requiere de la aplicación de un operador Φ^{-1} sobre el qudit cuatro, que depende de los resultados de las medidas sobre los qudit uno, dos y tres. Esto implica, la perfecta identificación de los

valores de (k, α, q). Sin embargo, los estados del qudit dos asociados con el índice α no son ortogonales. El producto interior de dos de estos estados es

$$\langle \nu_n | \nu_m \rangle = \sum_{k=0}^{d-1} \omega(k(m-n)) |\tilde{f}_k|^2. \tag{6.29}$$

Por lo tanto, no es posible distinguir deterministicamente entre los estados $|\nu_\alpha\rangle_2$, haciendo imposible la determinación conclusiva del valor de α, y consecuentemente, del operador Φ. Luego, de acuerdo a la relación (6.25), la distribución del estado de un qudit $|\psi\rangle$, está limitada a nuestra capacidad para discriminar el conjunto de estados no ortogonales $|\nu_\alpha\rangle_2$. La óptima probabilidad de discriminación sin ambigüedad de este tipo de estados es $S_{max} = d|\tilde{f}_k|^2$, donde $\tilde{f}_k$ es el coeficiente con menor valor absoluto del estado (6.27) [108, 109]. En este caso, el esquema de discriminación funciona de la siguiente manera. Una transformación unitaria U_2 se aplica sobre los estados $|\nu_\alpha\rangle_2 \oplus |0\rangle_a$, donde $|0\rangle_a$ es el estado inicial de la ancilla. El estado final después de la aplicación de la transformación unitaria es

$$U_2(|\nu_\alpha\rangle_2 \oplus |0\rangle_a) = \sqrt{S_{max}}\,|u_\alpha\rangle_2 + |\phi_\alpha\rangle_2\,, \tag{6.30}$$

donde, el conjunto de estados $\Omega_u = \{|u_\alpha\rangle_2\}$ está formado por estados mutuamente ortogonales. Además, este conjunto de estados es ortogonal al subespacio generado por los estados $\Omega_a = \{|a_k\rangle_2\}$, que expanden en ese subespacio a los estados de falla $|\phi_\alpha\rangle_2$. Después, de la aplicación de la transformación unitaria U_2, una medida proyecta el estado a ser discriminado en una de las bases Ω_u ó Ω_a. Dado que los estados $|\nu_\alpha\rangle_2$ y $|u_\alpha\rangle_2$ están en correspondencia uno a uno, la proyección sobre el subespacio Ω_u permite una discriminación conclusiva del estado. Sin embargo, la proyección del estado en el subespacio Ω_a genera un resultado inconclusivo. Esto se debe a que, cada estado en Ω_a tiene una componente en todos los estados $|\phi_\alpha\rangle$.

El protocolo para distribuir un estado cuántico ahora está sujeto a la discriminación de estados y queda de la forma

$$U_2 XOR_{21} |\psi\rangle_1 |B\rangle_{234} = \frac{\sqrt{Q}}{d^2} \sum_{q,k,\alpha=0}^{d-1} Z_1^{-\alpha} |k\rangle_1 \otimes (\sqrt{S_{max}}\,|u_\alpha\rangle_2 + |\phi_\alpha\rangle_2) \otimes |q\rangle_3 \otimes \Phi\,(k, \alpha, q)\,|\psi\rangle_4, \tag{6.31}$$

donde los estados $|\phi_\alpha\rangle_2$ son dados por

$$|\phi_\alpha\rangle_2 = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} A_k^\alpha |a_k\rangle_2, \quad \text{donde} \quad A_k^\alpha = \sum_{m=0}^{d-1} \omega(m(\alpha-k)) \sqrt{\tilde{f}_m^2 - \tilde{f}_{min}^2}. \tag{6.32}$$

La identidad (6.31) permite distribuir el estado cuántico $|\psi\rangle$ bajo el siguiente esquema. Después de que las medidas sobre las partículas uno y tres se han realizado, se mide sobre la partícula dos. Si el resultado de esta medida es $|u_\alpha\rangle_2$, el estado de la partícula cuatro se proyecta a

$$|\psi_{k,\alpha,q}\rangle_4 = \frac{\sqrt{QS_{max}}}{N_{k,\alpha,q} d^2} \Phi(k, \alpha, q) |\psi\rangle_4, \tag{6.33}$$

donde $N_{k,\alpha,q}$ es una constante de normalización. Este proceso tiene una probabilidad de éxito igual a $S_{max} = d|\widetilde{f}_{min}|^2$ en la discriminación del estado y por lo tanto, en el esquema de

distribución de la clave. De la condición de unitariedad del operador $\Phi(k,\alpha,q)$ que actúa sobre el estado $|\psi\rangle_4$, se obtienen condiciones que deben cumplir los coeficientes del canal

$$\frac{QS_{max}}{N_{k,\alpha,q}^2 d^2}\omega(\alpha(n-n'))\sum_{a=0}^{d-1} A_{n,q,a}^* A_{n',q,a} = \delta_{n,n'} \quad \forall \quad q=0,\ldots,d-1, \tag{6.34}$$

$$\frac{QS_{max}}{N_{k,\alpha,q}^2 d^2}\sum_{a=0}^{d-1} A_{a,q,n}^* A_{a,q,n'} = \delta_{n,n'} \quad \forall \quad q=0,\ldots,d-1, \tag{6.35}$$

De la condición de normalización, obtenemos $N_{k,\alpha,q}^2 = S_{max}/d^3$, y las condiciones (6.34) y (6.35) quedan

$$\sum_{a=0}^{d-1} A_{n,q,a}^* A_{n',q,a} = \frac{\delta_{n,n'}}{Qd}, \tag{6.36}$$

$$\sum_{a=0}^{d-1} A_{a,q,n}^* A_{a,q,n'} = \frac{\delta_{n,n'}}{Qd}. \tag{6.37}$$

Dado que el estado (6.23) es una deformación de los canales (6.18) y (6.20), los valores de los coeficientes f_p deben satisfacer la siguiente relación

$$Q = \sum_{p=0}^{d-1} |f_p|^2 = d. \tag{6.38}$$

Por lo tanto, las condiciones que deben cumplir los coeficientes $A_{p,q,r}$ del estado (6.23) son exactamente iguales al caso del canal cuántico ideal (6.2). Los casos en los cuales los estados $|\nu_\alpha\rangle_2$ son correctamente identificados permiten una perfecta distribución del estado $|\psi\rangle$. Por cuanto, el operador Φ puede ser invertido, en el caso que los usuarios esten de acuerdo en cooperar. En el caso, que la discriminación de los estados $|\nu_\alpha\rangle_2$ no sea exitosa, el estado del qudit dos después de la medida es $|a_s\rangle_2$. Este evento tiene una probabilidad igual a $1 - S_{max}$ y el qudit cuatro es proyectado al estado

$$|\psi_{k,s,q}\rangle_4 = \frac{1}{d^2\sqrt{d}}\sum_{\alpha=0}^{d-1}\omega(-\alpha k)A_s^\alpha \Phi(k,\alpha,q)|\psi\rangle_4. \tag{6.39}$$

El estado (6.39) constituye un estado de falla del proceso ya que, no es posible invertir la acción de la suma de los operadores Φ. Esto se debe a que la suma de operadores unitarios no es necesariamente unitario. Sin embargo, el estado (6.39) tiene alguna fidelidad con respecto al estado $|\psi\rangle$ a distribuir. Para cuantificar la fidelidad del estado de falla $|\psi_{k,s,q}\rangle_4$ con respecto al estado que deseamos teleportar $|\psi\rangle$ se utiliza la fidelidad promedio, la cual es definida por [131]

$$\bar{F} = \int d\psi \sum_{k,s,q} |\langle\psi|\psi_{k,s,q}\rangle|^2, \tag{6.40}$$

donde la integral $\int d\psi$ se realiza sobre el espacio de todos los estados puros y se ha considerado la siguiente identidad [131]

$$\hat{M}_{kl} = \int d\psi \langle\psi|k\rangle\langle l|\psi\rangle|\psi\rangle\langle\psi| = \frac{1}{d(d+1)}(\delta_{kl}\hat{1} + |k\rangle\langle l|). \tag{6.41}$$

Con lo cual, la fidelidad promedio del estado de falla $|\psi_{k,s,q}\rangle_4$ con respecto al estado que deseamos teleportar $|\psi\rangle$ es

$$\bar{F}_1 = \sum_{k,s,q=0}^{d-1} \int d\psi |_4\langle\psi|\psi_{k,s,q}\rangle_4|^2 = \frac{1 - d|\tilde{f}_{min}|^2}{d^2}. \tag{6.42}$$

Es posible incrementar la fidelidad promedio del protocolo [108]. Esto es posible dado que la fidelidad promedio se maximiza al aplicar el operador $Z^s X^{-r}$ al estado de falla $|\psi_{k,s,q}\rangle_4$. Esto se debe a que los coeficientes A_k^α alcanzan su máximo cuando $\alpha = s$. Con lo cual la fidelidad promedio $\bar{F}_2$ es

$$\bar{F}_2 = \frac{2}{d+1}[\frac{1}{d} - |\tilde{f}_{min}|^2 + \sum_{quu'_{t\neq t'}}^{d-1} A_{tqu} A_{t'qu'} \sqrt{|\tilde{f}_t|^2 - |\tilde{f}_{min}|^2} \sqrt{|\tilde{f}_{t'}|^2 - |\tilde{f}_{min}|^2}], \tag{6.43}$$

donde se tiene $\bar{F}_2 \geq \bar{F}_1$, por cuanto se incrementa la fidelidad promedio en el segundo caso.

6.4. Implementación del Protocolo

Un esquema físico para la implementación del protocolo propuesto tiene su origen en la transferencia de estados y del entrelazamiento cuántico. Cirac *et al.* [132] propuso un esquema para transferir estados cuánticos de iones almacenados en cavidades distantes. La transferencia del estado es mediante el intercambio unidireccional de fotones entre las cavidades, controlados por la aplicación de pulsos laser sobre los iones. Este esquema ha sido extendido al caso de qutrits [133]. En este caso, los qutrits son realizados mediante la estructura fina de los niveles $4S_{1/2}$ y $5D_{3/2}$ de iones ^{138}Ba y la transferencia del estado, es por medio de la emisión de fotones polarizados desde una de las cavidades y la absorción de los fotones polarizados por la otra cavidad. Los qutrits inicialmente se encuentran entrelazados. Dos qutrits son seleccionados para transferir el estado de uno de ellos a un qutrit en una cavidad alejada. Por lo tanto, el estado entrelazado de tres qutrits localizados puede ser transferido a tres qutrits espacialmente alejados. El protocolo de distribución de estados cuánticos también requiere de la implementación de una medida de Bell. Esto puede ser realizado mediante la aplicación de la transformada de Fourier, una compuerta control-not y mediciones en la base lógica. En el caso de la codificación de los qutrits en iones, ha sido demostrado que estas transformaciones pueden ser eficientemente implementadas [134].

Otra posible implementación del esquema de distribución de estados cuánticos, es utilizando óptica lineal. En este caso, se requiere generar un estado maximalmente entrelazado de tres partículas. Cada una de las partículas se envía a un usuario que puede realizar operaciones sobre su respectiva partícula. De esta manera, mediante el intercambio de información clásica es posible reconstruir el estado teleportado, en el cual se codifica la información secreta. Si se cuenta con una fuente de estados parcialmente entrelazados, uno de los usuarios se enfrenta al problema de discriminar estados simétricos. Una propuesta para la discriminación de estados simétricos fue analizada en el capítulo anterior, donde el proceso de discriminación de estados simétricos, se lleva a cabo con la probabilidad óptima en los procesos de discriminación sin ambigüedad y de discriminación con mínimo error.

Capítulo 7

Copia Probabilista de Estados Igualmente Separados

Los estados igualmente separados fueron propuestos por Roa *et al.* [135] en el año 2008, y representan el conjunto de estados cuánticos más simple que podemos utilizar, dado que están definidos sólo por un único parámetro, su producto interior α. En este capítulo, se determina la forma de los estados igualmente separados en términos de la base lógica. Además, es posible escribir los elementos de la base lógica en términos de los estados igualmente separados. Se demuestra que los estados igualmente separados son equivalentes a los estados simétricos en el caso que el producto interior α sea un número real. Una de las principales contribuciones de la tesis fue establecer la forma de los estados igualmente separados, algunas de las aplicaciones donde se pueden utilizar estos estados son: protocolos de comunicaciones cuánticas, criptografía cuántica y concentración del entrelazamiento.

Además, en este capítulo se estudia una máquina de copiado probabilista que genera M copias de un estado que pertenece a un conjunto de n estados igualmente separados. Los estados son puros, linealmente independientes y con igual probabilidad de preparación $1/n$. En particular, se analiza el efecto que posee la fase de α en la probabilidad de éxito del proceso de copia de los estados igualmente separados.

En los capítulos anteriores hemos analizado la discriminación de estados simétricos. En el capítulo 5 se ha propuesto un esquema de discriminación conclusiva y con mínimo error de los estados simétricos. Por otro lado, en el capítulo 6 nos enfrentamos a la discriminación de estados simétricos para realizar la distribución de estados, en el caso que inicialmente se tiene un estado parcialmente entrelazado como canal cuántico. Como ya se ha mencionado, una de las aplicaciones de los estados cuánticos no ortogonales es la criptografía cuántica. En partícular, se pueden utilizar un conjunto de n estados simétricos para realizar un protocolo de criptografía cuántica. Sin embargo, el número de parámetros al utilizar n estados simétricos resulta ser similar al número de estados simétricos, lo que genera dificultades en la obtención de los resultados. Posteriormente, se pretende realizar un protocolo de criptografía cuántica utilizando los estados igualmente separados, esta aplicación queda como una propuesta de trabajo futuro por lo que no se incluye en la tesis.

7.1. Introducción

La imposibilidad de copiar estados cuánticos desconocidos en forma perfecta y de manera determinista es una de las principales características de los sistemas físicos con propiedades cuánticas [44, 136]. Este resultado, fue demostrado por Wooters y Zurek [44] y es conocido como no-cloning theorem. Establece que debido a la linealidad de las operaciones cuánticas no es posible duplicar un estado cuántico $|\psi\rangle$ desconocido arbitrario. Sin embargo, no está prohibida la posibilidad de una copia aproximada. Esto fue demostrado por Bužek y Hillery [137] quienes construyerón una máquina de copiado universal, que permite duplicar en forma determinista estados en un espacio de Hilbert bidimensional con una fidelidad menor que la unidad. Este resultado fue extendido al caso de un espacio de Hilbert de dimensión más alta por Werner [138], por Keyl y Werner [139], por Alber *et al.* [140], entre otros.

Una clase diferente de máquina de copiado fue propuesta por Duan y Guo [141]. Esta máquina permite generar copias perfectas de un conjunto de estados, pero con una probabilidad de éxito menor que la unidad. También se demuestra que una máquina de copiado probabilista existe, si y sólo si, los estados son linealmente independientes. Además, se establece la conexión entre la copia probabilista y la discriminación de estados sin ambigüedad. En este contexto, Pati [142] propuso una máquina de copiado cuántica, donde el estado de salida puede ser una superposición de estados de todas las multiples posibles copias del mismo estado original. Por otro lado, se ha investigado el borrado cuántico, el cual resulta ser un proceso similar al copiado cuántico, pero en este caso, la información contenida en estados desconocidos no pueden ser completamente borrada [143]. Los procesos de copiado y borrado cuántico fueron presentados en una forma unificada [144, 145], donde una máquina cuántica puede realizar multiples copias y borrados en una única operación.

La forma explícita de este tipo de máquina de copiado y sus probabilidades de éxito se conocen sólo en algunos casos. Por ejemplo, Duan y Guo [146] encontró una máquina de copiado probabilista de dos estados no ortogonales $\{|\psi_0\rangle, |\psi_1\rangle\}$ que permite realizar dos copias. Cuando las probabilidades a priori de estos estados son iguales, la óptima probabilidad de copia es

$$P_{1\to 2} = \frac{1}{1 + |\langle\psi_0|\psi_1\rangle|}. \tag{7.1}$$

Este resultado fue extendido por Chefles y Barnett [147] a la generación de M copias del estado cuando se tiene inicialmente N copias. En este caso, la óptima probabilidad de copiar dos estados no ortogonales $\{|\psi_0\rangle, |\psi_1\rangle\}$ con igual probabilidad de preparación es

$$P_{N\to M} = \frac{1 - |\langle\psi_0|\psi_1\rangle|^N}{1 - |\langle\psi_0|\psi_1\rangle|^M}. \tag{7.2}$$

En el caso, de un conjunto con mayor número de elementos sólo se conoce la cota superior de la probabilidad de copiado. Una cota superior para la probabilidad de éxito en la copia de $N \to M$ de un conjunto de n estados no ortogonales fue obtenida por Qiu [148]. Donde, los estados se denotan por $|\psi_i\rangle$, con $i = 1, 2, ..., n$, y en el caso, que los estados tengan la misma probabilidad de preparación $1/n$, la probabilidad óptima de copia tiene una cota superior dada por

$$P_{clon}^{N\to M} \leq \frac{2}{n(n-1)} \sum_{i<j} \frac{1 - |\langle\psi_i|\psi_j\rangle|^N}{1 - |\langle\psi_i|\psi_j\rangle|^M}. \tag{7.3}$$

Este resultado fue extendido por Feng *et al.* [149] que dedujo una cota inferior para la probabilidad de falla en la copia de $N \to M$ de un conjunto de operadores densidad ρ_i, donde $i = 1, 2, ..., n$, con arbitrarias probabilidades de preparación.

7.2. Estados Igualmente Separados

Estamos interesados en la copia probabilista de un conjunto de estados cuánticos igualmente separados $A_n(\alpha)$ cuyos n elementos son estados cuánticos $|\alpha_k\rangle$ donde $k = 1, \ldots, n$, tal que el producto interior de cualquiera de ellos es igual a α, esto es

$$\langle \alpha_k | \alpha_{k'} \rangle = |\alpha| e^{i\theta}, \ \forall \ k > k', \tag{7.4}$$

dado esta propiedad del conjunto de estados $|\alpha_k\rangle$, los denominamos igualmente separados.

El conjunto de estados $A_n(\alpha)$ es linealmente independiente cuando la identidad

$$\sum_{k=1}^{n} A_k \, |\alpha_k\rangle = 0, \tag{7.5}$$

se satisface si y sólo si, los n coeficientes A_k son todos cero, de otro modo el conjunto de estados es linealmente dependiente. Multiplicando la ecuación (7.5) sobre todos los estados $|\alpha_k\rangle$, obtenemos un sistema de ecuaciones lineales homogéneo, donde los coeficentes A_k son las n cantidades desconocidas. Desde el sistema de ecuaciones lineales homogéneo se tiene que el conjunto $A_n(\alpha)$ es linealmente independiente cuando el determinante de la siguiente matriz es distinto de cero

$$M = \begin{pmatrix} 1 & \alpha & \alpha & \ldots & \alpha \\ \alpha^* & 1 & \alpha & \ldots & \alpha \\ \alpha^* & \alpha^* & 1 & \ldots & \alpha \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^* & \alpha^* & \alpha^* & \ldots & 1 \end{pmatrix}. \tag{7.6}$$

La matriz M es hermítica y tiene estructura de matriz de Toeplitz [150], puede ser diagonalizada por una matriz unitaria T, tal que $D = TMT^\dagger$ donde

$$T = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & \omega_1^1 & \omega_1^2 & \ldots & \omega_1^{n-1} \\ 1 & \omega_2^1 & \omega_2^2 & \ldots & \omega_2^{n-1} \\ 1 & \omega_3^1 & \omega_3^2 & \ldots & \omega_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^1 & \omega_n^2 & \ldots & \omega_n^{n-1} \end{pmatrix}, \tag{7.7}$$

donde

$$\omega_j = e^{i\theta_j} \qquad \text{y} \qquad \theta_j = \frac{2}{n}(\theta - (j-1)\pi), \qquad \text{para} \qquad j = 1, ..., n. \tag{7.8}$$

La matriz diagonal $D = diag(\lambda_1, ..., \lambda_n)$ contiene los autovalores reales de M, los cuales son dados por

$$\lambda_j = 1 - |\alpha| \frac{\sin(\theta + \frac{(j-1)\pi - \theta}{n})}{\sin(\frac{(j-1)\pi - \theta}{n})}, \qquad \text{para} \qquad j = 1, ..., n, \tag{7.9}$$

donde $\alpha = |\alpha| e^{i\theta}$ con $0 \leq \theta < 2\pi$. Si definimos a f_j, como el término que depende del coeficiente j, de la siguiente forma

$$f_j = -\frac{\sin(\theta + \frac{(j-1)\pi - \theta}{n})}{\sin(\frac{(j-1)\pi - \theta}{n})}, \tag{7.10}$$

luego, el mínimo valor de λ_j corresponde al caso donde el coeficiente f_j es mínimo. Dado que

$$f_j = f_2 \frac{1 + \tan(\frac{(j-2)\pi}{n})\text{cotan}(\theta + \frac{\pi - \theta}{n})}{1 + \tan(\frac{(j-2)\pi}{n})\text{cotan}(\frac{\pi - \theta}{n})}, \tag{7.11}$$

se puede demostrar que el mínimo autovalor es λ_2, el cual es dado por

$$\lambda_2 = 1 - |\alpha| \frac{\sin(\theta + \frac{\pi - \theta}{n})}{\sin(\frac{\pi - \theta}{n})}. \tag{7.12}$$

Luego, el determinante de la matriz M es cero cuando el autovalor $\lambda_2 = 0$. Por lo tanto, el conjunto de estados $A_n(\alpha)$ es linealmente independiente, si el modulo de α está en el intervalo $[0, |\overline{\alpha}_\theta|)$, donde $|\overline{\alpha}_\theta|$ es una función de θ y de n dada por

$$|\overline{\alpha}_\theta| = \frac{\sin(\frac{\pi - \theta}{n})}{\sin\left(\theta + \frac{\pi - \theta}{n}\right)}. \tag{7.13}$$

En el caso que $|\alpha| = |\overline{\alpha}_\theta|$ los estados en $A_n(\alpha)$ son linealmente dependientes y pertenecen a un subespacio $(n-1)$ dimensional. Además, el valor $|\overline{\alpha}_\theta|$ corresponde al máximo valor permitido de $|\alpha|$ para un cierto θ dado. La función (7.13) no es periódica y sólo esta bien definida en el intervalo $\theta \in [0, 2\pi)$.

Ahora, desde la condición $M = T^\dagger D T$, se deben satisfacer las siguientes n relaciones

$$\begin{aligned}
1 &= \frac{1}{n}(\lambda_1 + \lambda_2 + \lambda_3 + \ldots + \lambda_n), && (7.14)\\
\alpha &= \frac{1}{n}(\lambda_1 \omega_1^1 + \lambda_2 \omega_2^1 + \lambda_3 \omega_3^1 + \ldots + \lambda_n \omega_n^1), && (7.15)\\
\alpha &= \frac{1}{n}(\lambda_1 \omega_1^2 + \lambda_2 \omega_2^2 + \lambda_3 \omega_3^2 + \ldots + \lambda_n \omega_n^2), && (7.16)\\
&\vdots \\
\alpha &= \frac{1}{n}(\lambda_1 \omega_1^{n-1} + \lambda_2 \omega_2^{n-1} + \lambda_3 \omega_3^{n-1} + \ldots + \lambda_n \omega_n^{n-1}). && (7.17)
\end{aligned}$$

Desde el conjunto de n ecuaciones (7.14) a (7.17), se puede deducir la forma de los estados

igualmente separados, los cuales son

$$|\alpha_1\rangle = \frac{1}{\sqrt{n}}(\sqrt{\lambda_1}\,|1\rangle + \sqrt{\lambda_2}\,|2\rangle + \sqrt{\lambda_3}\,|3\rangle + \ldots + \sqrt{\lambda_n}\,|n\rangle), \tag{7.18}$$

$$|\alpha_2\rangle = \frac{1}{\sqrt{n}}(\sqrt{\lambda_1}(\omega_1^1)^*\,|1\rangle + \sqrt{\lambda_2}(\omega_2^1)^*\,|2\rangle + \sqrt{\lambda_3}(\omega_3^1)^*\,|3\rangle + \ldots + \sqrt{\lambda_n}(\omega_n^1)^*\,|n\rangle), \tag{7.19}$$

$$|\alpha_3\rangle = \frac{1}{\sqrt{n}}(\sqrt{\lambda_1}(\omega_1^2)^*\,|1\rangle + \sqrt{\lambda_2}(\omega_2^2)^*\,|2\rangle + \sqrt{\lambda_3}(\omega_3^2)^*\,|3\rangle + \ldots + \sqrt{\lambda_n}(\omega_n^2)^*\,|n\rangle), \tag{7.20}$$

$$\vdots$$

$$|\alpha_n\rangle = \frac{1}{\sqrt{n}}(\sqrt{\lambda_1}(\omega_1^{n-1})^*\,|1\rangle + \sqrt{\lambda_2}(\omega_2^{n-1})^*\,|2\rangle + \sqrt{\lambda_3}(\omega_3^{n-1})^*\,|3\rangle + \ldots + \sqrt{\lambda_n}(\omega_n^{n-1})^*\,|n\rangle), \tag{7.21}$$

con lo cual se satisface que el producto interior de cualquiera de ellos es igual a α, esto es

$$\langle\alpha_k|\alpha_{k'}\rangle = |\alpha|e^{i\theta},\ \forall\ k > k'. \tag{7.22}$$

Además, los estados de las ecuaciones (7.18) a (7.21) cumplen con la condición de normalización, es decir

$$\frac{1}{n}\sum_{k=1}^{n}\lambda_k = 1. \tag{7.23}$$

Es posible expresar los estados igualmente separados de manera más compacta, de la siguiente forma

$$|\alpha_j\rangle = \frac{1}{\sqrt{n}}\sum_{k=1}^{n}\sqrt{\lambda_k}(\omega_k^{j-1})^*\,|k\rangle\,, \qquad j = 1, ..., n. \tag{7.24}$$

La base lógica $\{|k\rangle\}$ con $k = 1, ..., n$, en función de los estados igualmente separados $|\alpha_r\rangle$ es

$$|k\rangle = \frac{1}{\sqrt{n\lambda_k}}\sum_{r=1}^{n}\omega_k^{r-1}\,|\alpha_r\rangle\,. \tag{7.25}$$

Los estados (7.25) son ortogonales, ya que satisfacen la siguiente relación

$$\langle k|k'\rangle = \delta_{k,k'}. \tag{7.26}$$

Además, existe una transformación unitaria U que conecta los estados igualmente separados, es decir

$$|\alpha_2\rangle = U\,|\alpha_1\rangle\,, \tag{7.27}$$

$$|\alpha_j\rangle = U^{j-1}\,|\alpha_1\rangle\,, \tag{7.28}$$

donde la transformación unitaria U es

$$U = \begin{pmatrix} (\omega_1^1)^* & 0 & 0 & \ldots & 0 \\ 0 & (\omega_2^1)^* & 0 & \ldots & 0 \\ 0 & 0 & (\omega_3^1)^* & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & (\omega_n^1)^* \end{pmatrix}. \tag{7.29}$$

Ahora, de la definición de los coeficientes ω_j de la ecuación (7.8), se puede descomponer la transformación unitaria U de la forma

$$U = exp(-\frac{2i\theta}{n})Z, \tag{7.30}$$

donde el operador Z actuando sobre una base ortogonal $\{|k\rangle\}$, que expande el espacio de Hilbert n-dimensional de los estados igualmente separados, es de la forma

$$Z\,|k\rangle = exp[\frac{2i\pi}{n}(k-1)]\,|k\rangle\,, \qquad k = 1, ..., n. \tag{7.31}$$

Por lo tanto, se tiene que la transformación unitaria U elevada a una potencia n es

$$U^n = exp(-2i\theta)Z^n, \tag{7.32}$$

dado que $Z^n = \mathbf{1}$, es el operador identidad en una dimensión n, se tiene que

$$U^n = exp(-2i\theta)\mathbf{1}. \tag{7.33}$$

Desde la ecuación (7.33) es posible establecer una conección entre los estados igualmente separados y los estados simétricos estudiados en los capítulos anteriores. Los estados simétricos se pueden generar a través de la aplicación de una transformación unitaria U tal como en las ecuaciones (7.27) y (7.28). Sin embargo, se requiere que la transformación unitaria U a la potencia n sea igual al operador identidad. Esta condición se satisface si el ángulo θ de la ecuación (7.33) toma los valores $\theta = 0$ y $\theta = \pi$. Estos dos posibles casos, definen un producto interior entre los estados que es real positivo ($\theta = 0$) o real negativo ($\theta = \pi$). Por lo tanto, los estados igualmente separados son simétricos si el producto interior entre los estados asume un valor real.

7.3. Discriminación sin Ambigüedad de Estados Igualmente Separados

La probabilidad óptima de discriminación sin ambigüedad del conjunto de estados igualmente separados fue obtenida por Roa *et al.* [135]. La discriminación sin ambigüedad del conjunto $A_n(\alpha)$ de los estados igualmente separados se describe por la siguiente transformación

$$U\,|\alpha_k\rangle\,|\kappa\rangle_a = \sqrt{1-|s|^2}\,|k\rangle\,|\perp\rangle_a + s|\alpha_k^{LD}(\theta)\rangle\,|\vdash\rangle_a\,, \tag{7.34}$$

donde, los estados $|\perp\rangle_a$ y $|\vdash\rangle_a$ corresponden a dos estados ortogonales que expanden el espacio bidimensional de la ancilla. La medida del estado $|\perp\rangle_a$ en el espacio de la ancilla, proyecta los estados no ortogonales $|\alpha_k\rangle$ a estados ortogonales $|k\rangle$ con una probabilidad igual a $1-|s|^2$. Los estados $|\alpha_k^{LD}(\theta)\rangle$ corresponden a estados linealmente dependientes que son generados al obtener el estado $|\vdash\rangle_a$ en el espacio de la ancilla. De la unitariedad de la transformación U se tiene

$$\langle\alpha_k|\alpha_{k'}\rangle = |s|^2\langle\alpha_k^{LD}(\theta)|\alpha_{k'}^{LD}(\theta)\rangle, \tag{7.35}$$

$$|\alpha|e^{i\theta} = |s|^2|\langle\alpha_k^{LD}(\theta)|\alpha_{k'}^{LD}(\theta)\rangle|e^{i\theta}, \tag{7.36}$$

luego,

$$|s|^2 = \frac{|\alpha|}{|\langle\alpha_k^{LD}(\theta)|\alpha_{k'}^{LD}(\theta)\rangle|}. \tag{7.37}$$

Si la probabilidad de preparación de los estados $|\alpha_k\rangle$ es la misma, es decir $\eta_k = 1/n$, la probabilidad de discriminación sin ambigüedad del estado $|\alpha_k\rangle$ es

$$P_k = \eta_k(1-|s|^2) = \frac{1}{n}(1-\frac{|\alpha|}{|\langle\alpha_k^{LD}(\theta)|\alpha_{k'}^{LD}(\theta)\rangle|}) = \frac{1}{n}(1-\frac{|\alpha|}{|\overline{\alpha}_\theta|}). \tag{7.38}$$

Luego, la probabilidad de éxito $P_s = \sum_k P_k$, en el proceso de discriminación sin ambigüedad es

$$P_s = 1-|\alpha|\frac{\sin(\theta+\frac{\pi-\theta}{n})}{\sin\frac{\pi-\theta}{n}}. \tag{7.39}$$

Por cuanto, la probabilidad de discriminación sin ambigüedad depende del modulo del producto interior $|\alpha|$, de la fase del producto interior θ y del número de estados a discriminar n.

7.4. Copia Probabilista de Estados

Duan y Guo [141] demuestran que un conjunto de estados pueden ser copiados en forma probabilista, si y sólo si, el conjunto de estados es linealmente independiente. Además, demuestran que un conjunto de estados $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_n\rangle\}$, puede ser copiado en forma probabilista generando M copias, con una matriz de eficiencia diagonal Γ, si y sólo si, la matriz

$$X^{(1)} - \sqrt{\Gamma}X_p^{(M)}\sqrt{\Gamma^\dagger}, \tag{7.40}$$

es semidefinida positiva, donde

$$X^{(1)} = [\langle\psi_i|\psi_j\rangle], \tag{7.41}$$
$$X_p^{(M)} = [\langle\psi_i|\psi_j\rangle^M\langle P^{(i)}|P^{(j)}\rangle], \tag{7.42}$$
$$\sqrt{\Gamma} = \sqrt{\Gamma^\dagger} = diag(\sqrt{p_1},\sqrt{p_2},,...,\sqrt{p_n}), \tag{7.43}$$

y la tranformación de copiado tiene la forma

$$U(|\psi_i\rangle|\Sigma\rangle^{\otimes(M-1)}|P_0\rangle) = \sqrt{p_i}|\psi_i\rangle^{\otimes M}|P^{(i)}\rangle + \sqrt{1-p_i}|\Phi_{ABP}^{(i)}\rangle, \qquad i=1,...,n. \tag{7.44}$$

Los estados de la máquina $|P_0\rangle$ y $|P^{(i)}\rangle$ con $i=1,...,n$, son estados normalizados que no son (en general) ortogonales, y los estados $|\Phi_{ABP}^{(1)}\rangle$, $|\Phi_{ABP}^{(2)}\rangle$,...,$|\Phi_{ABP}^{(n)}\rangle$, son n estados normalizados del sistema compuesto ABP que son en general no ortogonales.

Duan y Guo [141] también establecen la conección entre el copiado probabilista de los estados $|\psi_k\rangle$ y la discriminación sin ambigüedad de los estados $|\psi_k\rangle$. Cuando el número de copias es muy grande, es decir cuando M tiende a infinito, la probabilidad de copiar los estados se hace igual a la probabilidad de discriminación del conjunto de estados. Además, la condición bajo la cual se obtiene la máxima probabilidad de discriminación es que la matriz $X^{(1)}-\Gamma$ sea semidefinida positiva.

7.5. Copia Probabilista de los Estados Igualmente Separados

Ahora, consideramos la copia probabilista de $1 \to M$ de los estados $|\alpha_k\rangle$ con igual probabilidad de preparación $\eta_k = 1/n$. La máquina de copiado probabilista se construye mediante la aplicación de una transformación unitaria U y una medida proyectiva. Inicialmente, un sistema físico es preparado en uno de los estados igualmente separados $|\alpha_k\rangle$ para ser copiado. Se asume que $M-1$ sistemas están inicialmente preparados en el mismo estado conocido $|\Sigma\rangle$. El estado producto de los $M-1$ sistemas es $|\Sigma\rangle^{\otimes(M-1)}$. En estos M sistemas se codificarán las M copias del estado inicial $|\alpha_k\rangle$. También, se considera una ancilla que inicialmente está preparada en el estado $|\xi_0\rangle$.
La acción de la transformación unitaria U sobre los M sistemas junto con la ancilla es dada por

$$U(|\alpha_k\rangle\,|\Sigma\rangle^{\otimes(M-1)}\,|\xi_0\rangle) = \sqrt{P}\,|\alpha_k\rangle^{\otimes M}\,|\xi_0\rangle + \sqrt{1-P}\,|\Phi_k\rangle\,|\xi_1\rangle, \tag{7.45}$$

donde $|\xi_0\rangle$ y $|\xi_1\rangle$ son dos estados ortogonales de la ancilla y $|\Phi_k\rangle$ son estados normalizados linealmente dependientes de los M sistemas, que no son necesariamente ortogonales.
Después de la aplicación de la transformación unitaria U, se realiza una medida del observable $O = \lambda_0\,|\xi_0\rangle\,\langle\xi_0| + \lambda_1\,|\xi_1\rangle\,\langle\xi_1|$ sobre la ancilla. En el caso que el sistema de la ancilla se proyecte al estado $|\xi_0\rangle$, la transformación de copiado es exitosa generando M copias del estado $|\alpha_k\rangle$, con una probabilidad igual a P. En otro caso, el proceso falla con una probabilidad igual a $1-P$. Hemos considerado que todos los estados $|\alpha_k\rangle$ tienen la misma probabilidad P de ser copiados. Esto se justifica dado que los estados $|\Phi_k\rangle$ son linealmente dependientes y las probabilidades de preparación de los estados $|\alpha_k\rangle$ son todas iguales a $\eta_k = 1/n$. Luego, la probabilidad total de éxito en el proceso de copiado es $P_c = \sum_k \eta_k P_k = \frac{1}{n}\sum_k P_k$. Esta expresión alcanza su máximo valor cuando $P_k = P$, $\forall k$. Por lo tanto, la probabilidad total de copiado es $P_c = P$.

Duan y Guo [141] demostraron que una condición necesaria y suficiente para la existencia de la transformación U de la ecuación (7.45) es que los estados a ser copiados deben ser linealmente independientes. Esta condición se satisface si el modulo del producto interior α pertenece al intervalo $|\alpha| = [0, |\overline{\alpha}_\theta|)$, donde

$$|\overline{\alpha}_\theta| = \frac{\sin(\frac{\pi-\theta}{n})}{\sin\left(\theta + \frac{\pi-\theta}{n}\right)}, \qquad \text{para} \qquad 0 \le \theta < 2\pi. \tag{7.46}$$

Ahora, considerando el criterio de Duan y Guo [141], la probabilidad de éxito P para el proceso de copiado $1 \to M$ se obtiene exigiendo que la matriz

$$C = X^{(1)} - PX^{(M)}, \tag{7.47}$$

sea semidefinida positiva. Donde $X^{(1)} = [\langle\alpha_i|\alpha_j\rangle]$ y $X^{(M)} = [\langle\alpha_i|\alpha_j\rangle^M]$ son matrices cuyos coeficientes $X_{ij} = \langle\alpha_i|\alpha_j\rangle$ son los productos interiores entre los estados $|\alpha_k\rangle$ a ser copiados. En nuestro caso, la matriz C tiene la siguiente forma

$$C = \begin{pmatrix} \gamma & \beta & \beta & \dots & \beta \\ \beta^* & \gamma & \beta & \dots & \beta \\ \beta^* & \beta^* & \gamma & \dots & \beta \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta^* & \beta^* & \beta^* & \dots & \gamma \end{pmatrix}, \tag{7.48}$$

donde $\gamma = 1 - P$, y $\beta = \alpha - P\alpha^M$. La matriz en la ecuación (7.48) es hermítica y su estructura tiene forma de una matriz de Toeplitz [150]. Además, puede ser diagonalizada por una matriz unitaria T, tal que $D = TCT^\dagger$ donde

$$T = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & \omega_1^1 & \omega_1^2 & \dots & \omega_1^{n-1} \\ 1 & \omega_2^1 & \omega_2^2 & \dots & \omega_2^{n-1} \\ 1 & \omega_3^1 & \omega_3^2 & \dots & \omega_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^1 & \omega_n^2 & \dots & \omega_n^{n-1} \end{pmatrix}, \tag{7.49}$$

donde

$$\omega_j = e^{i\theta_j} \qquad \text{y} \qquad \theta_j = \frac{2}{n}(\theta_\beta - (j-1)\pi), \qquad \text{para} \qquad j = 1, ..., n. \tag{7.50}$$

Donde $\beta = |\beta|e^{i\theta_\beta}$ con $0 \leq \theta_\beta < 2\pi$. La matriz diagonal $D = diag(\lambda_1, ..., \lambda_n)$ contiene los autovalores reales de C, los cuales en una dimensión n están dados por

$$\lambda_j = \gamma + |\beta| \sum_{k=1}^{n-1} \cos\left((1 - \frac{2k}{n})\theta_\beta + (j-1)\frac{2\pi k}{n} \right), \text{ para } j = 1, ..., n. \tag{7.51}$$

Ahora, usando las identidades trigonométricas

$$\sum_{k=1}^{n} \sin(kx) = \frac{\cos\frac{x}{2} - \cos(n + \frac{1}{2})x}{2\sin\frac{x}{2}}, \tag{7.52}$$

$$\sum_{k=1}^{n} \cos(kx) = \frac{\sin(n + \frac{1}{2})x - \sin\frac{x}{2}}{2\sin\frac{x}{2}}, \tag{7.53}$$

los autovalores λ_j quedan de la forma

$$\lambda_j = \gamma - |\beta| \frac{\sin(\theta_\beta + \frac{(j-1)\pi - \theta_\beta}{n})}{\sin(\frac{(j-1)\pi - \theta_\beta}{n})}, \qquad \text{para} \qquad j = 1, ..., n. \tag{7.54}$$

La matriz C es definida semipositiva si todos sus autovalores son iguales o mayores que cero. Si definimos a f_j, como el término que depende del coeficiente j, de la siguiente forma

$$f_j = -\frac{\sin(\theta_\beta + \frac{(j-1)\pi - \theta_\beta}{n})}{\sin(\frac{(j-1)\pi - \theta_\beta}{n})}, \tag{7.55}$$

luego, el mínimo valor de λ_j corresponde al caso donde el coeficiente f_j es mínimo. Dado que

$$f_j = f_2 \frac{1 + \tan(\frac{(j-2)\pi}{n})\text{cotan}(\theta_\beta + \frac{\pi - \theta_\beta}{n})}{1 + \tan(\frac{(j-2)\pi}{n})\text{cotan}(\frac{\pi - \theta_\beta}{n})}, \tag{7.56}$$

se tiene que el mínimo autovalor es λ_2, el cual es dado por

$$\lambda_2 = \gamma - |\beta| \frac{\sin(\theta_\beta + \frac{\pi - \theta_\beta}{n})}{\sin(\frac{\pi - \theta_\beta}{n})}. \tag{7.57}$$

Luego, la matriz C es definida semi-positiva si $\lambda_2 \geq 0$

$$\lambda_2 = \gamma - |\beta| \frac{\sin(\theta_\beta + \frac{\pi - \theta_\beta}{n})}{\sin \frac{\pi - \theta_\beta}{n}} \geq 0. \tag{7.58}$$

Dado que $\gamma = 1 - P_{1\to M}$, tenemos

$$\lambda_2 = 1 - P_{1\to M} - |\beta| \frac{\sin(\theta_\beta + \frac{\pi - \theta_\beta}{n})}{\sin \frac{\pi - \theta_\beta}{n}} \geq 0. \tag{7.59}$$

Esto nos permite obtener implicitamente la probabilidad de éxito $P_{1\to M}$ de copiado de los estados igualmente separados $|\alpha_k\rangle$, la cual es dada por

$$P_{1\to M} = 1 - |\beta| \frac{\sin(\theta_\beta + \frac{\pi - \theta_\beta}{n})}{\sin \frac{\pi - \theta_\beta}{n}}, \tag{7.60}$$

donde

$$\beta = \alpha - P_{1\to M} \alpha^M. \tag{7.61}$$

La última ecuación indica que tanto la fase θ_β como el modulo $|\beta|$ son funciones de $P_{1\to M}$. Estas dos cantidades también aparecen en la ecuación (7.60) lo que dificulta encontrar una expresión analítica para $P_{1\to M}$ como función del producto interior α, el número de estados n y el número de copias M. Sin embargo, las ecuaciones (7.60) y (7.61) se pueden tratar numéricamente y para algunas elecciones de ángulo θ se puede obtener soluciones analíticas.

De acuerdo a la ecuación (7.60), la probabilidad de copiar $P_{1\to M}$ tiene la misma forma que la probabilidad de discriminación sin ambigüedad P_s de los estados $|\alpha_k\rangle$ dada por la ecuación (7.39)

$$P_s = 1 - |\alpha| \frac{\sin(\theta + \frac{\pi - \theta}{n})}{\sin \frac{\pi - \theta}{n}}, \tag{7.62}$$

esto permite que se satisfaga el límite $P_{1\to\infty} = P_s$, ya que cuando $M \to \infty$ tenemos $\beta = \alpha$, y por lo tanto,

$$P_{1\to\infty} = P_s = 1 - |\alpha| \frac{\sin(\theta + \frac{\pi - \theta}{n})}{\sin \frac{\pi - \theta}{n}}, \tag{7.63}$$

es decir, la probabilidad de copiado cuando realizamos un número muy grande copias es igual a la discriminación sin ambigüedad de los estados igualmente separados.

La probabilidad de éxito $P_{1\to M}$ también puede ser comparada con un límite superior [148, 149] de la probabilidad de copiado óptimo en el proceso de $N \to M$ copias. Este límite superior es válido para un conjunto arbitrario de n estados no ortogonales linealmente independientes $|\psi_k\rangle$, con $k = 1, ..., n$, que tienen probabilidades de generación iguales a $\eta_k = 1/n$. Este límite es dado por

$$P_{N\to M} \leq \frac{2}{n(n-1)} \sum_{i<j} \frac{1 - |\langle\psi_i|\psi_j\rangle|^N}{1 - |\langle\psi_i|\psi_j\rangle|^M}, \tag{7.64}$$

el cual en el caso particular de los estados igualmente separados $|\alpha_k\rangle$ es

$$P_{1\to M} \leq \frac{1-|\alpha|}{1-|\alpha|^M}. \tag{7.65}$$

Este límite superior para la probabilidad de copiado de la ecuación (7.65) se alcanza cuando $\theta = 0$. En este caso, se tiene $\theta = \theta_\beta = 0$, y $|\alpha| \in [0,1)$, con lo cual la probabilidad de copiado $1 \to M$ en la ecuación (7.60) es

$$P_{1\to M} = \frac{1-|\alpha|}{1-|\alpha|^M}. \tag{7.66}$$

Por lo tanto, en el caso que el conjunto de estados tenga un producto interior real positivo $|\alpha| \in [0,1)$, la máquina de copiado probabilista es óptima en el sentido que permite alcanzar la máxima probabilidad en el proceso de copiado de $1 \to M$ copias. El resultado de la ecuación (7.66) es válido para un conjunto arbitrario de n estados igualmente separados bajo la condición que el producto interior α tenga un valor real positivo. Además, la ecuación (7.66) generaliza la probabilidad de copiado $P_{1\to M}$ de la ecuación (7.2) para dos estados no ortogonales, obtenida por Chefles y barnett [147], al caso de un número arbitrario de estados igualmente separados.

La Fig. (7.1) muestra la probabilidad de copia de los estados igualmente separados, en función del modulo del producto interior α, en el caso real $\theta = 0$, para n estados igualmente separados y cuando realizamos varias copias $M = 2$, $M = 3$, $M = 4$ y $M = 10$.

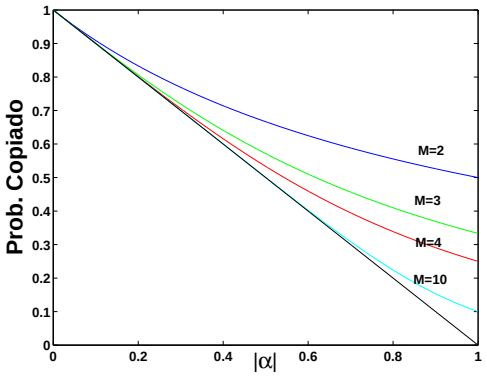

Figura 7.1: Probabilidad de copiado en función del modulo de α para varios valores del número M de copias.

De la figura se puede concluir, que la probabilidad de copia de los estados para un M fijo, alcanza un máximo igual a uno cuando los estados son ortogonales $|\alpha| = 0$, y luego, disminuye hasta alcanzar un mínimo (que depende de M) cuando el modulo del producto interior es igual a uno. Además, vemos que a medida que aumenta el número de copias M la probabilidad de copiar los estados disminuye y se acerca asintóticamente a la probabilidad de discriminar los estados $P_s = 1 - |\alpha|$, que corresponde a la linea negra del gráfico.

Para valores de la fase θ distintos de cero, se requiere resolver simultáneamente las ecuaciones

(7.60) y (7.61). Descomponiendo, $\beta = \alpha - P_{1\to M}\alpha^M$ en su parte real e imaginaria, tenemos

$$|\beta|\sin(\theta_\beta) = |\alpha|\sin(\theta) - P_{1\to M}|\alpha|^M \sin(M\theta), \tag{7.67}$$
$$|\beta|\cos(\theta_\beta) = |\alpha|\cos(\theta) - P_{1\to M}|\alpha|^M \cos(M\theta). \tag{7.68}$$

Luego, es posible expresar el modulo de β en términos de $|\alpha|$, θ, M y el ángulo θ_β, de la siguiente forma

$$|\beta| = |\alpha|\frac{\sin(M\theta-\theta)}{\sin(M\theta-\theta_\beta)}. \tag{7.69}$$

Sustituyendo la ecuación (7.69) en la ecuación (7.60), la probabilidad de copia $P_{1\to M}$ queda

$$P_{1\to M} = 1 - |\alpha|\frac{\sin(M\theta-\theta)}{\sin(M\theta-\theta_\beta)}\frac{\sin(\theta_\beta + \frac{\pi-\theta_\beta}{n})}{\sin\frac{\pi-\theta_\beta}{n}}. \tag{7.70}$$

De manera de determinar la probabilidad de copia de los estados igualmente separados desde la ecuación (7.70), se necesita encontrar el valor de θ_β como función de $|\alpha|$, θ, M y n. Para esto, se requiere resolver numéricamente la siguiente ecuación

$$\frac{\sin(\theta_\beta + \frac{\pi-\theta_\beta}{n})}{\sin\frac{\pi-\theta_\beta}{n}} = \frac{\sin(M\theta-\theta_\beta)}{|\alpha|\sin(M\theta-\theta)} - \frac{\sin(\theta-\theta_\beta)}{|\alpha|^M\sin(M\theta-\theta)}. \tag{7.71}$$

Desde la ecuación (7.70) se puede ver fácilmente que cuando los estados igualmente separados son ortogonales, es decir $|\alpha| = 0$, la probabilidad de copiado es igual a uno, lo cual es consistente con el hecho que es posible copiar de manera perfecta estados ortogonales. En otro caso, tenemos una probabilidad de éxito en el proceso de copiado es menor que la unidad.

En los siguientes gráficos, vemos el efecto que produce la fase del producto interior θ en función del modulo del producto interior $|\alpha|$ en la probabilidad de copia (7.70), al fijar el número de estados n y el número de copias M.

De los gráficos vemos que, en cualquiera de las curvas, para un valor fijo de θ la probabilidad de copia decrece con el modulo de α, desde su máximo valor igual a uno cuando los estados son ortogonales $|\alpha| = 0$, hasta su mínimo valor igual a cero cuando los estados son linealmente dependientes, esto es para $|\alpha| = |\overline{\alpha}_\theta|$. También es claro desde la Fig. (7.2) que la probabilidad de copiado tiene a la curva $\theta = 0$ como su límite superior y decrece a medida que aumenta θ hasta alcanzar su mínimo valor para $\theta = \pi$. Este comportamiento no depende del número de copias M y del número de estados n. También se puede apreciar de las figuras que para un M y $\theta \neq 0$ fijos, la probabilidad de copiado decrece con el número n de estados igualmente separados. Se debe notar que la probabilidad de copiado satisface $P_{1\to M}(\theta) = P_{1\to M}(-\theta)$, que permite completar el rango de valores de $\theta \in [0, 2\pi)$.

En los siguientes gráficos fijamos el número de estados $n = 3$, y el ángulo θ y analizamos como cambia la probabilidad de copia (7.70) en función del modulo del producto interior, al aumentar el número de copias M.
La Fig. (7.3) muestra el comportamiento de la probabilidad de copiado en función de α para cuatro valores del ángulo θ. En cada uno de los gráficos de la figura mantenemos el número de

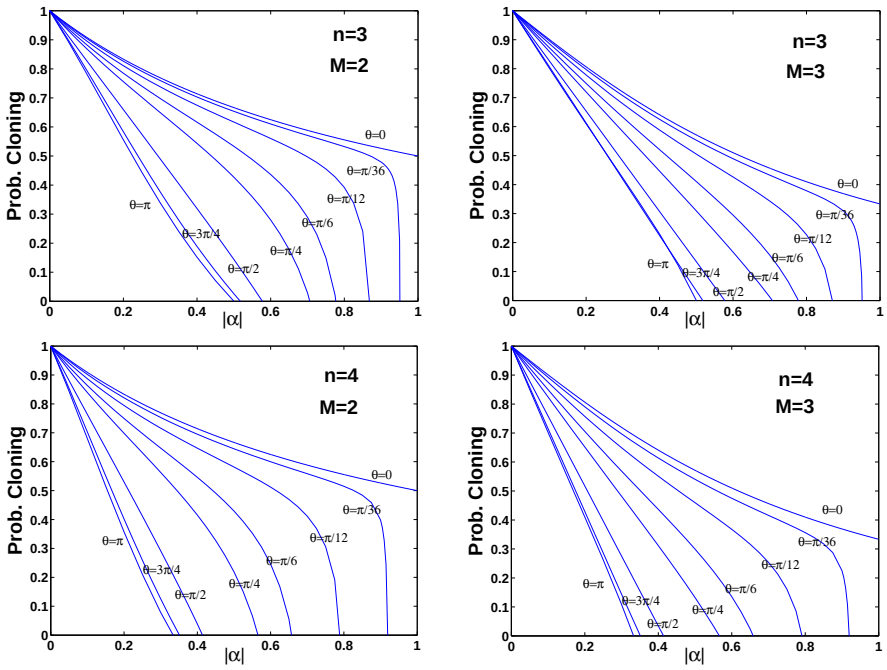

Figura 7.2: Probabilidad del copiado en función de la fase y del modulo de α para algunos valores del número de copias M y de la dimensión n de los estados: a) n=3, M=2; b) n=3, M=3; c) n=4, M=2; d) n=4, M=3.

estados $n = 3$ y cambiamos el número de copias M. En los gráficos, la linea negra representa la probabilidad de discriminación sin ambigüedad P_s dada por la ecuación (7.39). Se puede apreciar que a medida que se incrementa el ángulo θ la probabilidad de éxito $P_{1\to M}$ converge más rápido a la probabilidad de discriminación sin ambigüedad P_s, en este sentido se requieren menos copias. Además, las figuras para $\theta = \pi/2$ y para $\theta = \pi$, muestran que para ciertos valores de M la probabilidad de copiado es menor que la probabilidad de discriminación sin ambigüedad P_s. En este caso, parece más conveniente discriminar los estados y luego, preparar tantas copias como se desee. Además, estas figuras también muestran que para ciertos casos $P_{1\to M}$ es mayor que $P_{1\to M'}$, cuando M es más grande que M'. Por lo tanto, para algunos valores de α y n es mejor realizar un mayor número de copias. Una posible explicación a este comportamiento en la probabilidad de copiado es que para ciertos casos la máquina de copiado propuesta no es óptima. En estos puntos, podría existir otra máquina de copiado que alcance mayores probabilidades de copiado. Esto fue analizado por Roa *et al.* [151] al introducir un sistema auxiliar que permite absorver la fase del producto interior de los estados y en principio alcanzar mayores probabilidades de copiado.

Algunos de los resultados no esperados expuestos anteriormente pueden ser deducidos desde las ecuaciones (7.60) y (7.61). Por ejemplo, para el caso $\theta = \pi$ obtenemos

$$P_{1\to M}(\theta = \pi) = \frac{1 - 2|\alpha|}{1 + 2(-1)^M |\alpha|^M}, \tag{7.72}$$

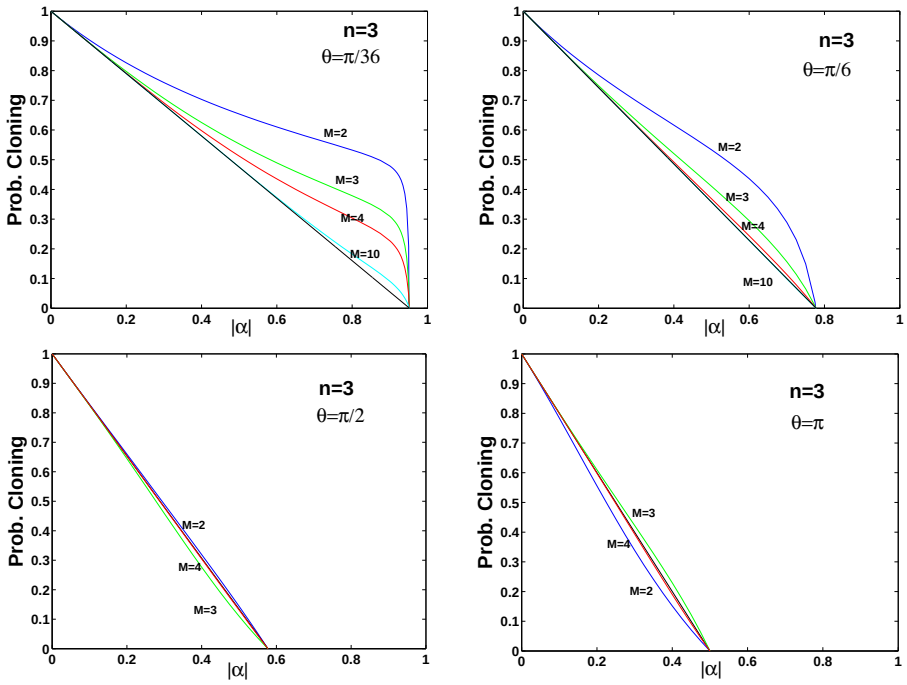

Figura 7.3: Probabilidad del copiado en función del modulo de α para algunos valores del número de copias M y para una dimensión fija $n = 3$, y para los valores del ángulo θ igual a: a) $\pi/36$, b) $\pi/6$, c) $\pi/2$, d) π. En la figura, hay una correspondencia entre el color y el número de copias, azul $M = 2$, verde $M = 3$, rojo $M = 4$ y celeste $M = 10$.

donde $|\alpha| \in [0,1/2)$. Usando esta expresión se puede mostrar que $P_{1\to 2} \leq P_s \leq P_{1\to 3}$, lo cual esta de acuerdo con la solución numérica de las ecuaciones (7.60) y (7.61) que aparece en la Fig. (7.3d). Un resultado similar se obtiene en el caso $\theta = \pi/2$, para un número M de copias impar, tenemos

$$P_{1\to M}(\theta = \pi/2) = \frac{1 - |\alpha|\text{cotan}(\frac{\pi}{2n})}{1 + (-1)^{\frac{M+1}{2}}|\alpha|^M \text{cotan}(\frac{\pi}{2n})}. \tag{7.73}$$

Es posible deducir un límite para los valores de θ donde aparece este extraño comportamiento. Considerando que $\theta_\beta \approx \theta$ y comparando las ecuaciones (7.39) con la ecuación (7.60) vemos que la probabilidad de discriminación sin ambigüedad es mayor que la probabilidad de copiado de los estados cuando $|\beta| > |\alpha|$. La ecuación (7.61) se puede expresar de la forma

$$|\beta|^2 = |\alpha|^2(1 + P_{1\to M}|\alpha|^{M-1}[P_{1\to M}|\alpha|^{M-1} - 2\cos(M-1)\theta]), \tag{7.74}$$

luego, se tiene que $|\beta| > |\alpha|$ cuando $P_{1\to M}|\alpha|^{M-1} > 2\cos(M-1)\theta$, esto ocurre cuando se cumple la condición $\cos(M-1)\theta < 0$. Por lo tanto, cuando el ángulo θ está en el intervalo

$$\frac{\pi}{2(M-1)} < \theta < \frac{3\pi}{2(M-1)}. \tag{7.75}$$

En general, es posible encontrar un valor de M para un cierto ángulo $\theta \neq 0$ donde por ejemplo la probabilidad de copiado es menor que la probabilidad de discriminación sin ambigüedad de

los estados. Esto puede indicar que la máquina de copiado propuesta es sólo óptima cuando $\theta = 0$ y cuando se tiene $\theta \neq 0$ podría existir en principio una mejor máquina de copiado. Por otro lado, si bien nuestros resultados aparentemente no son los óptimos para todas las fases θ del producto interior α, no hay conflictos con el principio de Relatividad Especial. El principio de Relatividad Especial impone un límite sobre la velocidad de propagación de señales. Este principio se ha utilizado para encontrar un cotas superiores para la probabilidad máxima de copiado permitida por la Mecánica Cuántica [152, 153]. Además, se sostiene [152] que la Teoría Cuántica tampoco permite en forma probabilista violar el principio de Relatividad Especial. Por otro lado, para el caso del copiado determinista, D. Bruss [54] demostró la imposibilidad de la transferencia de información en forma superlumínica. Además, se sostiene que la "pacifica coexistencia" entre Mecánica Cuántica y Relatividad está automáticamente garantizada por la linealidad y completitud de cualquier proceso mecánico cuántico.

7.6. Conclusiones

Se ha caracterizado el conjunto de estados igualmente separados, esta familia de estados se describe por sólo un paramétro complejo α que es producto interior entre los estados. Se ha encontrado la forma explícita de los estados en la base lógica y la transformación unitaria que conecta los estados. También, se logro expresar la base lógica en términos de los n estados igualmente separados. Además, hemos estudiado una máquina de copiado probabilista que genera M copias de n estados igualmente separados. Se ha estudiado el efecto de la fase y el modulo del producto interior α que caracteriza a los estados igualmente separados, en la probabilidad de copiado. Nuestros resultados están de acuerdo con límites conocidos de este tipo de transformaciones. Por ejemplo, la probabilidad de copiado es igual a uno si los estados son ortogonales, y si los estados son linealmente dependientes la probabilidad de copiado es igual a cero. En el límite asintótico de un número infinito de copias, la probabilidad de copiado tiende a la probabilidad de discriminación sin ambigüedad de los estados igualmente separados. También se demostró que la probabilidad de copiado óptima se alcanza cuando los estados igualmente separados tienen un producto interior real positivo. En este caso, la probabilidad de copiado parece ser una generalización de un resultado obtenido previamente para el caso de dos estados no ortogonales. Para determinar la probabilidad de copiado en un caso más general con la fase del producto interior distinto de cero es dificil obtener una expresión analítica para la probabilidad de copiado. Sin embargo, fue posible demostrar para ciertos valores de la fase la probabilidad de copiado es menor que la probabilidad de discriminación sin ambigüedad. Además, para algunos casos se tiene una mayor probabilidad de copiado al generar un mayor número de copias. Esto nos indica que para ciertos casos la máquina de copiado no es la óptima y en principio es posible construir una máquina de copiado probabilista que permita alcanzar mayores probabilidades de copiado.

Capítulo 8

Conclusión

Los principales resultados de la tesis son: primero, establecer un esquema experimental para discriminar estados simétricos; segundo, una propuesta para realizar la distribución de estados cuánticos al utilizar estados entrelazados y finalmente la caracterización de los estados igualmente separados, con los cuales se realizó el copiado probabilista de estados.

Habitualmente, en los protocolos de comunicaciones cuánticas se utilizan estados cuánticos ortogonales para codificar la información. Sin embargo, como la generación experimental de los estados no es perfecta y dado la presencia de ruido en el canal de comunicación, se tiene generalmente estados cuánticos no ortogonales. Un recurso que también se utiliza en Información Cuántica es el entrelazamiento entre dos o más partículas. Pero, dado que la generación experimental de estados entrelazados no es del todo perfecta se cuenta sólo con estados parcialmente entrelazados. Esto origina que la eficiencia en los protocolos de comunicaciones cuánticas disminuya. Una técnica utilizada para aumentar el grado de entrelazamiento entre las partículas parcialmente entrelazadas es conocida como concentración del entrelazamiento. La concentración del entrelazamiento se puede realizar en forma probabilista y mediante la discriminación de estados no ortogonales. Además, si se utilizan estados parcialmente entrelazados para transmitir información uno de los usuarios en el canal de comunicación debe realizar la discriminación de estados no ortogonales. Los estados cuánticos no son observables, es decir no se pueden medir en el sentido clásico. Por esta razón, no podemos acceder directamente a la información codificada en los estados. De manera de acceder a la información codificada en los estados debemos ser capaces de distinguir o discriminar los estados. Sin embargo, los estados no ortogonales no pueden ser identificados o copiados de manera determinista. Esta propiedad de los estados no ortogonales es ampliamente utilizada en criptografía cuántica. En los protocolos de criptografía cuántica, si un usuario no autorizado trata de obtener información desde los estados no ortogonales, inevitablemente introducirá perturbaciones detectables en el estado. Por lo tanto, los estados no ortogonales permiten generar canales de comunicación seguros entre los usuarios autorizados. Por las razones expuestas anteriormente, una etapa fundamental en los protocolos de comunicaciones cuánticas es la discriminación de estados. Si el conjunto de estados estados es mutuamente ortogonal es posible discriminar los estados en forma conclusiva. Sin embargo, si el conjunto de estados posee a lo menos dos estados no ortogonales, sólo se tiene una cierta probabilidad de discriminación que es menor que la unidad. La optimización de la probabilidad de éxito en el proceso de discriminación se enfrenta con dos posibles estrategias conocidas como:

discriminación con mínimo error y discriminación sin ambigüedad.

Bajo ciertas condiciones los estados no ortogonales a ser discriminados forman un conjunto de estados simétricos linealmente independientes. La discriminación conclusiva de esta clase de estados permite por ejemplo, la criptografía cuántica [62], la concentración del entrelazamiento [97], la teleportación cuántica de qudits [108], el intercambio del entrelazamiento [109] y codificación densa [110]. Por este motivo es importante la implementación experimental de esquemas de discriminación. En este contexto, hemos propuesto un esquema experimental para discriminar cuatro estados simétricos mediante la estrategia de discriminación sin ambigüedad. Mediante una modificación del esquema para la discriminación sin ambigüedad de los estados es posible también implementar la discriminación con mínimo error de los cuatro estados simétricos. En el esquema experimental se utiliza óptica lineal para realizar las cuatro etapas en el proceso de discriminación sin ambigüedad: (I) preparación de los estados, (II) aplicación de la transformación unitaria condicional, (III) la medida en la ancilla y (IV) la detección de los estados en la base lógica. Para el proceso de discriminación con mínimo error sólo se requiere realizar las etapas de preparación de los estados y detección de los estados en la base lógica. Las propuestas experimentales han sido diseñadas para obtener la probabilidad óptima tanto en el proceso de discriminación sin ambigüedad como en la discriminación con mínimo error de los estados simétricos. En el esquema experimental se requiere la presencia de fotones individuales para realizar el proceso de discriminación de los estados. Para producir fotones individuales se considera la generación de estados de dos fotones en el proceso de conversión paramétrica espontánea descendente. Dado que los fotones generados en este proceso están entrelazados, uno de ellos nos permite realizar el proceso de discriminación mientras que el otro fotón nos permite asegurar la presencia de un fotón individual en el esquema de discriminación al medir los fotones en coincidencia. Los estados simétricos se codifican en los cuatro posibles caminos de propagación del fotón, y la ancilla en el proceso de discriminación sin ambigüedad es la polarización del fotón. En el caso de la discriminación sin ambigüedad, la transformación unitaria condicional se realiza mediante una rotación de la polarización del fotón que es dependiente del camino de propagación del fotón. Por otro lado, la medida en la ancilla nos estrega un resultado conclusivo si se mide el fotón con polarización vertical. Uno de los principales requerimientos experimentales es la estabilización de los interferómetros en la configuración de Mach-Zehnder que permiten generar la transformada de Fourier en dimensión cuatro, para medir el fotón en la base lógica. Los esquemas de discriminación consideran un número reducido de elementos ópticos y puede ser generalizado fácilmente al caso de 2^N estados simétricos. En el caso de otras dimensiones, el protocolo también funciona con la implementación óptica de la transformada inversa de Fourier. Con los cuatro estados simétricos considerados también es posible construir dos estados mixtos, los cuales son superposiciones incoherentes de los estados simétricos. Modificando los respectivos esquemas experimentales para la discriminación de los estados simétricos es posible realizar la discriminación sin ambigüedad y con mínimo error de dos estados mixtos. En este caso, también se alcanza la probabilidad de discriminación óptima en los procesos de discriminación sin ambigüedad y de la discriminación con mínimo error de los dos estados mixtos.

La criptografía cuántica provee de una forma segura para transmitir información entre dos o más usuarios. Los protocolos de criptografía cuántica son diseñados de manera que cualquier intruso en el canal de comunicación deje una marca en la llave usada para codificar la infor-

mación. Por medio de esto, es posible decidir si una llave puede ser usada en forma segura o se debe generar una nueva. Recientemente, la criptografía cuántica ha sido extendida al caso de distribución de secretos cuánticos. Esta generalización se origina cuando examinamos la versión clásica del problema de distribución de secretos, esto es, la distribución de información sensible entre muchas partes de manera que una parte deshonesta no puede tener acceso a la información completa. En el caso cuántico el secreto a ser distribuido puede ser una clave clásica o un estado cuántico. El estado distribuido puede ser recuperado por una de las partes si las restantes cooperan, al entregarle la información de sus respectivas medidas. En este contexto, se estudió la distribución de estados cuánticos de dimensión d entre tres usuarios y caracterizamos el conjunto de estados maximalmente entrelazados que pueden ser usados como canal cuántico en el protocolo. También consideramos el uso de un canal no ideal, es decir, estados que están parcialmente entrelazados. En este caso, relacionamos los protocolos para distribuir un qudit con el problema de la discriminación de estados simétricos. Esto permite la formulación de un protocolo, donde la recuperación del estado se logra con una cierta probabilidad de éxito.

Los estados simétricos aparecen en forma natural en los protocolos de comunicaciones cuánticas. Sin embargo, a medida que aumentamos el número de estados linealmente independientes la cantidad de parámetros que debemos manejar dificulta la obtención de resultados. Este problema se resuelve parcialmente con los estados igualmente separados, donde tenemos sólo un parámetro α, el producto interior entre los estados, independiente del número de estados que posee el conjunto de estados igualmente separados. Por esta razón, se decidió estudiar las propiedades de los estados igualmente separados.

Los estados igualmente separados $\{|\alpha_k\rangle\}$ representan un nuevo conjunto de estados cuánticos. Sin embargo, cuando el producto interior entre los estados igualmente separados es un número real, hemos demostrado que el conjunto de estados igualmente separados es también un conjunto de estados simétricos. Además, hemos parametrizado los estados igualmente separados en una dimensión n arbitraria, y hemos establecido una transformación unitaria que conecta los estados igualmente separados. Luego, se estudió la probabilidad de discriminación óptima sin ambigüedad de los estados igualmente separados para todo valor del parámetro α. Una aplicación de los estados igualmente separados fue la copia probabilista, se propuso una máquina de copiado probabilista y se determinó la probabilidad de copia para el proceso de $1 \to M$ copias. Además, se analizó el efecto que produce la fase θ del producto interior de los estados en la probabilidad de copia de los estados. Se obtuvo algunos resultados conocidos tales como: si los estados son ortogonales la probabilidad de copiado es igual a la unidad y cuando los estados son linealmente dependientes la probabilidad de copiado es igual a cero. Se verificó que en el límite de muchas copias la probabilidad de copia se hace igual a la probabilidad de discriminación sin ambigüedad de los estados igualmente separados. La probabilidad de copiado en el caso $\theta = 0$ de n estados igualmente separados parece ser una generalización de un resultado previo obtenido para el caso de considerar sólo dos estados no ortogonales. La fase θ del producto interior en el proceso de copia probabilista de los estados introduce un efecto de atenuación de la probabilidad de copiado. Es decir, la máxima probabilidad de copiado se obtiene en el caso que los estados tienen un producto interior real $\theta = 0$ y a medida que aumentamos la fase θ la probabilidad de copiado disminuye hasta alcanzar un mínimo en $\theta = \pi$. En el caso, que el producto interior es un número real positivo, hemos demostrado que la máquina de copiado es óptima. Sin embargo,

la máquina de copiado propuesta no es óptima bajo ciertos valores de la fase θ y del número de copias M. Dado que aparece una oscilación de la probabilidad de copiado de los estados en torno a la probabilidad de discriminación con el número de copias. Este extraño comportamiento de la probabilidad de copiado hace que por ejemplo sea más probable generar un mayor número de copias de un estado que un menor número de copias. Además, fue posible demostrar que para ciertos valores de la fase θ, la probabilidad de copiado de la máquina propuesta es menor que la probabilidad de discriminación sin ambigüedad de los estados igualmente separados. Por lo tanto, en principio se podría proponer una máquina de copiado probabilista que realice con mayor probabilidad el proceso para aquellos casos donde la probabilidad de copiado es menor que la probabilidad de discriminación sin ambigüedad.

Los estados igualmente separados $\{|\alpha_k\rangle\}$ generan toda una nueva linea de investigación, dado que representan el conjunto de estados cuánticos más simple que podemos utilizar. Una de las principales contribuciones de la tesis fue proporcionar la forma explícita de los estados igualmente separados en términos de una base ortogonal. También, se proporciona la transformación inversa, es decir la base lógica ortogonal en función de los estados igualmente separados. Esto permite que los estados igualmente separados puedan ser utilizados en muchos procesos de Óptica e Información Cuántica. Los posibles trabajos futuros son por ejemplo: proponer un esquema de discriminación de los estados igualmente separados para una posible realización experimental. Realizar el copiado probabilista y determinista de estados simétricos. Proponer una máquina de copiado probabilista que sea óptima para todo valor del producto interior α de los estados igualmente separados. Realizar el copiado determinista de n estados igualmente separados, lo que permite posteriormente proponer un esquema de criptografía cuántica utilizando los estados igualmente separados.

Apéndice A

Medidas de Entrelazamiento

- **Entropía relativa del entrelazamiento**(E_R), es un tipo de distancia del estado entrelazado ρ con respecto al estado separable σ que pertenece a un conjunto S de estados separables, aunque esta no es una distancia en el sentido matemático, se define como:

$$E_R(\rho) = \inf_{\sigma \in S} \; Tr[\rho(log\rho - log\sigma)]. \tag{A.1}$$

- **Destilación del entrelazamiento**(E_D), nos entrega la razón r a la cual un estado mixto ρ puede ser convertido en un estado maximalmente entrelazado sólo mediante LOCC. Se define como,

$$E_D(\rho) = \sup \left\{ r : \lim_{n\to\infty} \left[\inf_{\Psi} \; Tr|\Psi(\rho^{\otimes n}) - \Phi(2^{rn})| \right] = 0 \right\}, \tag{A.2}$$

donde Ψ es una operación LOCC que preserva la traza y $\Phi(K) = |\psi_K\rangle \langle\psi_K|$ es el operador densidad correspondiente a un estado maximalmente entrelazado en dimensión K, donde $|\psi_K\rangle$ es dado por la expresión(3.19).

- **Costo del entrelazamiento**(E_C), para un estado ρ dado, cuantifica la máxima razón r posible a la cual se puede convertir bloques de 2-qubit maximalmente entrelazados, en estados de salida que son copias aproximadas de ρ, en el límite de muchos bloques la copia aproximada tiende al estado ρ.

$$E_C(\rho) = \inf \left\{ r : \lim_{n\to\infty} \left[\inf_{\Psi} \; Tr|\rho^{\otimes n} - \Psi(\Phi(2^{rn}))| \right] = 0 \right\}. \tag{A.3}$$

Bibliografía

[1] C. Shannon. *The mathematical theory of communication*. Bell Systems Technical Journal **27**, 379-423 (1948).

[2] C. Shannon. *Communication theory of secrecy systems*. Bell Systems Technical Journal **28**, 656-715 (1949).

[3] N. Abramson. *Teoría de la Información y Codificación*. Paraninfo (1966).

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

[5] M. Dusek, N. Lütkenhaus, M. Hendrych, arXiv:quant-ph/0601207v3 (2006).

[6] W. Diffie, M. Hellman, IEEE Transactions on Information Theory **22**, 644 (1976).

[7] R. Rivest, A. Shamir, L. Adleman, Communications of the ACM, **21**(2), 120 (1978).

[8] A. Oprea, *Efficient Cryptographic Techniques for Securing Storage Systems*, Ph.D. thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh (2007). http://www.rsa.com/rsalabs/node.asp?id=2218.

[9] A. Turing, Proc. Lond. Math. Soc. Ser. 2, **42**, 230 (1936).

[10] A. Church, Am. J. Math. **58**, 345 (1936).

[11] A. Delgado, *Stabilization of quantum coherence and entanglement*, Ph.D. thesis, Fakultät für Naturwissenschaften, Universität Ulm. (2001).

[12] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[13] W. Heisenberg, Zeitschrift für Physik, **43**, 172-198 (1927).

[14] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

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

[16] P. Shor, e-print arXiv:quant-ph/9508027v2 (1996).

[17] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[18] E. Schrödinger, *Proc. Cambridge Phil. Soc.***31**: p. 555 (1935).

[19] A. Eisntein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935).

[20] N. Bohr, Phys. Rev. **48**, 696 (1935).

[21] D. Bohm, Phys. Rev. **85**, 166 (1952).

[22] J. S. Bell, Physics **1**, 195 (1964).

[23] M. Zukowski, A. Zeilinger, M. A. Horne, A. K. Ekert, Phys. Rev. Lett **71**, 4287 (1993).

[24] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[25] K. Tamaki, M. Koashi, N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[26] R. Werner, Phys. Rev. A **40**, 4277 (1989).

[27] J. Clauser, M. Horne, A. Shimony, R. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[28] A. Aspect, P. Grangier, G. Roger, Phys. Rev. Lett. **49**, 91 (1982).

[29] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, N. Gisin, Phys. Rev. A **57**, 3229 (1998).

[30] D. Boschi, S. Franca, F. De Martini, L. Hardy, S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[31] E. Hagley, X. Maitre, G. Nogues, C. Wunderlich, M. Brune, J. M. Raimond, S. Haroche, Phys. Rev. Lett. **79**, 1 (1997).

[32] M. Plenio, S. Virmani, arXiv:quant-ph/0504163v3 (2006).

[33] M. Donald, M. Horodecki, O. Rudolph, quant-ph/0105017v2 (2002).

[34] D. Bruß, quant-ph/0110078v1 (2001).

[35] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

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

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

[38] P. Horodecki, Phys. Lett. A **232**, 333 (1997).

[39] G. Vidal, R. Werner, Phys. Rev. A **65**, 032314 (2002).

[40] A. Holevo, *Information theoretical aspects of quantum measurements*. Problems of Information Transmission, 9, 177-183, (1973).

[41] K. Mattle, H. Weinfurter, P. Kwiat, A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[42] X. Fang, X. Zhu, M. Feng, X. Mao, F. Du, Phys. Rev. A **61**, 022307 (2000).

[43] J. Mizuno, K. Wakui, A. Furusawa, M, Sasaki, Phys. Rev. A **71**, 012304 (2005).

[44] W. K. Wootters, W. H. Zurek. Nature **299**, 802 (1982).

[45] D. Bouwmeester, J. Pan, K. Matte, M. Eibl, H. Weinfurter, A. Zeilinger, Nature **390**, 575 (1997).

[46] A. Furusawa, J. Sørensen, S. Braunstein, C. Fuchs, H. Kimble, E. Polzik. Science, **282**, 706 (1998).

[47] M. Nielsen, E. Knill, R. Laflamme, Nature **396**, 52 (1998).

[48] H. Kimble, S. J. van Enk, Nature (London) 429, 712 (2004).

[49] J. Pan, D. Bouwmeester, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett **80**, 3891 (1998).

[50] N. Boulant, K. Edmonds, J. Yang, M. Pravia, D. Cory, Phys. Rev. A **68**, 032305 (2003).

[51] J. León, C. Sabín, Phys. Rev. A **78**, 052314 (2008).

[52] S. Bose, V. Vedral, P. Knight, Phys. Rev. A **57** 822, (1998).

[53] A. Delgado, *Apuntes de clases del curso: Información Cuántica*, Departamento de Física, Universidad de Concepción.

[54] D. Bruss, G. DÁriano, C. Macchiavello, M. Sacchi, Phys. Rev. A **62**, 062302 (2000).

[55] K. Kraus. *States, effects and operations*. Lectures notes in physics; 190. Springer-Verlag, Berlin, (1983).

[56] V. Bužek, M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[57] V. Bužek, M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).

[58] V. Scarani, S. Iblisdir, N. Gisin, A. Acín, Rev. Mod. Phys. **77**, 1225 (2005).

[59] R. Werner, Phys. Rev. A **58**, 1827 (1998).

[60] M. Keyl, R. Werner, J. Math. Phys. **40**, 3283 (1999).

[61] C. H. Bennett, G. Brassard, *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, p.175, IEEE, New York (1984).

[62] Joonwoo Bae, Antonio Acín, Phys. Rev. A **75**, 012334 (2007).

[63] I. Csiszár, J. Körner, IEEE Trans. Information Theory **24**, 339 (1978).

[64] C. Fuchs, N. Gisin, R. Griffiths, C. Niu, A. Peres, Phys. Rev. A **56**, 1163 (1997).

[65] D. Bruß, M. Cinchetti, G. DÁriano, C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).

[66] A. Holevo, *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, edited by G. Murayama and J.V. Prokhorov, Lect. Notes Math. Vo.. 330 (Springer-Verlag, Berlin, 1973), p.104.

[67] P. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[68] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, Swiss Federal Institute of Technology, Zurich, quant-ph/0512258 (2005).

[69] J. Bae, *Entanglement and Quantum cryptography*, Ph.D. thesis, Institut de Ciències Fotòniques, Barcelona (2007).

[70] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

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

[72] C. Bennett, G. Brassard, N. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[73] R. Feynman, Inter. J. Theoret. Phys. **21**, 467 (1982).

[74] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).

[75] P. Shor, *Proc. 35th IEEE Symp. on Foundations of Computer Science*, Santa Fe, NM, pp. 124 (1994).

[76] L. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[77] A. Chefles, arXiv:quant-ph/0010114v1 (2000).

[78] M. Neumark: Izv. Akad. SSSR Ser. Mat. **4**, (1940).

[79] C. W. Helstrom, *Quantum detection and estimation theory* (Academic, New York, 1976).

[80] S. M. Barnett, E. Riis, J. Mod. Opt. **44**, 1061 (1997).

[81] A. Holevo, Journal of multivariable analysis **3**, 337 (1973).

[82] H. Yuen, R. Kennedy, M. Lax, IEEE Trans. Inform. Theory **IT-21**, 125 (1975).

[83] S. Barnett, S. Croke, J. Phys. A: Math. Theor. **42**, 062001 (2009).

[84] C. Chou, L. Hsu, Phys. Rev. A **68**, 042305 (2003).

[85] M. Ban, K. Kurokama, R. Momose, O. Hirota, Int. J. Theor. Phys. **55**, 22 (1997).

[86] J. Bergou, U. Herzog, M. Hillery, *Discrimination of Quantum States*, Lect. Notes Phys. **649**, 417-465 (2004).

[87] M. Barnett, Phys. Rev. A **64**, 030303(R) (2001).

[88] R. Clarke, V. Kendon, A. Chefles, S. Barnett, E. Riis, M. Sasaki, Phys. Rev. A **64**, 012303 (2001).

[89] J. Mizuno, M. Fujiwara, M. Akiba, T. Kawanishi, S. Barnett, M. Sasaki, Phys, Rev. A **65**, 012315 (2001).

[90] P. J. Mosley, S. Croke, I. A. Walmsley, S. M. Barnett, Phys. Rev. Lett. **97**, 193601 (2006).

[91] Y. Eldar, Phys. Rev. A **68**, 052303 (2003).

[92] D. Qiu, Phys. Rev. A **77**, 012328 (2008).

[93] I. D. Ivanovic, Phys. Lett. A, **123**, 257 (1987); D. Dieks. Phys. Lett. A, **126**, 303 (1988); A. Peres, Phys. Lett. A, **128**, 19 (1988).

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

[95] R. Clarke, A. Chefles, S. Barnett, E. Riis, Phys. Rev. A **63**, 040305R (2001).

[96] G. Jaeger, A. Shimony, Phys. Lett. A **197**, 83 (1995).

[97] A. Chefles, Phys. Lett. A **239**, 339 (1998).

[98] Y. Sun, M. Hillery, J. Begou, Phys. Rev. A **64**, 022311 (2001).

[99] M. Mohseni, A. Steinberg, J. Bergou, Phys. Rev. Lett. **93**, 200403 (2004).

[100] A. Chefles, S. Barnett, Phys. Lett. A **250**, 223 (1998).

[101] S. Zhang, Y. Feng, X. Sun, M. Ying, Phys. Rev. A **64**, 062103 (2001).

[102] T. Rudolph, R. Spekkens, P. Turner, Phys. Rev. A **68**, 010301(R) (2003).

[103] P. Raynal, N. Lütkenhaus, S. J. van Enk, Phys. Rev. A **68**, 022308 (2003).

[104] P. Raynal, N. Lütkenhaus. Phys. Rev. A **72**, 022342 (2005).

[105] P. Raynal, *Unambiguous State Discrimination of two density matrices in Quantum Information Theory*, Ph.D. thesis, Friedrich-Alexander-Universität, Erlangen-Nürnberg, (2006) arXiv:quant-ph/0611133.

[106] C. Zhang, Y. Feng, M. Ying, Phys. Lett. A **353**, 300 (2006).

[107] Y. Eldar, M. Stojnic, B. Hassibi, Phys. Rev. A **69**, 062318 (2004).

[108] L. Roa, A. Delgado, I. Fuentes-Guridi, Phys. Rev. A **68**, 022310 (2003).

[109] A. Delgado, L. Roa, J. C. Retamal, C. Saavedra, Phys. Rev. A **71**, 012303 (2005).

[110] A. K. Pati, P. Parashar, P. Agrawal, Phys. Rev. A **72**, 012329 (2005); S. Wu, S. M. Cohen, Y. Sun, and R. B. Grifo, Phys. Rev. A **73**, 042311 (2006) .

[111] O. Jiménez, X. Sánchez-Lozano, E. Burgos-Inostroza, A. Delgado, C. Saavedra, Phys. Rev. A, **76**, 062107 (2007).

[112] Bing He, János Bergou, Phys. Lett. A **356**, 306 (2006).

[113] M. Zukowski, A. Zeilinger, A. Horne, Phys. Rev. A **55**, 2564 (1996).

[114] C. K. Hong, L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).

[115] A. U'Ren, C. Silberhorn, J. Ball, K. Banaszek, I. Walmsley, Phys. Rev. A **72**, 021802(R) (2005).

[116] L. Mandel, E. Wolf, *Optical coherence and Quantum Optics*, Cambridge University Press 1995.

[117] H. Bachor, T. Ralph, *A Guide to Experiments in Quantum Optics*. WILEY-VCH Verlag 2004.

[118] A. B. Klimov, R. Guzman, J.C. Retamal, C. Saavedra, Phys. Rev. A **67**, 062313 (2003).

[119] G. Schaller, R. Schutzhold, Phys. Rev. A **74**, 012303 (2006).

[120] A. E. Siegman, Opt. Lett. **26**, 1215 (2001).

[121] C.-L. Chou, L. Y. Hsu, Phys. Rev. A **68**, 042305 (2003).

[122] A. Shamir, Communications of the ACM **22**(11), 612 (1979).

[123] G. Blakley, Proceeding of the National Computer Conference **48**, 313 (1979).

[124] R. Cleve, D. Gottesman, H. Lo, Phys. Rev. A **83**, 648 (1999).

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

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

[127] I. Jex, G. Alber, S. Barnett, A. Delgado, arXiv:quant-ph/0209062v1 (2002).

[128] G. Gordon, G. Rigolin, Phys. Rev. A **73**, 062316 (2006).

[129] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).

[130] G. Alber, A. Delgado, N. Gisin, I. Jex, J. Phys. A: Math. and Gen. **34**, 8821 (2001).

[131] K. Banaszek, Phys. Rev. A **62**, 024301, (2000).

[132] J. Cirac, P. Zoller, H. Kimble, H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).

[133] A. Delgado, C. Saavedra, J.C. Retamal, Phys. Lett. A **370**, 22 (2007).

[134] A.B. Klimov, R. Guzmán, J.C. Retamal, and C. Saavedra, Phys. Rev. A **67**, 062313 (2003).

[135] L. Roa, C. Hermann-Aviliano, R. Salazar, A.B Klimov, B. Burgos, and A. Delgado, arXiv:quant-ph/0808.0725 (2008).

[136] V. Sacarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, No. 4 (2005).

[137] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[138] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).

[139] M. Keyl and R. F. Werner, e-print quant-ph/9807010.

[140] G. Alber, A. Delgado, I. Jex, Quantum Inf. and Comput. Vol.**1**, No. 3 (2001) 33-51.

[141] Lu-Ming Duan and Guang-Can Guo, Phys. Rev. Lett. **80**, 4999 (1998).

[142] A.K. Pati, Phys. Rev. A **83**, 2849 (1999).

[143] A. K. Pati, S. L. Braunstein, Nature (London) **404**, 164 (2000).

[144] D. Qiu, Phys. Rev. A **65**, 052329 (2002).

[145] Y. Feng, S. Zhang, and M. Ying, Phys. Rev. A **65**, 042324 (2002).

[146] Lu-Ming Duan and Guang-Can Guo, Phys. Lett. A **243**, 261 (1998).

[147] A. Chefles, S. Barnett, J. Phys A **31**, 10097 (1998).

[148] D. Qiu, J. Phys. A: Math. Gen **35** (2002) 6931.

[149] Y. Feng, R. Duan, Z. Ji, Phys. Rev. A **72**, 012313 (2005).

[150] I.S. Iohvidov, *Hankel and Toeplitz matrices and forms*, Edited by I. Gohberg, Birkhäuser, Boston (1982).

[151] L. Roa, A. Delgado, O. Jiménez, Copia Probabilista de estados cuánticos igualmente separados, en preparación.

[152] A. K. Pati, Phys. Lett. A **270**, 103 (2000).

[153] L. Hardy, D. Song, Phys. Lett. A, **259**, 331 (1999).

Omar Alejandro Jiménez Henríquez omarjimenez@udec.cl

Publicaciones

- Phys. Rev. A **76**, 062107 (2007). O. Jiménez, X. Sánchez-Lozano, E. Burgos-Inostroza, A. Delgado and C. Saavedra. "Experimental scheme for unambiguous discrimination of linearly independent symmetric state".
- En referato: Quantum Information & Computation. O. Jiménez, C. Muñoz, A. Delgado and A. B. Klimov. "Sharing of D-dimensional quantum states".
- En referato: L. Roa, C. Hermann, R. Salazar, A.B. Klimov, B. Burgos, O. Jiménez and A. Delgado. "Petal-shape probability areas: complete quantum state discrimination".
- En referato: O. Jiménez, L. Roa and A. Delgado. "Probabilistic cloning of equidistant states".

Presentaciones en Congresos

- 27 - 30 Noviembre, 2006. "Quantum Optics III", Pucón, Chile. Presentación de Poster: "Sharing of D-dimensional quantum states".
- 1 - 5 Junio, 2007. "14th Central European Workshop on Quantum Optics", Palermo, Italia. Presentación Oral: "Experimental scheme for unambiguous discrimination between linearly independent symmetric states".
- 6 - 16 Agosto, 2007. "Quantum Information: School and Workshop", Paraty-Rio de Janeiro, Brazil. Presentación de Poster: "Experimental scheme for discrimination between linearly independent symmetric states".
- 13 - 17 Octubre, 2008. "Quantum Optics IV", Florianópolis, Brazil. Presentación de poster: "Experimental scheme for discrimination of symmetric states".

Estadía en centros internacionales de investigación:

- En el CUCEI (Centro Universitario de Ciencias Exactas e Ingeniería) de la Universidad de Guadalajara, México, durante enero de 2006, con el Dr. A. Klimov.
- En el Instituto de Ciencias Fotónicas (ICFO), Barcelona, España, desde el 1 de abril hasta el 31 de junio de 2008, con el Dr. Antonio Acín.